

# Secrets Manager Operation Guide Product Documentation





#### Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

#### STencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

#### Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

### Contents

**Operation Guide Custom Secret Creating Secrets** Editing a Secret Managing Multiple Secret Versions Deleting a Secret Database Credential Overview Instructions Creating a Database Credential Editing a Database Credential Enabling a Database Credential Deleting a Database Credential Tag Editing a Tag Examples of Management via Tags CVM SSH Key Secret Creating an SSH Key Secret Deleting an SSH Key Secret **Download Private Key Binding Management** Log Audit Access Control Overview Managing Sub-Accounts Creating an Access Control Policy

## Operation Guide Custom Secret Creating Secrets

Last updated : 2024-01-02 15:07:14

### Scenarios

You can create a secret in the SSM console. After creation, you can manage the secret by enabling, disabling, editing, and scheduling deletion.

### Directions

- 1. Log in to the SSM Console and click Custom Secret on the left sidebar.
- 2. In the upper left corner, choose a region and click **Create** to create a secret.
- 3. Enter the configuration in the pop-up Create Credential window and then click Confirm to return to the

Credential List. The newly created secret will be at the top of the credential list.

🔗 Tencent Cloud

Create Credential			>
Credential Name *			
Credential Version *			
Credential Content *			
Description			
Tag	Tag Key	Tag Value	Oper
	Please select 🔹		Delete
Encryption Key *	Add If there is no desired tag of the Console. The CMK that SSM ha Custom encryption ke If you have activated KMS managed CMK that SSM h	or tag value, you can creat s created in KMS by defaul y , you can use the Tencent ( has created by default in Ki	te 🗹 one in It. Cloud MS for
	use it for encryption.Creat	e Key in KMS	ey in Kws and
	Confirm	Cancel	

#### Field description:

**Credential Name**: its length can be 1-128 bytes, containing letters, digits, hyphens (-), and underscores (\_). It must start with a letter or digit.

Credential Version: required.



#### Credential Content: required.

Description: optional.

Tag: optional.

#### **Encryption Key**:

Use the default CMK that SSM has created in KMS.

Use a custom encryption key.

#### Note:

If you are using SSM, you have activated KMS. You can create an encryption key in either of the following ways: Use the default Tencent Cloud managed CMK created in the KMS console as the encryption key, and use the envelope encryption method for encrypted storage.

Use a custom key created in the KMS console as the encryption key for encrypted storage.

## Editing a Secret

Last updated : 2024-01-02 15:07:13

### Overview

You can log in to the Tencent Cloud SSM console to view and edit the secret information list, secret name, status, region, and other information.

## Editing a Secret

1. Log in to the SSM console and click **Credential List** in the left sidebar. You can switch between regions on the upper left corner of the page to view and edit secrets in other regions.

Credential List	😴 Guangzhou 🔻						
	Create All Credentials <b>*</b> Edit						
	Credential Name						
	Total items: 1						

2. In the search box on the right, enter the full or partial name of the secret to search for the target secret.

Separate keywords with " "; press Enter to separate filter tags Q						Q,
Key Status		Opera	tion			
		Schedule Deletion   Edit Tag				
	20 🔻 / page		1	/ 1 page		

3. Click the name of the secret to view the detailed information about the secret. You can enable or disable the key of the secret.

Credential Na	me Encryption Key	Tag (key:value)	Creation Time 🗘	Key Status	Operation
fe-test		bfzhu1:bfzhu-test1	2020-11-03 16:41:35		Schedule Deletion   Edit Tag
Total items: 1					20 ▼ / page H 4 1 / 1 page ▶ H

4. Go to the secret details page to view information about the secret, such as the credential name, status, description, and version. You can also update, delete, and manage secret versions, and perform other operations.



