Secrets Manager

Operation Guide

Product Documentation

Contents

Operation Guide
Encrypting a Secret

Last updated : 2021-08-18 14:18:51

This document describes how to activate Key Management Service (KMS) in Secrets Manager (SSM) and authorize SSM. It also guides you on how to use KMS to encrypt secrets in SSM.

Background

Secret management is important for the OPS security of an enterprise IT system. You can use SSM to host secrets of all types, including access keys, API keys, private keys, account passwords, and much more. SSM uses keys hosted in Tencent Cloud KMS to encrypt and protect secrets, ensuring secret security on the server. With a more secure and convenient SSM, you no longer need to build and maintain infrastructure for secret management.

> Note :
> When SSM uses KMS hosted keys for encryption, KMS fees might be incurred. For more information, please see Billing Overview.

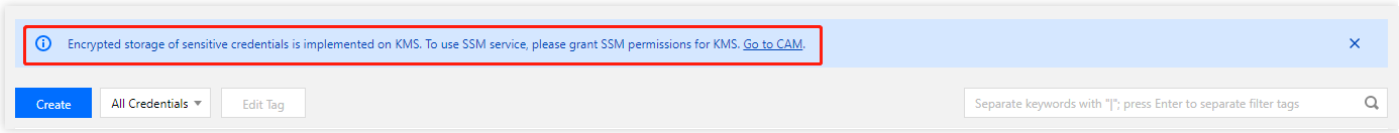
Directions

Step 1: Activate KMS and authorize SSM

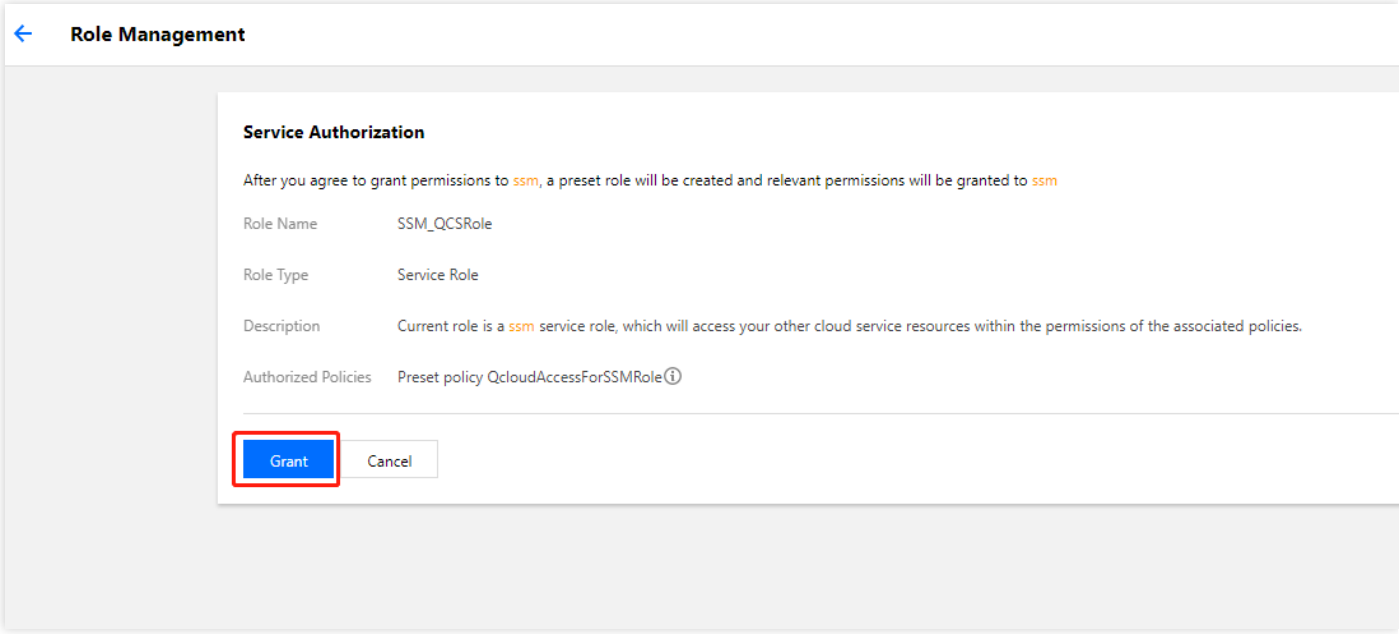
- SSM uses KMS to store encrypted sensitive secrets. Therefore, before using SSM, ensure that KMS is activated.
- To ensure that you can use SSM normally, please grant service role permissions to SSM in KMS. You can go to CAM to authorize SSM.

