Cloud Access Management

FAQs

Product Documentation

Contents

FAQs
CAM Users and Permissions

Last updated：2024-01-23 18:03:29

How do I grant permissions to the root account?

The root account has all permissions by default and doesn't need to be authorized.

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

You can create a custom policy with the policy generator, select the products and operations you need, and associate the policy with the user. After association, your sub-account will be able to manage the resources under the root account within the scope of permissions you set.

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 do I reset a sub-account's password?

For more information on how to change a sub-user's password, please see Resetting Login Passwords for Sub-Users.
For more information on how to change a collaborator's password, please see Modifying Account Password.

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.

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

Some of Tencent Cloud products are still in beta test, and a few products do not support CAM yet. Please see CAM-Enabled Products to check whether and at what granularity you can manage permissions of a product in CAM.
If you want to use CAM to manage permissions of a product in beta test, please submit a ticket.

How do I implement granular permission management for project resources?

You can implement granular permission management by using tags.

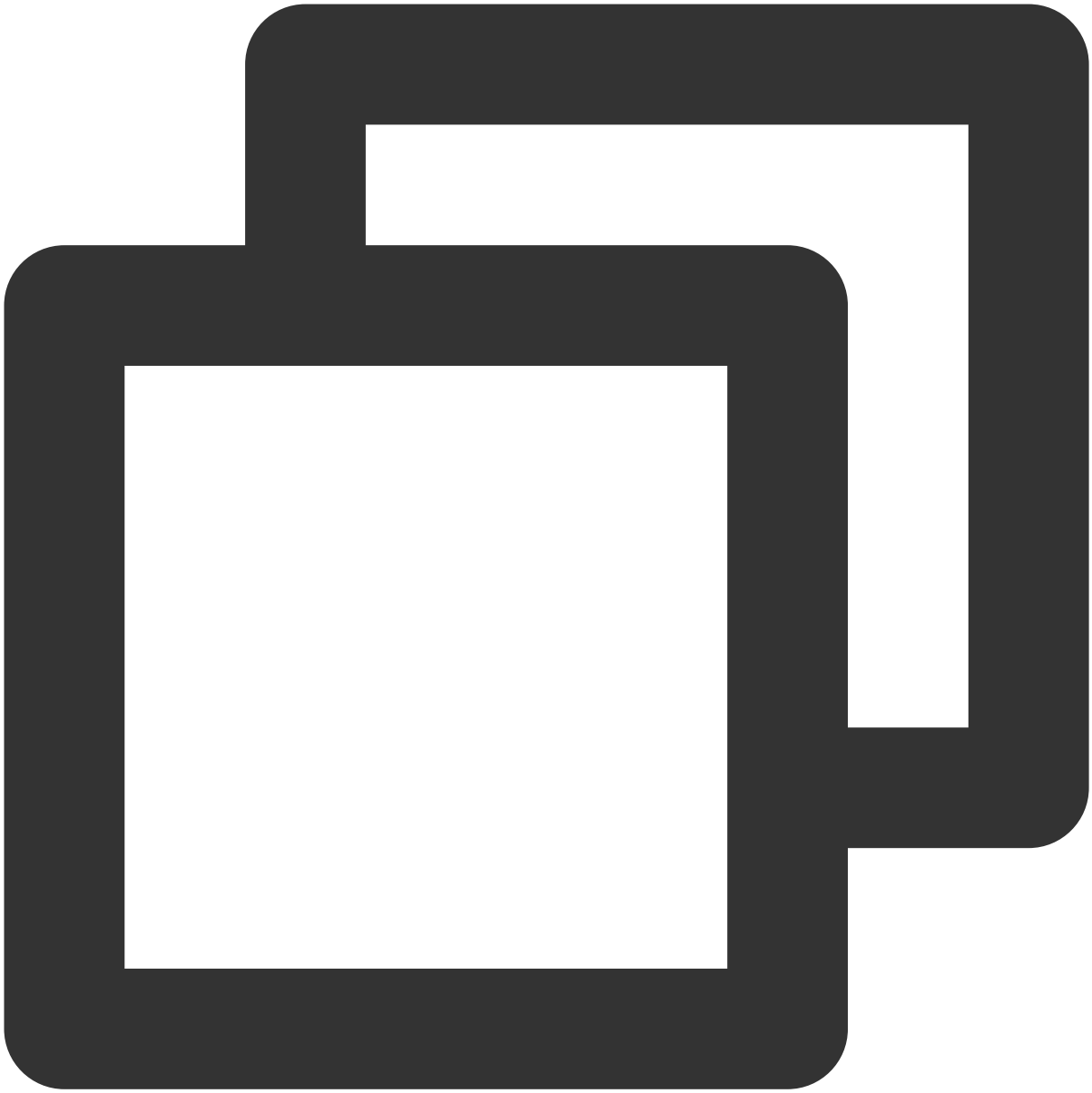
Why can't a sub-account access certain Tencent Cloud products after it has been authorized with the read-only policy (ReadOnlyAccess)?