Basic Informat	ion		
Credential Name	fe-test		
Status Toggle			
Status	Normal		
Region	Guangzhou		
Creation Time	2020-11-03 16:41:35		
Creator	The second se		
Description	fe-test-desc Modify		
Credential Mar	nagement		
	-		+ Add
Version Numbe	r	Operation	
1.0.0		View Change Delete	

## Managing Multiple Secret Versions

Last updated : 2024-01-02 15:07:13

### Overview

SSM allows you to manage multiple versions of secrets. You can leverage this feature to rotate secrets at the application layer in beta tests.

### Directions

1. Log in to the SSM console and click **Credential List** in the left sidebar. You can switch between regions on the upper left corner of the page to find the secret to which you want to add a version. You can click the name of the secret to go to the **Basic Information** page.

fe-test	bfzhu1:bfzhu-test1	2020-11-03 16:41:35		Schedule Deletion   Edit Tag
---------	--------------------	---------------------	--	------------------------------

2. In the **Credential Management** module, click **Add** to go to the **Add Credential Information** page.

Credential Management		+ Add
Version Number	Operation	
1.0.0	View Change Delete	



3. On the Add Credential Information page, enter the credential version and credential content, and then click Add.

Add Credential Inf	ormation	×
Credential Version *		
Credential Content *		
	Add Cancel	

4. If you want to delete an added secret, you can click **Delete** in the **Operation** column to the right of the unwanted version, and then click **Delete** to confirm the deletion.

Credential Management	+ Add
Version Number	Operation
1.0.0	View Change Delete

Note :

Each secret can have a maximum of 10 versions at the same time.

## **Deleting a Secret**

Last updated : 2024-01-02 15:07:13

### Note

SSM provides the schedule deletion feature against accidental secret deletions. Each deletion has **a mandatory waiting period of 0-30 days**, that is, there will be 0-30 days to wait before the deletion becomes permanent. Once deleted, a secret **cannot be restored**, and all of its content **cannot be called**.

### Directions

1. Log in to the SSM Console and click Secret List on the left sidebar. You can switch between regions in the upper left corner of the page to view secrets in other regions as needed.

2. Select the secret to be deleted on schedule in the **Secret List**. If the secret is enabled, you need to disable it first and then click **Schedule Deletion** in the **Operation** column.

Secret Name	Encryption Key	Tag (key:value)	Creation Time 🕈	Secret Status	Operation
		-			Schedule Deletion   Edit Tag

3. Set the number of schedule deletion days and then click **Confirm**. The secret will be deleted after the set number of days.



#### Note:

If the waiting period is set to "0", the secret will be deleted immediately.

4. The deletion of a secret can be canceled within the waiting period (1-30 days). You can click **Cancel Deletion** in the **Operation** column on the right. After the deletion is canceled, the secret key will be restored to the "enabled" status. You can disable, edit, delete, or perform other operations on the secret.

Secret Name	Encryption Key	Tag (key:value)	Creation Time 🕈	Secret Status	Operation
		-			Delete on 2021-10-14 15:02:47 Cancel Deletion

## Database Credential Overview

Last updated : 2024-01-02 15:07:13

There are security challenges your account may face, such as improper use of management permission, your password unchanged for a long time, and key information in plaintext, leading to a loss of digital assets. Given these risks, **database credentials** will be periodically rotated to create strong passwords and manage sensitive configuration information, securing your data while reducing security risks and threats to your account.

### **Key Features**

SSM allows the application and distribution of database accounts on the console. Combing with Tencent Cloud KMS, SSM can secure your sensitive information by encryption. SSM can automatically create a strong password for periodic rotation. SSM enables you to set a period of time that automatic rotation repeats.

### **Product Architecture**





#### **Process Description**

1. Create a database instance and set its account and password as an admin.

2. Create a database credential object on SSM as an admin.

Grant SSM permissions to access MySQL management services.

Set the database credential's username prefix.

Configure the automatic rotation policy.

3. When the application system needs to access the database, it can request access to the credential via the GetSecretValue API. For details, see GetSecretValue.

4. The application system parses the plaintext credential based on the content returned by the API, and obtains its account and password, thereby accessing the target database.

