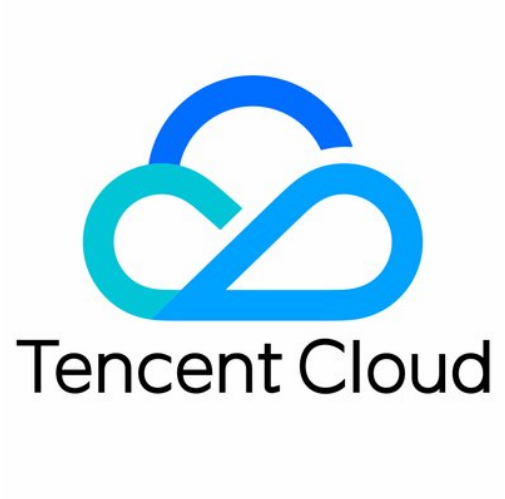
Secrets Manager

Getting Started

Product Documentation



Getting Started

Last updated：2021-09-28 10:13:20

You can use Secrets Manager (SSM) to centrally retrieve, manage, and store different types of secrets, including encrypted database credentials, API keys, other keys, and sensitive configuration. SSM enables you to effectively avoid plaintext leakage caused by hardcoding and business risks caused by out-of-control permissions.

Step 1. Register an account

Sign up for a Tencent Cloud account and complete the identity verification. For more information, please see Signing up for a Tencent Cloud Account.

Step 2. Purchase SSM service

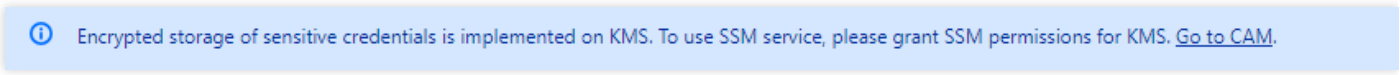
Go to the SSM Purchase Page, read and select the relevant billing description, and then click **Activate Now**.

Step 3. Activate KMS and authorize SSM

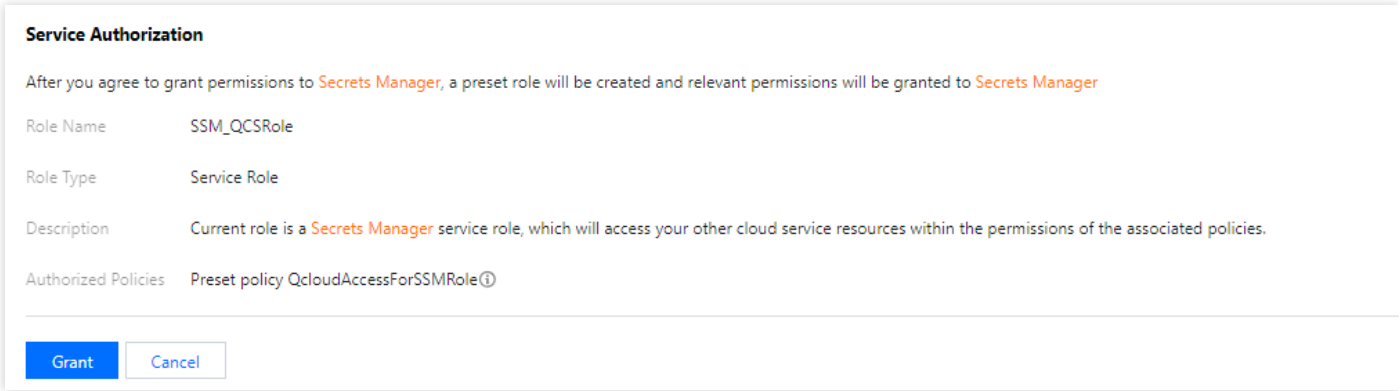
- SSM uses KMS to store encrypted sensitive secrets. Therefore, before using SSM, ensure that KMS is activated.
- To ensure that you can use SSM normally, please grant service role permissions to SSM in KMS. You can go to CAM to authorize SSM.

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. Click **KMS** of the tip at the top of the console.
4. On the KMS activation page, click **Activate Now**.

Step 4. Mange secrets in the console

After activation, you can manage secrets by enabling and saving to deleting in the SSM console, SDK or the command line interface (CLI).