Secrets Manager
Operation Guide

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Operation Guide
Custom Secret
Creating Secrets

Last updated：2024-08-23 11:14:18

Operation scenarios

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

Operation step

1. Log in to SSM Console, in the left navigation bar, click **Custom Definition Credentials**.
2. In the top left corner of the Custom Definition Credentials, select the region for creating the credential, click **Create New**.
3. In the pop-up configuration box, enter the relevant information. Once the information has been completed, click **Confirm** to return to the credential list. The newly created credential will appear at the top of the list.

Field Description:

- Secret Name: supports 1-128 bytes of letters, digits, hyphens (-), and underscores (_). It must start with a letter or digit.
- Credential Version: Required.
- Credential Content: Required. (Up to 32KB in size)
- Description Information: Optional.
- Tag: optional item.
- Encryption Key:
  - Use the default CMK that SSM has created in KMS.
  - Use a custom encryption key.

Description

If you use SSM it indicates that you have enabled KMS. You can create encryption keys in the following two ways:

- Choose the default cloud product master key created in the KMS Console as the encryption key and encrypt the data using the envelope encryption scheme.
- Choose to create a user key in the KMS Console and use this key as your Custom Definition encryption key to encrypt and store credentials.

Editing a Secret

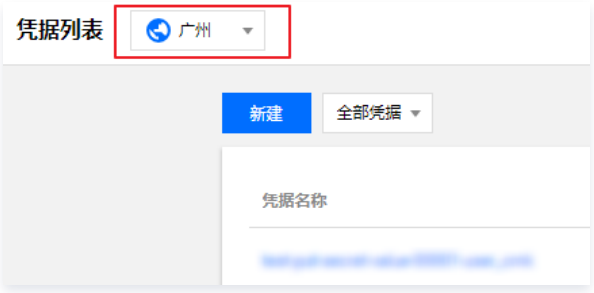
Last updated: 2024-08-23 11:16:17

Operation scenarios

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

Editing a Secret

1. Log in to SSM Console. In the left navigation bar, click **Credentials List**. At the top left of the credentials list, you can switch between different regions to view and edit the credentials list of other regions as needed.



2. In the search box on the right side of the page, enter the full or partial name of the credential to find the credential you need.

3. Click **Credential Name** to view the detailed information of the credential. You can also set the enable or disable status of the credential's key.

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.

Managing Multiple Secret Versions

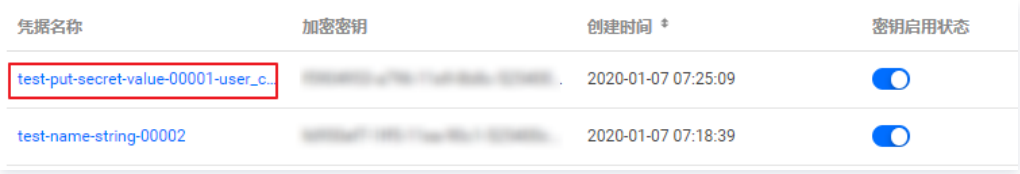
Last updated: 2024-08-23 11:16:39

Operation scenarios

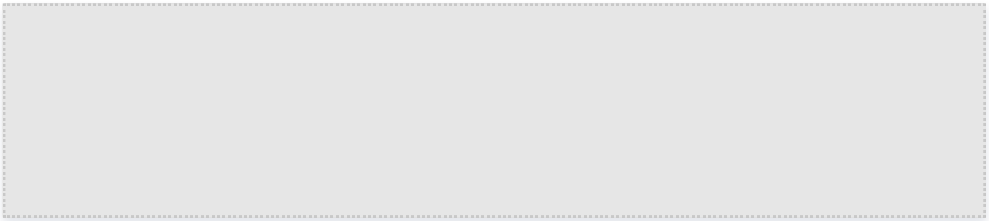
SSM provides users with multi-version credential management service. Users can implement credential rotation at the application layer through the multi-version management feature.

Operation step

1. log in to SSM Console , in the left navigation bar, click **Credentials List**. At the top left of the Credentials List, you can switch to different regions to find the target credential where you want to add a credential version, click on the credential name to enter the credential details page.



2. In the Credentials Management area, click **Add** to enter the Add Credential Information page.



3. On the Add Credential Information page, fill in the credential version and credential content. Once filled, click **Add** to complete the addition of a new credential version.

4. After adding the credential, if you need to delete it, you can click **Delete** in the operation column on the right side of the corresponding version. In the pop-up deletion confirmation box, confirm the deletion.