### **Usage Limits**

Automatic rotation is only available on **TencentDB for MySQL** and **TDSQL for MySQL**.

### Usage Guide



Creating a Database Credential Editing a Database Credential Deleting a Database Credential Access Control

## Instructions

Last updated : 2024-01-02 15:07:13

### Prerequisites

You have created a database credential. If haven't, see Creating a Database Credential. You have enabled rotation for the credential. If haven't, see Enabling a Database Credential.

### **Rotation Effect**

SSM rotates accounts and passwords stored in the credential upon a periodical rotation preset by the user, so that the client can obtain the newest account and password by calling GetSecretValue.

The rotation does not affect the credential's access to the corresponding database using the newest account and password, as SSM synchronizes the account and password information to the database.

### Integrating Application with SSM

Only by calling GetSecretValue, the application can obtain the newest account and password for database access.

### **Risk Notice**

#### Risk

The database credential's account password has been updated after the periodical rotation. If you access the database with the expired password, an access failure occurs.

#### Solution

To prevent access failure, do not enable the client to save passwords automatically. Also, use Tencent Cloud's SSM SDK (Go and Python) recommended in **Best Practices** instead of a third-party SDK that implements database connection pooling.

## Creating a Database Credential

Last updated : 2024-01-02 15:07:13

### Scenarios

You want to enable rotation and encryption for database credential created in the SSM console, securing your data while reducing disclosure risks and security threats to your account.

### Prerequisites

Before using database credentials, please note the following prerequisites: You have enabled KMS services, as SSM encrypts data based on keys managed in KMS. You have created a TencentDB for MySQL instance or TDSQL for MySQL instance. For details, see Creating MySQL Instance, and Creating TDSQL Instance.

### Directions

1. Log in to the SSM Console and click Database Credential on the left sidebar.



2. Click the drop-down button in the top left corner of the credential list to modify the region.

Secret List	·		
Create All Secrets 🔻	Edit Tag		
Secret Name	Sec T	Encryption Key	Tag (key:value)

3. Click **Create** in the top left corner of the credential list.

4. Enter the information required to create a credential and click **OK**. The credential will be displayed at the top of the credential list.

Basic settings			
Secret Name *	Enter the secret name	Description	Enter the secret description
Secret Type *	Select a secret type 💌		
Database Accour	nt Settings		
Bound Instance *	Select a CVM instance to bind 🔹 🗘 🗳	Account Prefix	Enter the account prefix
Host *	Enter one or more server IPs	Permission Configuration *	Authorization O Not authorized
	1. Enter the server IP. % is supported. 2. Separate IPs with separators ([;[]), carriage returns or spaces.		
Configure Rotati	On ③ Learn more about secret rotation     Enable it to update your database account automatically, so as to reduce security risks		
Others			
Tag	Tag key 🔹 Tag value 💌 🗙	Encryption Key *	<b>O</b> The CMK that SSM has created in KMS by default. Custom encryption key
	+ Add If there is no desired tag or tag value, you can create ☑ one in the Console.		If you have activated KMS, you can use the Tencent Cloud managed CMK that SSM has created by default in KMS for encryption, or you can create a custom encryption key in KMS and use it for encryption.Create Key in KMS
Fees C	NY/month View the billing details 🛛		
OK Car	ncel		

#### Fields

#### **Basic settings**

Secret Name: supports 1–128 bytes of letters, digits, hyphens (-), and underscores (\_). It must start with a letter or digit.

**Description**: contains information of a credential using up to 2048 bytes (optional).

#### **Database account settings**

**Bound Instance**: a MySQL instance or TDSQL instance of your choice.

**Account Prefix**: It contains 1-8 characters, including letters, digits and underscores (\_). It must start with an upper- or lower-case letter.

#### Note:

Two account names will be generated in the format of [prefix]*SSM*[three random digits]. These two account names will be shifted for rotation.

#### Server:

Must be in IP format. % is supported.

Multiple servers should be separated with a carriage return or space.