The read-only policy (ReadOnlyAccess) only covers read APIs of Tencent Cloud products where the authorization granularity is operation level or resource level. If you access service-level products or the write APIs of operation-

level/resource-level products, the prompt for no access will be displayed. For the authorization granularity of Tencent Cloud products, please see CAM-Enabled Products.

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

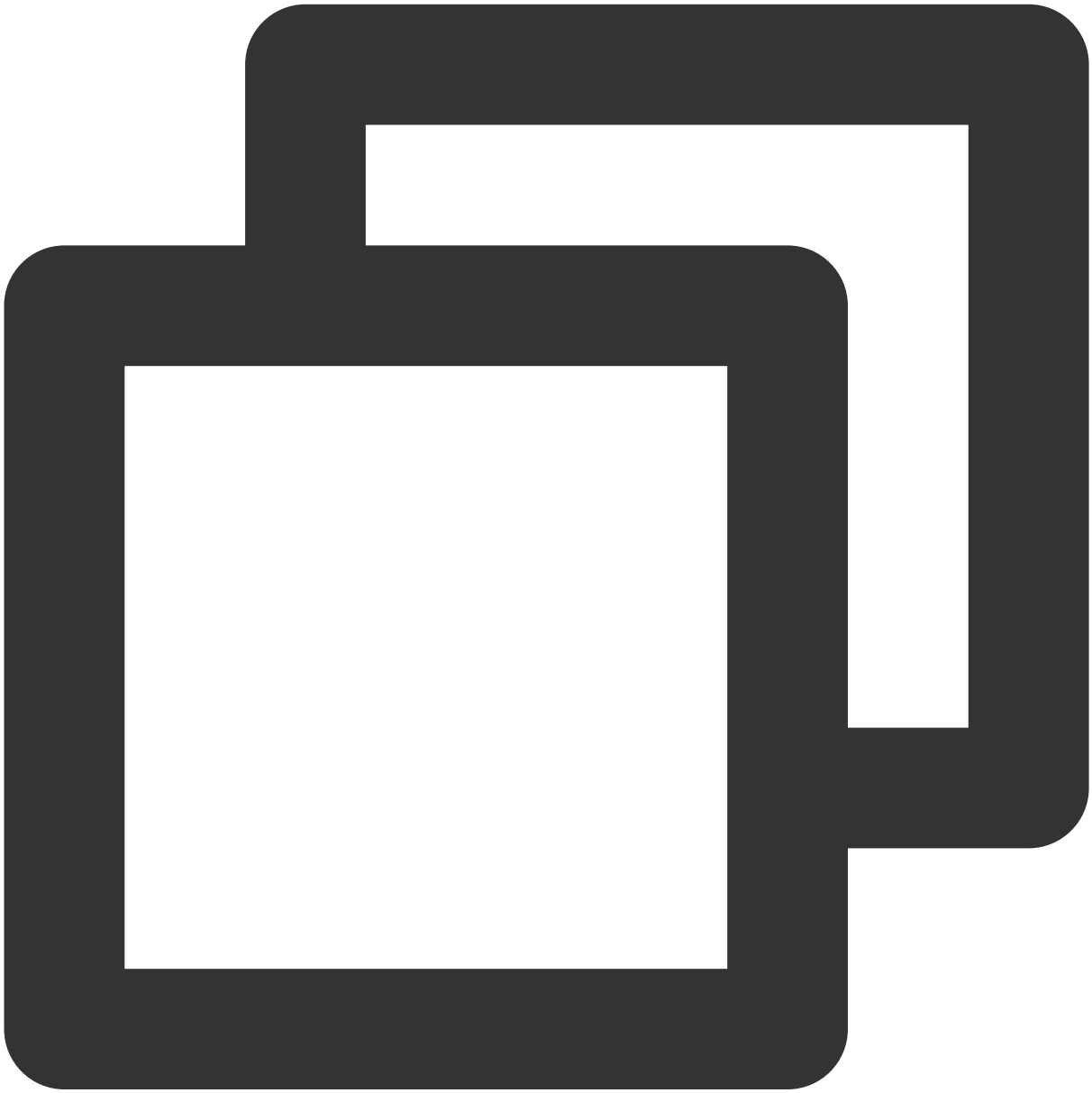
The following example describes how to allow a sub-account to view only part of the resources:
The enterprise account `CompanyExample` (ownerUin: 12345678) has a sub-account `Developer`. `CompanyExample` wants to allow the sub-account to view only part of its resources in the console.
For example, to allow the sub-account to view in the console two CVM instances `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 grant the sub-account a wider permission, such as full access. To grant the sub-account full access to CVM instances in the Guangzhou region, create the following policy:



```
{
  "version": "2.0",
  "statement": [
      {
```

```
            "action": [
                "cvm:*"
                ],
            "resource": "qcs::cvm:gz::*",
            "effect": "allow"
        }
    ]
}
```

