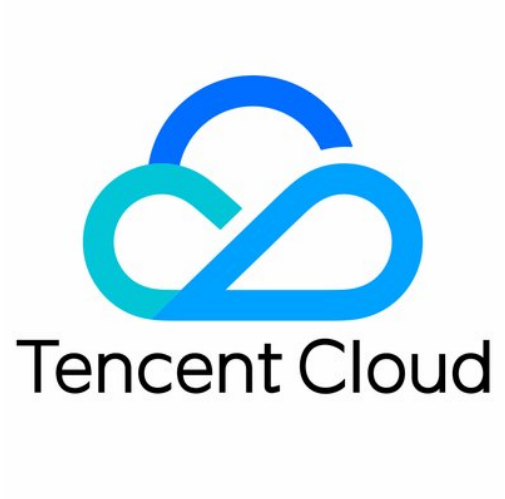
Cloud Access Management

Best Practice

Product Introduction



Best Practice

Last updated：2018-09-14 10:43:36

Basic Principles

1. Enable MFA protection

We suggest that you bind all the accounts with MFA: Enable login protection and sensitive operation protection for the root account, and sensitive operation protection for all the sub-accounts. It is strongly recommended to perform MFA secondary validation for the accounts that support login with email or WeChat accounts.

2. Access Tencent Cloud using sub-account

Try not to access Tencent Cloud using the identity credential of root account, or even share the credential with other users. Generally, you should create a sub-account for each user accessing Tencent Cloud, and grant the management permission to this sub-account.

3. Grant permissions to sub-account using group

Define groups based on different responsibilities, and assign management permission for each group. Assign users to the corresponding group. In this case, when you modify the permissions of a group, the permissions of the users in this group will change accordingly. In addition, when the organizational structure changes, you only need to update the relationship between new users and the group.

4. Principle of minimum permission

The principle of minimum permission is a standard security principle. Only minimum permissions, instead of more irrelevant permissions, required for task execution are granted. For example, if a user only uses CDN service, you don't need to grant resource access permissions (such as COS read/write permissions) of other services to this user.

5. Users, permissions and resources are managed by different sub-accounts respectively

It is recommended that a sub-account does not manages users, permissions and resources simultaneously. Different sub-accounts should be used to manage users, account management permissions or other cloud resources respectively.

6. Change identity credential on a regular basis

We recommend you or CAM users to change login password or cloud API key periodically. This can limit the length of time during which the identity credential is affected due to its disclosure.

7. Delete unnecessary certificates and permissions

Delete the certificates and permissions that users don't need anymore. Minimize the security risks caused by the disclosure of access credential.

8. Use policy conditions to enhance security

Enhance the security by defining policies more specifically and limiting the scenarios where policies become effective. For example, users are only allowed to perform certain operations on a specified CVM for a specified period of time.