To activate KMS and authorize SSM, you can perform the following steps:

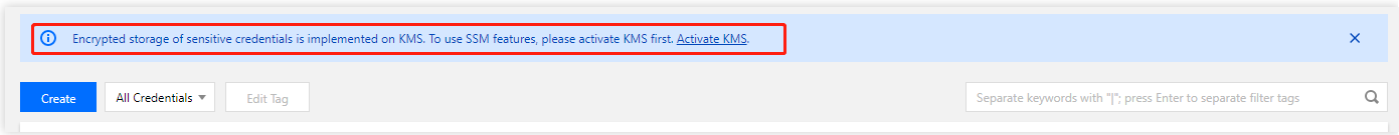
1. Log in to the SSM console and click CAM in the instructions at the top of the page.



2. On the **Service Authorization** page, click **Grant**.



3. After service role authorization, click KMS in the instructions at the top of the page.



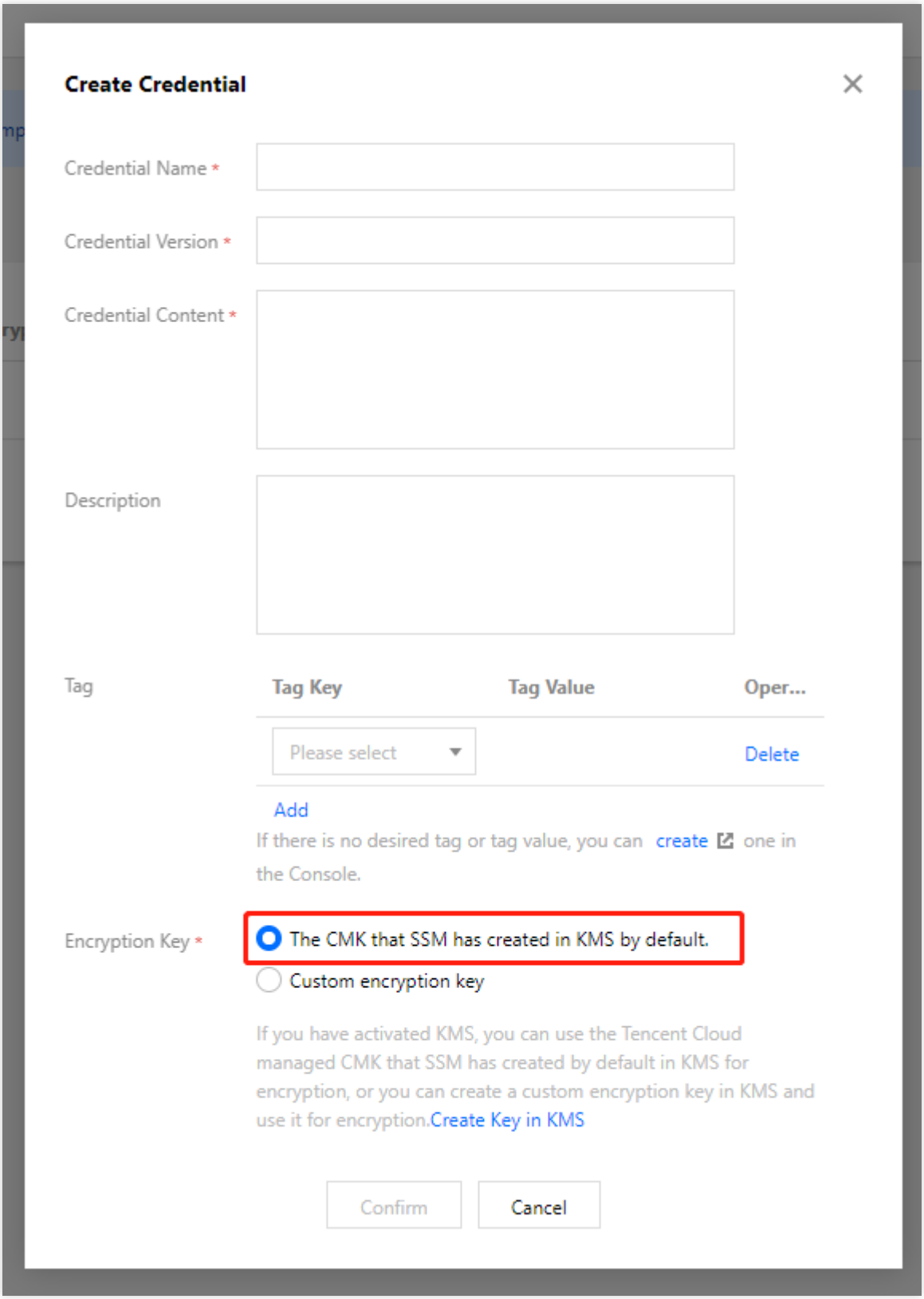
4. On the KMS activation page, click **Activate Now**.