Authorization: enables you to set permissions on the database.

atabase Permissions		Rese
Global Permissions	SHOW VIEW	TRIGGER
Object-level Permissions	DELETE	INDEX
	LOCK TABLES	ALTER ROUTINE
	CREATE ROUTINE	DROP
	REFERENCES	SELECT
	UPDATE	ALTER
	EVENT	EXECUTE
		DDOCESS

#### **Rotation settings**

Rotation Status: with rotation enabled, SSM will update the database credential password periodically. It is recommended to enable rotation for safety.

Rotation Cycle: ranges from 30 days to 365 days.

Next Rotation Start: enables you to set the start time (in seconds) for next rotation as needed.

Others



Tag: optional item.

#### **Encryption Key**:

Use the default CMK that SSM has created in KMS.

Use a custom encryption key.

#### Note:

If you are using SSM, you have activated KMS. You can create an encryption key in either of the following ways:

Use the default Tencent Cloud managed CMK created in the KMS console as encryption key, and use the envelope encryption method for encrypted storage.

Use a custom key created in the KMS console as encryption key for encrypted storage.

## Editing a Database Credential

Last updated : 2024-01-02 15:07:13

### Overview

You can log in to the Tencent Cloud SSM console to view and edit information list, name, status, region and other details of the credential.

### Prerequisites

You have created your account and password in the SSM console. You have created a database credential. If haven't, see Creating a Database Credential.

### Directions

1. Log in to the SSM Console and click Database Credential on the left sidebar.

Secrets Manager		Secret List	© .	٣
🔒 Credential List				
Database Credential				

2. Click the drop-down button in the top left corner of the credential list to modify the region.

Secret List 🔇 📃 👻			
Create All Secrets *	Edit Tag		
Secret Name	Sec <b>T</b>	Encryption Key	Tag (key:value)

3. Search for a credential by entering keywords relevant to tags and credential names in the search box.



4. Click **Secret Name** to check the details of the credential.

#### Note:

You can enable or disable rotation by clicking **Rotation Status**. For details, see Modifying rotation information.

Basic Informatio	on	
Secret Name		
Status Toggle		
Status	Enabled	
Region	Guangzhou	
Creation Time	2021-10-12 17:12:53	
Creator		
Encryption Key		
Secret Type	Mysql	
Database Instance		
Description	Modify	
Rotation Details		
Rotation Details	Disabled	
Rotation Details Rotation Status Rotation Cycle	Disabled 30Days	
Rotation Details Rotation Status Rotation Cycle Configure Ret	Disabled 30Days	
Rotation Details Rotation Status Rotation Cycle Configure Rot	Disabled 30Days ation Rotate Now	
Rotation Details Rotation Status Rotation Cycle Configure Rot	Disabled 30Days ation Rotate Now	
Rotation Details Rotation Status Rotation Cycle Configure Rot Version Informa	ation Rotate Now	

5. On the credential details page, you can modify the credential description and version information, enable/disable the credential, and set rotation.

#### Modifying basic information

**Secret Status** can be changed by enabling the status toggle. If the toggle displays grayed out, the credential is disabled.

**Description** describes what the credential is used for. Maximum length: 2048 bytes. This is an optional field.

#### Modifying rotation information

The "Rotation Information" section displays the rotation status, rotation cycle, end time of last rotation and start time of next rotation (this information is available only when rotation is enabled).

**Configure Rotation**: Click this button to enter the rotation information including rotation cycle (from 30 to 365 days) and start time of next rotation (from current time plus 24 hours to current time plus 365 days) in the pop-up window.



Rotate Now: Click this button to read through a pop-up notice and then click OK to start rotation.

#### Note:

To start rotation, the rotation status must be enabled.



#### **Version Information**

The version number of a credential will be shown in the "Version Information" section. To check the credential's account name and password, you can click **View**.

#### Note:

The plaintext of the password is automatically obtained and updated by the SSM API. For security considerations, it is not recommended that you check the values of the managed credentials on the console.

