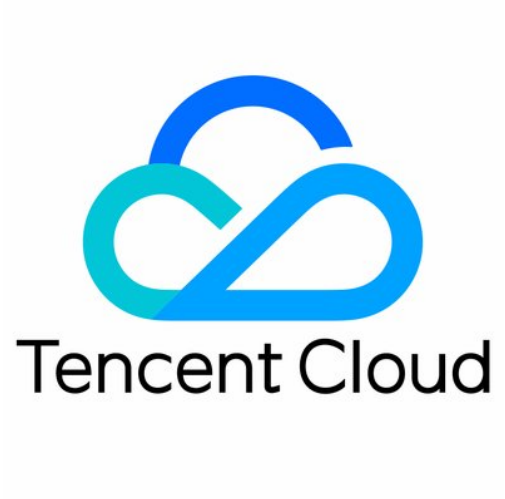
Cloud Access Management

Best Practice

Product Documentation



Contents

Best Practice
Multi-Identity Personnel Permission Management

Last updated : 2021-08-04 17:44:10

Overview

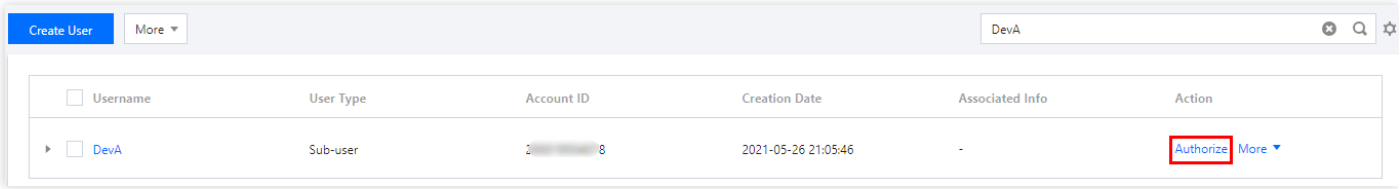
If your company has management personnel with different identities, you can use CAM to divide permissions and grant different permissions to different people to facilitate management and control. This document uses a typical case to describe how to manage the permissions of different identities through sub-accounts.

Suppose that:

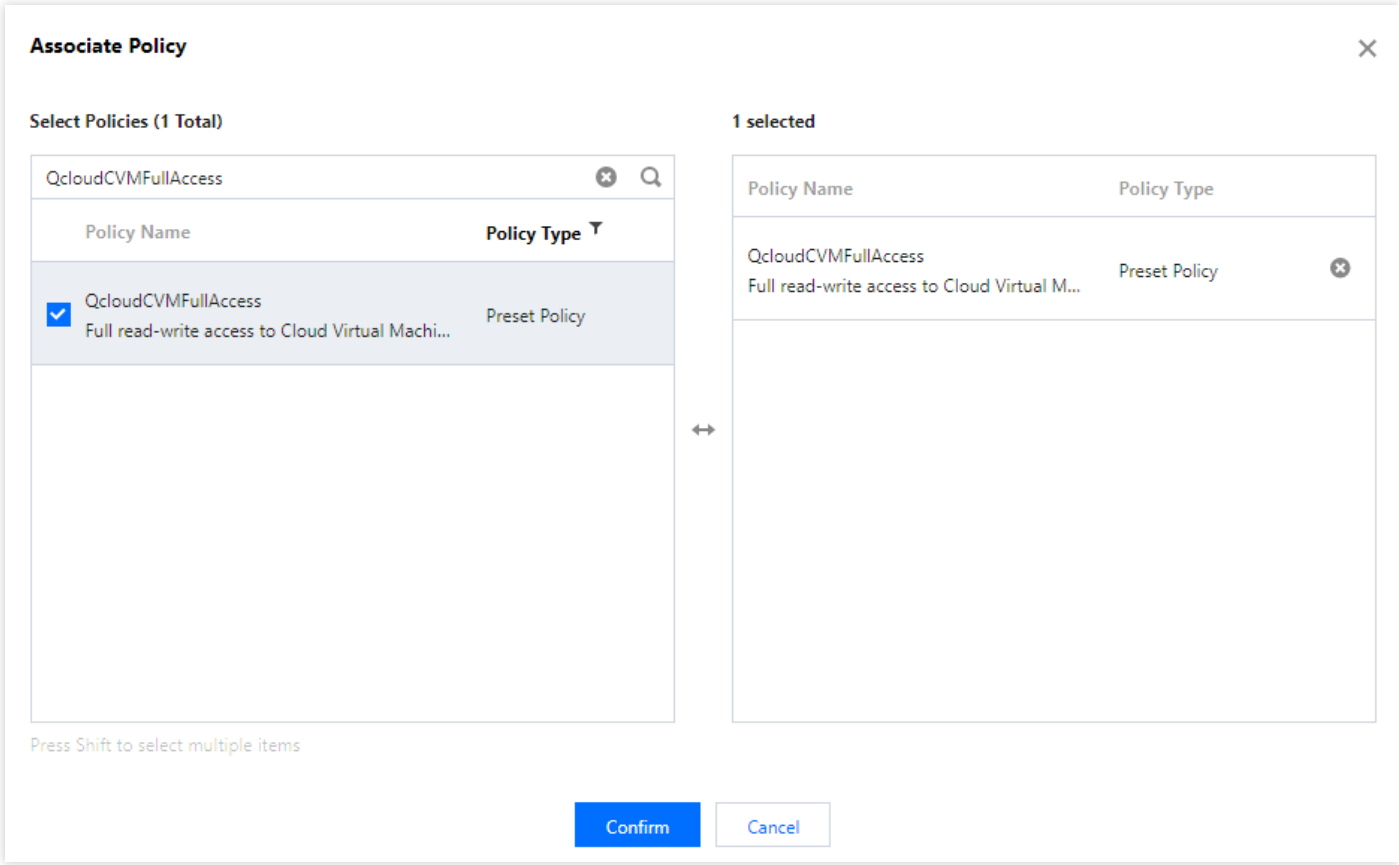
- The company account `CompanyExample` has two OPS engineers `DevA` and `DevB`.
- The OPS engineer `DevA` is responsible for server OPS and has all operation permissions of CVM instances under the company account `CompanyExample`.
- The OPS engineer `DevB` is responsible for TencentDB for MySQL OPS and has all operation permissions of TencentDB for MySQL instances under the company account `CompanyExample`.