Step 2: Select a key for secret encryption

As the core resources of KMS, CMKs are protected by hardware security modules certified by third parties. CMK contains metadata information such as key ID, creation date, description, and key status.

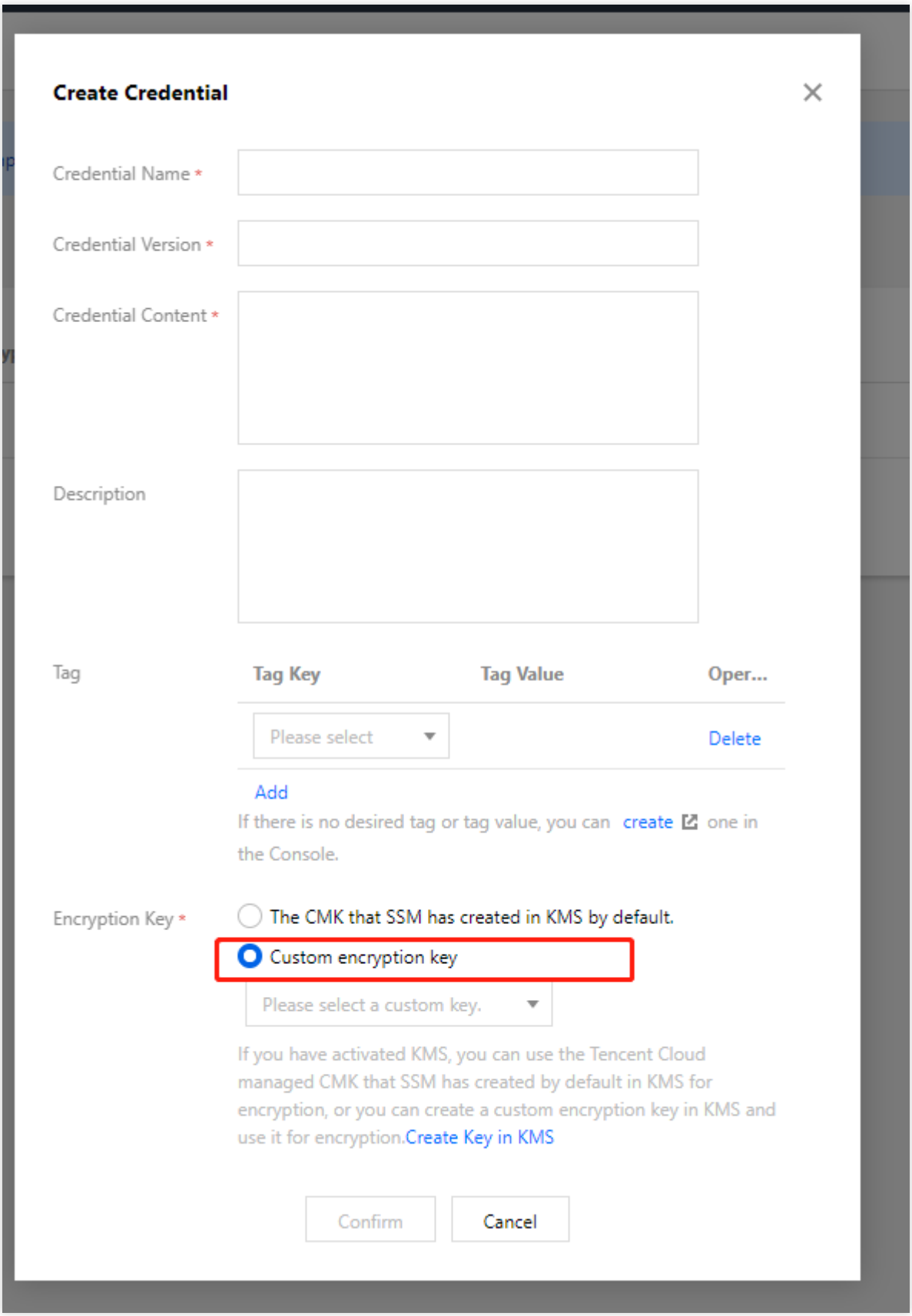
When using SSM to create secrets, you will be provided with two types of encryption keys. Select a type as needed.

- After KMS is activated, KMS will create a Tencent Cloud managed CMK for SSM by default. The default key cannot be deleted or disabled. You can use the default key as the encryption key.



- You can also go to the KMS console to create a key on your own and define the key policies and usage. KMS enables users to choose keys as needed. You can either **create keys in KMS** or **import external keys** (BYOK). For more information, please see Creating Keys and Importing

External Keys for KMS.



Log Audit

Last updated : 2020-11-16 14:14:41

Overview

SSM combines with CloudAudit to perform supervision, compliance checks, operational reviews, and risk reviews on your Tencent Cloud accounts. All management operations and usage of the secrets can be recorded.

Directions

1. Log in to the CloudAudit console and click **Event History** in the left sidebar. You can view the operation records of the Tencent Cloud account for up to the last 30 days.
2. Click the **Expand** icon on the left of the target event to view the event details.
   You can view the following content:

- **Operation record list**: includes the event time, username, event name, resource type, and resource name.
- **Operation record details**: includes the access key, region, error code, event ID, event name, event source, event time, request ID, resource IP address, and username.

Access Control Overview

Last updated : 2020-11-16 14:15:03

If you do not need to manage the access permissions to SSM resources for sub-accounts, you can skip this chapter. Doing so will not affect your understanding and use of other documentation.
If you use multiple services such as SSM, VPC, CVM, and databases, and these services are managed by different users with a shared cloud account key, there would be a high risk of leakage. Besides, since the access permissions of other users cannot be limited, security risks caused by misoperations may occur.
CAM is used to manage the resource access permissions of a Tencent Cloud account. You can manage the resource operation permissions for sub-accounts using CAM identity management and policy management. For example, if your root account has a secret that you want it to be used only by sub-account A and not by sub-account B, you can configure a policy in CAM to manage the sub-account permissions.