Version Information			
Version Number	Creation Time	Status	Operation
SSM_Current	-	Valid	View
SSM_Rotate_	2021-10-12 17:50:55	Expired	View

## Enabling a Database Credential

Last updated : 2024-01-02 15:07:13

### Prerequisites

You have created your account and password in the SSM console. You have created a database credential. If haven't, see Creating a Database Credential.

### Directions

1. Log in to the SSM Console and click Database Credential on the left sidebar.



2. Click the drop-down button in the top left corner of the credential list to modify the region.

Secret List 💿 💻 🔹			
Create All Secrets *	Edit Tag		
Secret Name	Sec ¥	Encryption Key	Tag (key:value)

3. Search for a credential by entering keywords relevant to tags and credential names in the search box.

Se	Separate keywords with " "; press Enter to separate filter				
Count	Detetie	Next Detection Time	Orantian		
Secret	Kotatio	Next Kotation Time	Enable Disable	_	
Enabled		-	More 💌		

4. On the right of the credential of your choice, click **Enable/Disable** to enable/disable it.

#### Note:

By clicking the credential name, you can change its status on the credential details page. For details, see Editing a Database Credential.

Secret Name	Sec ¥	Encryption Key	Tag (key:value)	Creation Time *	Secre
					Enabl
					Enabl

## **Deleting a Database Credential**

Last updated : 2024-01-02 15:07:13

### Note

SSM provides the schedule deletion feature against accidental secret deletions. Each deletion has **a mandatory waiting period of 0-30 days**, that is, there will be 0-30 days to wait before the deletion becomes permanent. Once deleted, a secret **cannot be restored**, and all of its content **cannot be called**.

### Directions

1. Log in to the SSM Console and click Database Credential on the left sidebar.



2. Click the drop-down button in the top left corner of the credential list to modify the region.

Secret List	S	]		
Create	All Secrets 🔻	Edit Tag		
Secret	t Name	Sec <b>T</b>	Encryption Key	Tag (key:value)

3. In the search box on the right, enter the full or partial name of the credential you want to search.

Separate keywords with " "; press Enter to separate filter				
Secret	Rotatio	Next Rotation Time	Operation	
Enabled		-	Enable Disable More 🔻	

4. Select a credential you schedule to delete and then click **Schedule Deletion** in the **Operation** column.

#### Note:

If the credential is enabled, you need to disable it first by clicking **Disable**.

Secret Name	Sec ▼	Encryption Key	Tag (key:value)	Creation Time <sup>‡</sup>	Secret .
	_			[	Disabled
	_				Enabled

5. Set the number of schedule deletion days and then click **Confirm**. The credential will be deleted after the set number of days.

#### Note:

If the waiting period is set to "0", the credential will be deleted immediately.

Schedule Deletion	×
Note: To prevent accidental deletion, the waiting period before the deletion can be set as 0 to 30 days. If it is set to "0", the secret will be deleted immediately.	
The secret will be automatically deleted in $-1$ + day.	
Confirm	

6. Within the 1-30 waiting period, you can cancel the schedule deletion. To cancel it, click **Cancel Deletion**.



Secret Name	Sec ¥	Encryption Key	Tag (key:value)	Creation Time <sup>‡</sup>	Secret
	_				Schedu Deletic (j)

7. Enable the credential you just disabled for cancelling the deletion. Now you can disable, edit and delete the credential again.

## Tag Editing a Tag

Last updated : 2024-01-02 15:07:13

#### Overview

This document describes how to edit the tags of resources.

#### **Use Limits**

There are some limits on the usage of tags (tag key and tag value). For more information, please see Use Limits.

#### **Prerequisites**

- 1. You have logged in to the SSM console.
- 2. You have selected the region where the secret to be edited is located.