Directions

1. Log in to the CAM console with the company account `CompanyExample`.
2. Create two sub-accounts with usernames of `DevA` and `DevB` through custom sub-user creation.
3. On the **User List** page, find the just created sub-user `DevA` and click **Authorize** in the **Operation** column on the right as shown below:



4. In the **Associate Policy** window that pops up, search for and select `QcloudCVMFullAccess` and click **OK** as shown below:



5. Associate the `QcloudCDBFullAccess` policy with the sub-account `DevB` as instructed in steps 2 and 3.
6. After the authorization is successful, the sub-account `DevA` has all the operation permissions of CVM instances, while the sub-account `DevB` has all the operation permissions of TencentDB for MySQL instances.

> Note :
> If you need to configure a CAM user as another role, you can follow the above process and search for and select the corresponding permissions policy name in steps 2 and 3. For specific permissions, please see System Permissions

System Permissions

Owner	Policy Name	Description
Admin	AdministratorAccess	This policy allows you to manage all users and their permissions, related

		financial info, and cloud service assets under this account.
Financial admin	QCloudFinanceFullAccess	This policy allows you to manage related financial information under the account, such as payment and invoicing.
Database admin	QcloudCynosDBFullAccess	Full access to TDSQL-C
	QcloudMariaDBFullAccess	Full access to TencentDB for MariaDB
	QcloudSQLServerFullAccess	Full access to TencentDB for SQL Server
	QcloudCDWPGFullAccess	Full access to TencentDB for PostgreSQL
Network admin	QcloudCLBFullAccess	Full access to CLB
	QcloudVPCFullAccess	Full access to VPC
	QcloudDCFullAccess	Full access to Direct Connect
Monitoring admin	QcloudMonitorFullAccess	Full access to Cloud Monitor, including the permission to view user groups
	QcloudCATFullAccess	Full access to CAT