Basic CAM Concepts

The root account can associate policies to sub-accounts to implement permissions. The policies support multiple dimensions, such as API, resource, user, user group, allowing, forbidding, and condition.

- **Account**
  - **Root account**: the owner of Tencent Cloud resources and the fundamental entity for resource usage, usage calculation, and billing. It can be used to log in to Tencent Cloud services.
  - **Sub-account**: an account created by the root account. It has a specific ID and identity credential that can be used to log in to the Tencent Cloud console. A root account can create multiple sub-accounts (users). By default, a sub-account does not own any resources and must be authorized by its root account.
  - **Identity credential**: includes login credentials and access certificates. Login credential refers to a user’s login name and password. Access certificate refers to Cloud API keys (SecretId and SecretKey).
- **Resource and permission**
  - **Resource**: an object that is operated in Tencent Cloud Services, such as an SSM secret, a CVM instance, a COS bucket, or a VPC instance.

- **Permission**: an authorization that allows or forbids users to perform certain operations. By default, the root account has full access to all resources under the account, while a sub-account does not have access to any resources under its root account.
- **Policy**: syntax rule that defines and describes one or more permissions. The root account performs authorization by associating policies with users/user groups.

For more information, please see Tencent Cloud CAM.

Managing Sub-Accounts

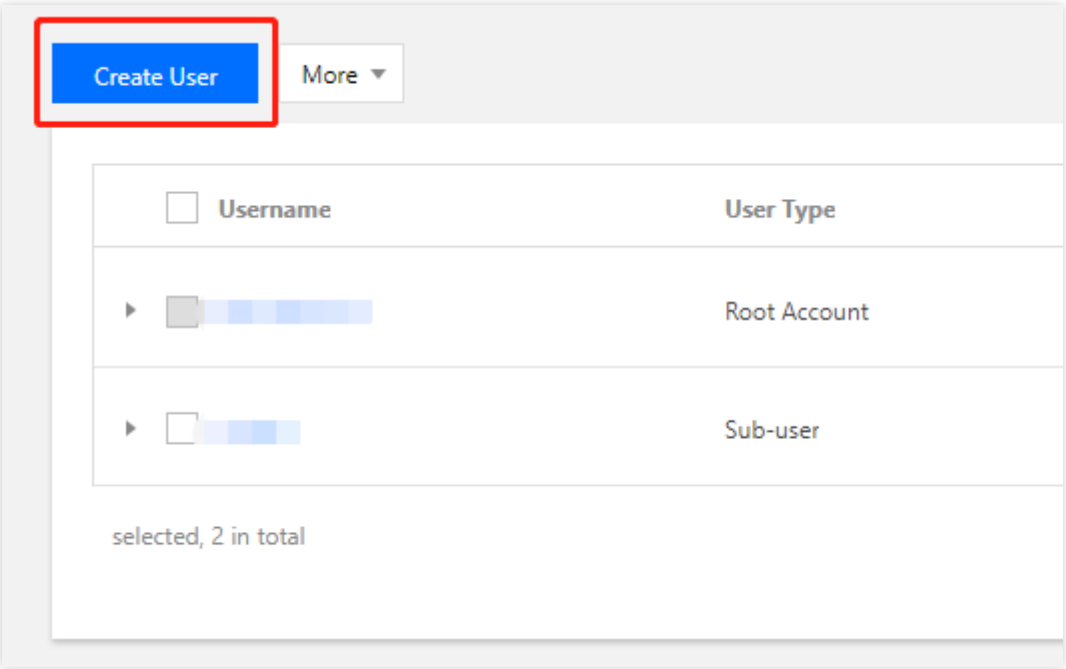
Last updated : 2020-11-16 14:15:58

Overview

This document shows you how to create a sub-account and grant permissions to it to manage SSM.