#### Directions

#### Editing the tags of a secret

1. Find the secret whose tags need to be edited and click Edit Tag in the Operation column on the right.

Create All Credentials <b>*</b> Edit Ta	9			Separate keywords with " "; pre	ss Enter to separate filter tags	Q
Credential Name	Encryption Key	Tag (key:value)	Creation Time \$	Key Status	Operation	
	11eb-b75b-52540	bfzhu1:bfzhu-test1	2020-11-03 16:41:35		Schedule Deletion Edit Tag	
Total items: 1				20 🔻 / page	1 / 1 page 🕨 🕅	4

2. In the "1 resource selected" section of the pop-up window, Add or Delete tags as needed.

#### Editing the tags of multiple secrets

1. Select the secrets whose tags need to be edited and click Edit Tag at the top of the page.

Create All Credentials <b>v</b> Edi	t Tag			Separate keywords with "["; pre-	ss Enter to separate filter tags Q
Credential Name	Encryption Key	Tag (key:value)	Creation Time \$	Key Status	Operation
	b-b75b-52540	bfzhu1:bfzhu-test1	2020-11-03 16:41:35		Schedule Deletion   Edit Tag
Total items: 1				20 🔻 / page 🛛	4 1 /1 page ▶ ▶

2. In the "n resources selected" section of the pop-up window, Add or Delete tags as needed.

For information about how to use tags, please see Examples of Management via Tags.

## Examples of Management via Tags

Last updated : 2024-01-02 15:07:13

#### Overview

Tags are used to manage resource classification and permissions from different dimensions.

For SSM, tags are used for User Credentials.

By adding tags to a secret, you can classify, track, and manage secrets more easily. Also, you can summarize the usage of secrets according to their tags.

#### **Use Limits**

There are some limits on the usage of tags (tag key and tag value). For more information, please see Use Limits.

#### Directions

#### Setting tags in the SSM console

- 1. Log in to the SSM console.
- 2. Select the region where the secret to be edited is located.
- 3. Find the secret whose tags need to be edited and click Edit Tag on the right.

Credential Name	Encryption Key	Tag (key:value)	Creation Time Ŧ	
		bfzhu1:bfzhu-test1	2020-11-03 16:41:35	

4. Set the tags in the "1 resource selected" section of the pop-up window.

The following figure shows you how to add two sets of tags.

he tag is used to r ag does not meet	manage resource your requiremer	es by category from diffe ats, please go to <mark>Manag</mark> e	erent dimensi e Tags 🛂	ions. If the existing
resource selected	I			
bfzhu1	*	bfzhu-test1	Ψ.	×
Tag key	•	Tag value	*	×
<b>⊢</b> Add				

5. Click **OK**. A message indicating the edit was successful will be prompted.

#### Filtering keys with tags

- 1. Log in to the SSM console.
- 2. Select the region where the secret to be edited is located.

3. In the **Credential List** of the selected region, use **tags** as the filter criteria, enter the filter content, and press the Enter key, as shown in the following figure.

For example, if you want to filter keys whose owner is alex, you can enter the "owner:alex" tag.

	Create All Credentials   Edit Television	àg			Та
	Credential Name	Encryption Key	Tag (key:value)	Creation Time 🕏	Key State
		leb-b75b-52540	bfzhu1:bfzhu-test1	2020-11-03 16:41:35	
	Total items: 1				
L					

## CVM SSH Key Secret Creating an SSH Key Secret

Last updated : 2024-01-02 15:07:13

### Scenarios

This document describes how to create an SSH key pair and encrypt the SSH private key on the SSM console. **Note:** 

You should meet the following requirements to use CVM SSH Key.

You have enabled KMS services, as SSM encrypts data based on keys managed in KMS.

You have created a CVM instance. For details, see Guidelines for Creating Instances.