2. Associate the policy with the sub-account. For more information on authorization, please see Authorization Management.

The products that **support** read-only permission at the resource level include CVM, TencentDB for MySQL, and TKE. Other products do not support granting read-only permission of specific resources. A sub-account either has the permission to view all the resources or has no permission to view any resources.

Which Tencent Cloud services support limiting access via IPs?

Service	Limiting Access via IP
CPM	✔
TKE - CI	✔
TKE - Cluster	✔
CLB	✔
COS	✔
Dayu Anti-DDoS - Anti-DDoS Advanced	✔

Key

Last updated：2024-01-23 18:03:29

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 is the access key. For more information on how to view the root account API key, please see Root Account Access Key. For more information on how to view the sub-account API Key, please see Access Key.

How do I authorize a sub-account key?

The sub-account key is consistent with the permissions of the sub-account. You only need to grant the sub-account permissions, and the sub-account key will have the same permissions. For more information on sub-account permission settings, please see “Setting Sub-user Permission”.

Role

Last updated：2024-01-23 18:03:29

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.
In addition, if you have used a service before it supports service-linked roles, a role will be automatically created under your account after we notify you of this via email or other notification channels.

Was there a change in the policy associated with the service role?

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 the role?

You can go to Roles in the CAM console, click the name of the desired role to go to the role details page, and query in the **Role Info** area.

How many types of CAM roles are there?

There are three types of CAM roles based on different role entities:
Tencent Cloud service: Authorize a Tencent Cloud service to use your cloud resources with the role.
Tencent Cloud account: Authorize the root account or other root accounts to use your cloud resources with the role.
Identity provider: Authorize an external user identity (such as enterprise user pool) to use your cloud resources.

Others

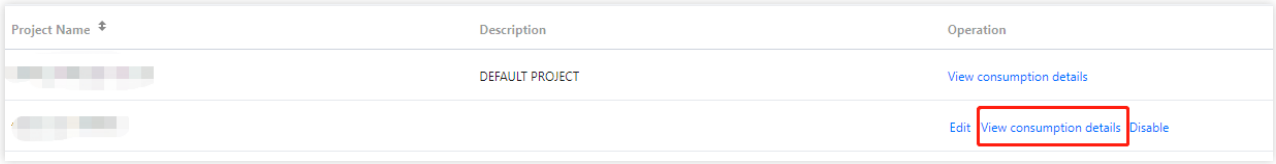
Last updated：2024-01-23 18:03:29

How do I manage project resource permissions in a refined manner?

You can implement refined permissions management as instructed in Authorization by Tag.

Can I view the resources consumed for a project?

No. However, you can view the consumption details in the CAM console.



You can view all the resources used under the current account on the Overview page in the console.

What should I do if the message “Failed to verify the SAML with a certificate” is prompted when I log in to Tencent Cloud as a sub-user?

You can troubleshoot as follows:

1. Use the SAML tool to verify whether the SAML response format is correct.
2. Check whether the required parameters (especially role-related parameters) are provided in the SAML response in correct format.
3. Check whether the parameters in the previous step have been used to create an IdP and a role as instructed in Accessing Tencent Cloud Console as SAML 2.0 Federated Users.

If the problem persists, submit a ticket for assistance.