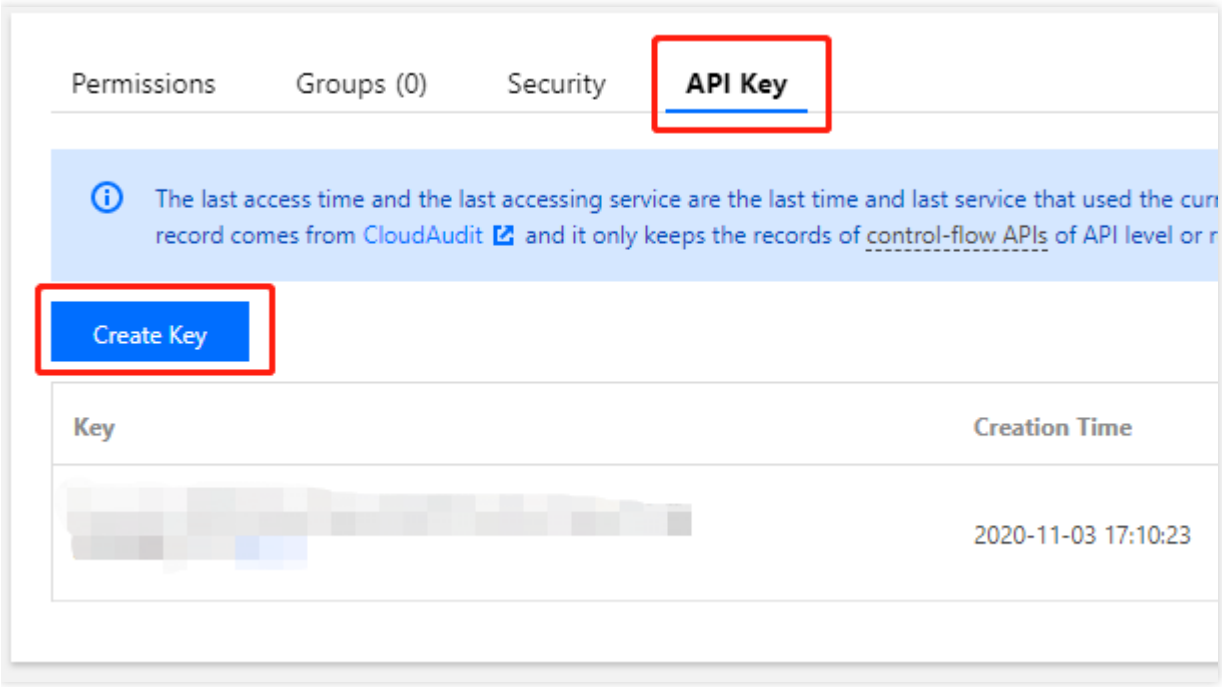
Directions

1. Create a sub-account. Log in to the Tencent Cloud CAM console using the root account. In the left sidebar, click **Users** -> **User List**. On the **User List** page, click **Create User** to create a sub-account.