### Directions

1. Log in to the SSM Console and click CVM SSH Key on the left sidebar.

Secrets Manager	CVM SSH Key
🕞 Credential List	
Database Credential	Create Edit Tag
OVM SSH Key	Secret Name

2. On the **CVM SSH Key** page, click the drop-down list in the top left corner to select a region.

Secrets Manager	CVM SSH Key 🛇 🗾 👻
🗟 Credential List	
Database Credential	Create Edit Tag
CVM SSH Key	Secret Name



- 3. Click Create in the top left corner of this page to create an SSH key secret.
- 4. Enter the information and then click **OK**. You will see the new secret at the top of the list on the management page.

Create an SS	H key X
Secret Name *	t
Description	
	0 / 1024
Project *	DEFAULT PROJECT *
Tag	Tag key Tag value 💌 🗙
	+ Add If there is no desired tag or tag value, you can create <sup>™</sup> one in the Console.
Encryption Key	The CMK that SSM has created in KMS by default. Custom encryption key
	Confirm Cancel

#### **Field description**

**Secret Name**: must be unique in the same region. It supports up to 128 bytes of letters, digits, hyphens and underscores and must begin with a letter or digit.

**Description**: description, such as what it is used for. It contains up to 1,024 bytes.

**Project ID**: ID of the project to which the created key pair belongs.

Tag: optional item.

#### Encryption Key:

Use the default CMK that SSM has created in KMS.

Use a custom encryption key.

#### Note:

If you are using SSM, you have activated KMS. You can create an encryption key in either of the following ways:



Use the default Tencent Cloud managed CMK created on the KMS console as encryption key, and use the envelope encryption method for encrypted storage.

Use a custom key created on the KMS console as encryption key for encrypted storage.

## Deleting an SSH Key Secret

Last updated : 2024-01-02 15:07:14

This document describes how to delete a CVM SSH key pair on the SSM console.

### Prerequisite

You have created a CVM SSH key secret.

Before deleting a secret, you need to disable it first.

The secret that is to be deleted does not bound to an instance.

#### Note:

If the secret you want to delete is bound to a CVM instance, unbind them first.

### Directions

1. Log in to the SSM Console and click CVM SSH Key on the left sidebar.

Secrets Manager	CVM SSH Key
🕞 Credential List	
Database Credential	Create Edit Tag
CVM SSH Key	Secret Name

2. On the CVM SSH Key page, click the drop-down list in the top left corner to select a region.

Secrets Manager	CVM SSH Key 🛇 🗾 👻
🗟 Credential List	
Database Credential	Create Edit Tag
OVM SSH Key	Secret Name



3. Click the search box, select a filter (Tag or Secret Name) from the list, and enter keywords to get results.

[	Separate keywords with "['; press Enter to separate filter tags			Q
	Select a filter			
n	Tag Bound CV	Ms On/Off T	Operation	
	Secret Name			

4. Locate the secret you want to remove, and click **Delete** on the right of the secret.

Secret Name	SSH Key	Encryption Key	Tag	Creation Time	Description	Bound CVMs	On/Off <sup>▼</sup>	Operation
			_		1			Associated Resources Delete

5. On the deletion page, choose an option as needed, and then click **OK**.

How to Delete
Only delete the SSH key stored in SSM
<ul> <li>Also delete the SSH key stored in SSM and CVM</li> </ul>
Confirm Cancel

## Download Private Key

Last updated : 2024-01-02 15:07:14

This document describes how to download your private key on the SSM console.

### Prerequisite

You have created an SSH key secret.

### Directions

1. Log in to the SSM Console and click CVM SSH Key on the left sidebar.

Secrets Manager	CVM SSH Key 🕓 🗸
🕞 Credential List	
Database Credential	Create Edit Tag
CVM SSH Key	Secret Name

2. On the **CVM SSH Key** page, click the drop-down list in the top left corner to select a region.

Secrets Manager	CVM SSH Key 🛇 🗾 👻
🕞 Credential List	
Database Credential	Create Edit Tag
CVM SSH Key	Secret Name

3. Click the search box, select a filter (Tag or Secret Name) from the list, and enter keywords to get results.

Separate keywords wit	")"; press Enter to separate filter tags			Q
Select a filter				
<sub>п</sub> Тад	Bound CVMs	On/Off <sup>▼</sup>	Operation	
Secret Name				