Authorizing Certain Operations by Tag

Last updated : 2021-08-05 10:04:03

Overview

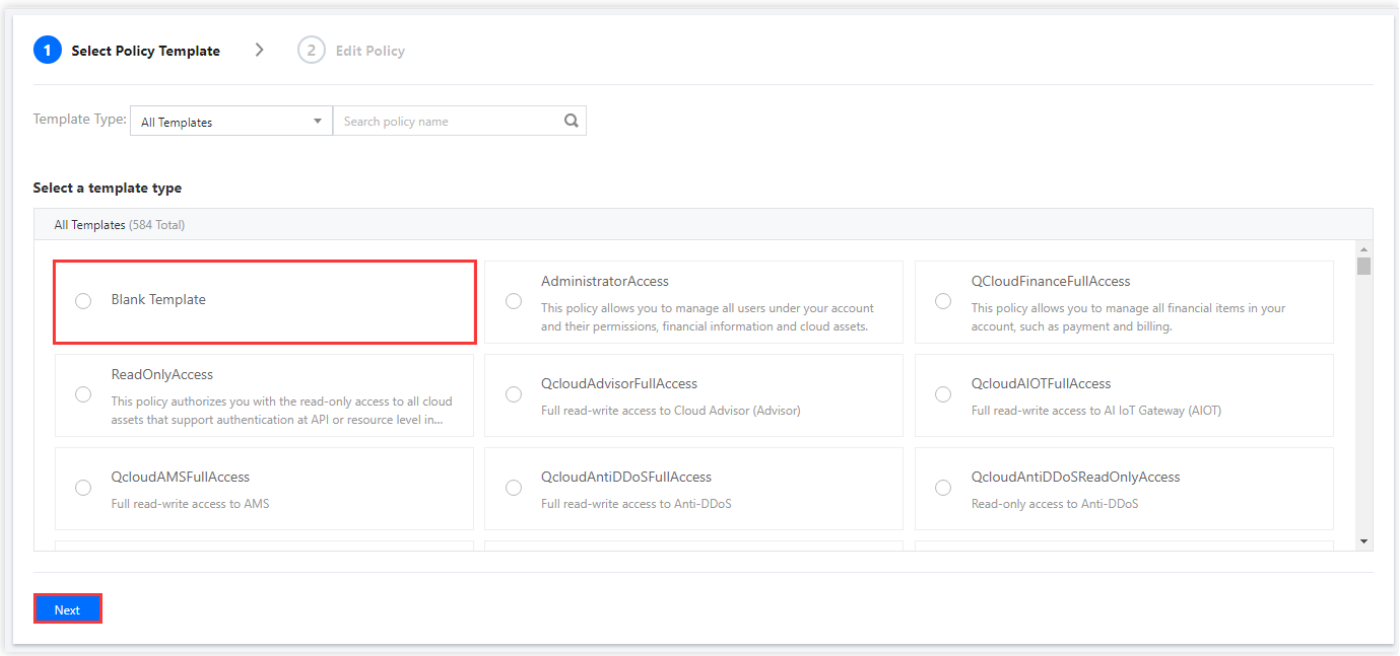
If you have purchased multiple types of Tencent Cloud resources which are grouped and managed by tag, you can grant employees of different teams permissions to use corresponding APIs by tag on an as-needed basis. This document uses a typical case to describe how to grant sub-accounts certain operation permissions of resources through tags.

Suppose that:

- The company account `CompanyExample` has a sub-account `DevA`.
- The company account `CompanyExample` has a tag key-value pair `test1&amp;test1`.
- The company account `CompanyExample` wants to grant the sub-account `DevA` the permission to restart CVM instances (cvm:RebootInstances) under the tag `test1&amp;test1`.

Directions

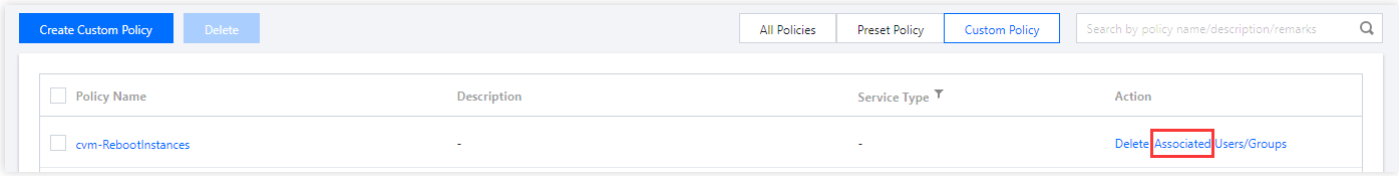
1. Log in to the CAM console with the company account `CompanyExample`.
2. On the **Policy** page, click **Create Policy** > **Create by Policy Syntax**.
3. Select **Blank Template** under **Select a template type** and click **Next** to enter the **Edit Policy** page