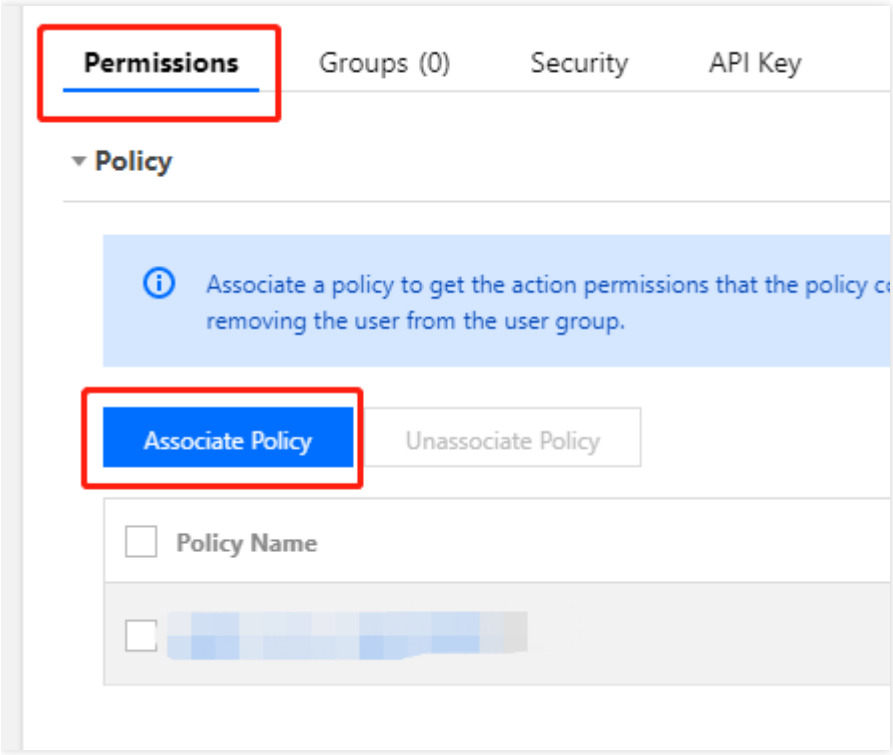


2. Create an API key. You can click the name of the sub-account to go to its **User Details** page. Click **API Key** -> **Create Key** to create SecretId and SecretKey. You can use this API key to access SSM.

> **Note :**
>
> If you do not need to manage SSM through APIs, you can authorize the sub-account directly.