4. Locate the secret you want to check, and click the secret itself to enter the secret details page.

Secret Name	SSH Key	Encryption Key	Tag	Creation Time	Description	Bound CVMs	On/Off <sup>▼</sup>	Operation
			-		1			Associated Resources Delete

5. This page displays the SSH key information, including the name and ID of the private key and the public key content. On the right of the private key content, click **Download**.



ecret Deta	ails				
Basic In	formation				
	Secret Nam	e	•	Region	
•	Creator		Q	Creation Time	
	Encryption I	(ey		Description	
$\bigtriangledown$	Tag				
SSH key	/ informatic	on			
Key Nam	ne				
Key ID					
Key Desc	ription				
Bound C	VMs				
Project					
Public ke content	ey -			6	
Private K Content	(ey	Jownload			

## **Binding Management**

Last updated : 2024-01-02 15:07:13

This document describes how to associate SSH keys with CVM instances on the SSM console.

### Prerequisite

You have created a CVM SSH key secret.

You have created a CVM instance. For details, see Guidelines for Creating Instances.

### Directions

1. Log in to the SSM Console and click CVM SSH Key on the left sidebar.

Secrets Manager	CVM SSH Key 🛇 🗾 🗸
🕞 Credential List	
Database Credential	Create Edit Tag
CVM SSH Key	Secret Name

2. On the **CVM SSH Key** page, click the drop-down list in the top left corner to select a region.

Secrets Manager	CVM SSH Key 🛇 🗾 👻
🕞 Credential List	
Database Credential	Create Edit Tag
CVM SSH Key	Secret Name

3. Click the search box, select a filter (Tag or Secret Name) from the list, and enter keywords to get results.

Separate keywords	with " "; press Enter to separate filter tags				Q
Select a filter					
m Tag		Bound CVMs	On/Off <sup>▼</sup>	Operation	
Secret Name					

4. Select the secret you want to associate with a CVM instance, and click Associated Resources on the right.

Secret Name	SSH Key	Encryption Key	Tag	Creation Time	Description	Bound CVMs	On/Off <sup>▼</sup>	Operation
			-		P	_		Associated Resources Delete

5. On the SSH Key page of the CVM console, click Bind Instance on the right of the CVM instance you selected.

SSH Key All Projects *				
New Delete				
D/Name	Bound Instances	Bound Custom Images	Creation Time	Operation
			2021-10-19 10:06:29	Bind an instance Unbind an instance Delete

## Log Audit

Last updated : 2024-01-02 15:07:13

### 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 : 2024-01-02 15:07:13

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 : 2024-01-02 15:07:13

### 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.

Create User More 💌	
Username	User Type
>	Root Account
	Sub-user
selected, 2 in total	

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.



Permissions	Groups (0)	Security	API Key	
The last record of	t access time and the la comes from CloudAud	ast accessing ser it 🛯 and it only	vice are the last tir keeps the records	me and last service that used the curr of <u>control-flow APIs</u> of API level or r
Create Key				
Кеу				Creation Time
				2020-11-03 17:10:23

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.

Permissions	Groups (0)	Security	API Key
• Policy			
<ul> <li>Associ</li> <li>remov</li> </ul>	ate a policy to get th ing the user from th	ne action permiss e user group.	sions that the policy co
Associate Po	licy Unasso	ciate Policy	
Policy N	ame		

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.

Use group permissions	Use existing user policies	Select policies from the policy list
Authorization Notes     If you want to grant to     Create Custom Policy  Policy List (493 in total, 0 selected)	the sub-account the full access per access to all resources except CAN read-only access to all resources u	rmissions of all resources under the current account, pl I and billing center under the current account to the su nder the current account to the sub-account, please se
Policy Name		Description
Press Shift to select multiple	e items	
Next		

## **Creating an Access Control Policy**

Last updated : 2024-01-02 15:07:13

### 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