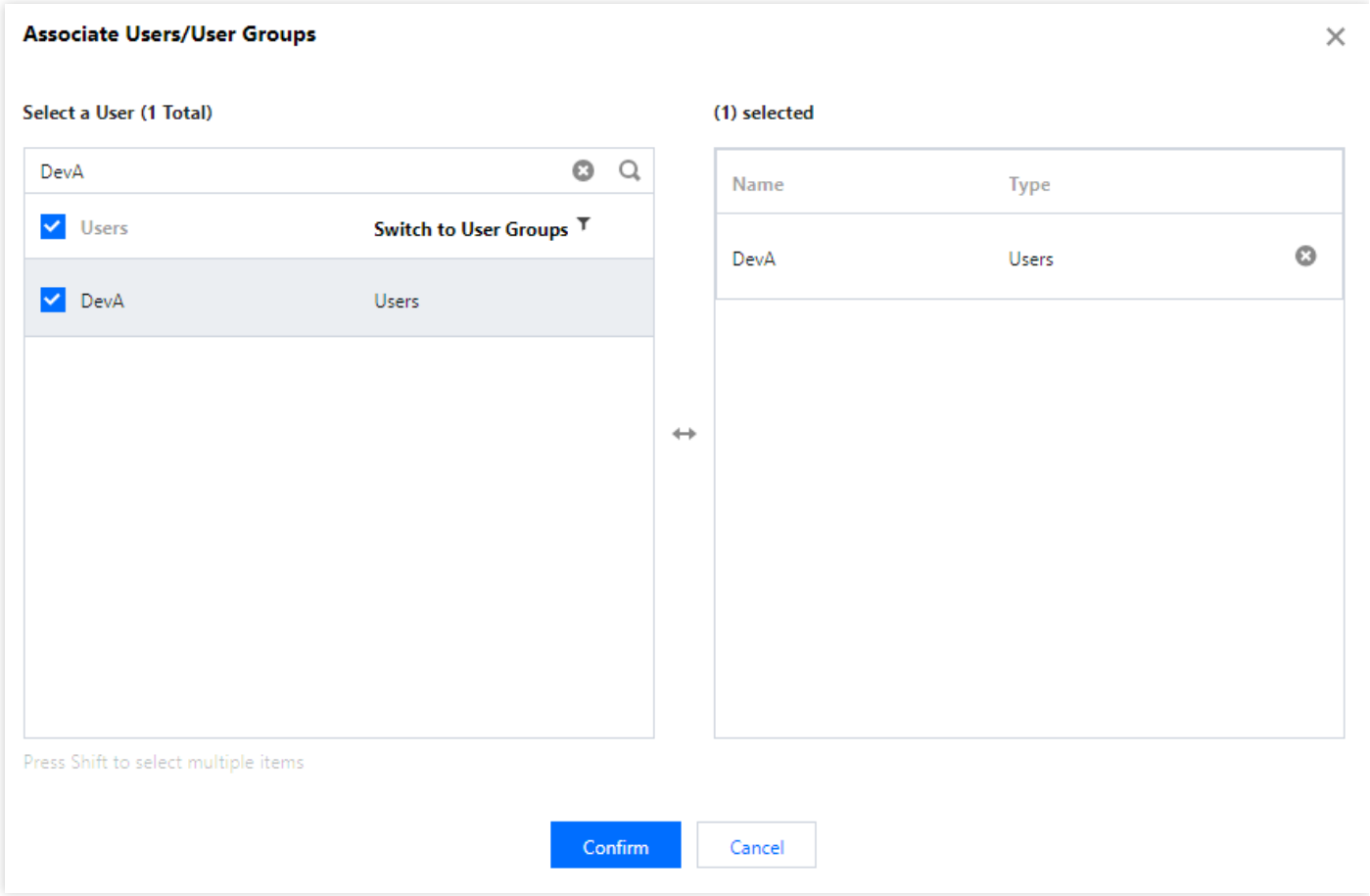
4. On the **Edit Policy** page, fill out the following form:
   - Policy Name: the default value is `policygen-current date` . We recommend you define a unique and meaningful policy name, such as `cvm-RebootInstances` .
   - Description: write a description, which is optional.
   - Policy Content: copy and paste the following content. Here, `cvm:RebootInstances` is the name of the API that needs to be authorized, and `test1&amp;test1` is the tag key-value pair that needs to be authorized.

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

5. Click **Complete** to create the policy, which will be displayed on the **Policy List** page.
6. Find the just created policy in the Policy List and click **Associate** in the **Operation** column on the right.



7. In the **Associate with User/User Group** window that pops up, search for and select the sub-account `DevA` and click **OK** to complete the authorization.
   The sub-account `DevA` will have the permission to restart CVM instances under the `test1&amp;test1` tag.



Related Documents

If you want to know how to associate resources with tags, please see Managing Tags.
If you want to know how to grant all operation permissions of the resources under a tag, please see

Authorizing Different Sub-accounts Separate Permissions to Manage Tencent Cloud Resources.