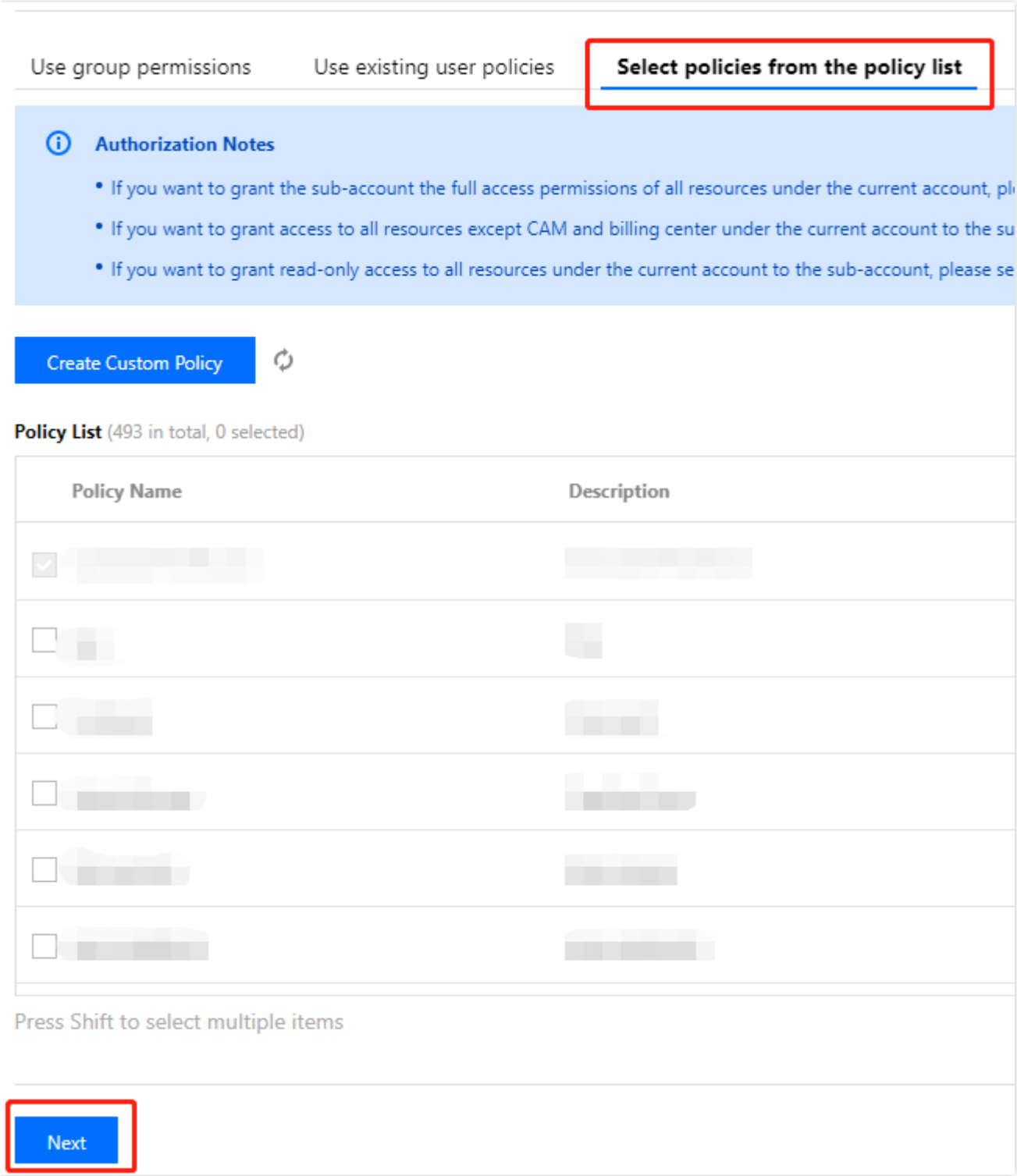


3. Authorize the sub-account. You can add the SSM policy to the newly created sub-account so that it can access SSM. On the **User Details** page of the sub-account, click **Permissions** > **Associate Policy** to go to the **Add Policy** page.



4. Add a policy. On the **Add Policy** page, click **Select policies from the policy list**, choose the appropriate SSM policy, and click **Next** > **Confirm**. In this way, you can grant permissions to the

sub-account to access SSM.



Creating an Access Control Policy

Last updated : 2020-11-16 14:16:27

Authorizable Resource Types

Resource-level permission refers to the capability to specify resources that an account can perform operations on. Some SSM APIs support operations on secrets using resource-level permissions. This can control when a user can perform operations and whether the user can use specific resources. For example, if you allow a user to have access to secrets in the Guangzhou region, the authorizable resource type in CAM is as follows:

```
qcs::ssm:ap-guangzhou:uin/${uin}:*
qcs::ssm:ap-guangzhou::*
```

If you authorize an API to access all secrets created by a certain UIN, the resource type is as follows:

```
qcs::ssm:$region:uin/$uin:secret/creatorUin/*
```

If you authorize an API to access a certain secret, the resource type is as follows:

```
qcs::ssm:$region:uin/$uin:secret/creatorUin/$creatorUin/$secretName
```

Where,

- `$region` : region
- `$uin` : root account ID
- `$creatorUin` : account ID of the creator of the resource
- `$secretName` : name of the secret that requires configuration

Resource-level Authorization APIs

The resource paths of the `DeleteSecretVersion` , `UpdateDescription` , `RestoreSecret` , `EnableSecret` , `PutSecretValue` , `DescribeSecret` , `UpdateSecret` , `DeleteSecret` , `GetSecretValue` , `DisableSecret` , and `ListSecretVersionIds` APIs are as follows:

```
qcs::ssm:$region:uin/$uin:secret/*
qcs::ssm:$region:uin/$uin:secret/creatorUin/*
qcs::ssm:$region:uin/$uin:secret/creatorUin/$creatorUin/$secretName
```

API-level Authorization List

API	Description
CreateSecret	Creates a secret
GetRegions	Obtains the list of available regions to be displayed on the console
GetServiceStatus	Obtains the service status, which can be used to determine whether the service is activated
ListSecrets	Obtains the information list of all secrets