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

Deleting a Secret

Last updated: 2024-08-23 11:17:12

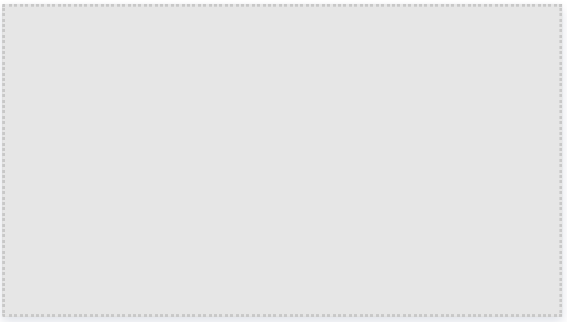
Notes

- To avoid accidental deletions, SSM uses a planned deletion mechanism, that is, **each deletion has a mandatory waiting period of 0 – 30 days**, and after confirmation of deletion, there will be an additional 0 – 30 days before the credential is permanently deleted.
- Once deleted, a credential **cannot be restored**, and all its content **cannot be invoked**.

Operation step

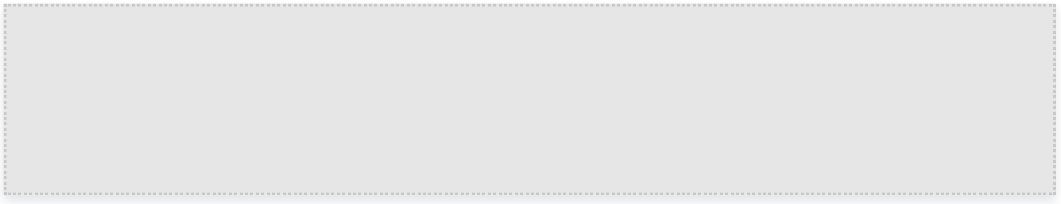
1. Log in to SSM Console, click **Credential List** in the left sidebar. At the top left of the credential list, you can switch between different regions to view credentials in other regions as needed.
2. In the credential list, select the credential to be scheduled for deletion. If the credential is in the enabled state, please disable it first. Then, in the planned deletion operation column, click **Schedule Deletion**.

3. Enter the number of days for scheduled deletion, click **Confirm**, and the credential will be deleted as scheduled.



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

4. Within the 1 – 30 days waiting period, you can cancel the deletion of the scheduled credential. To cancel the deletion, go to the right-side planned deletion operation column, click **Cancel Deletion**. After confirmation, the credential will reset to the "enabled" state, allowing disable, modify, and delete operations.



Tag
Edit tag

Last updated：2024-08-23 11:17:45

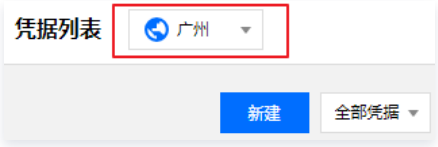
This document will guide you on how to use the Edit Tag feature in SSM.

Use Limits

For the restrictions on using Tags (Tag keys and Tag values), please refer to Tag Usage Restrictions.

Operation step

1. log in to the SSM Console, and in the left navigation pane, click **Credentials List**.
2. Switch between different regions at the top left of the credential list to view and edit the credentials tags of the desired region



- **Edit Individual Credential Tags**

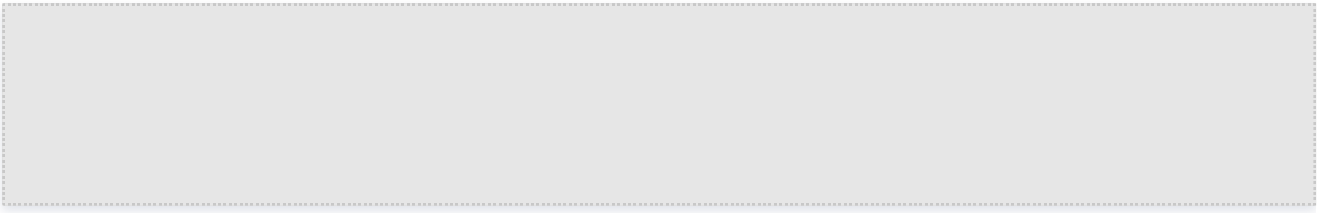
  2.1.1 Find the credentials with the tags you want to edit. In the right action column, click **Edit Tag**.\n

  2.1.2 In the pop-up "Edit Tag" window, add or delete tags as needed.

> **Note:**
> For information on how to use tags, please see Example of Tag Management.

- **Bulk Edit Tags**

  2.1.1 Select the credentials with the tags you want to edit. At the top of the credential list, click **Edit Tag**.\n



  2.1.2 In the pop-up "Edit Tag" window, add or delete tags as needed.

> **Note:**
> For information on how to use tags, please see Example of Tag Management.

Example of Managing with Tags

Last updated: 2024-08-23 11:19:32

This document will guide you on how to set tags and filter credentials by tags.

Operation scenarios

- Tags are used to classify and manage resources and permissions from different dimensions.
- In SSM, tags are mainly used for managing user credentials.
- Adding tags to credentials makes it easy for users to classify and track credentials, and also allows them to analyze the usage of credentials based on tags.

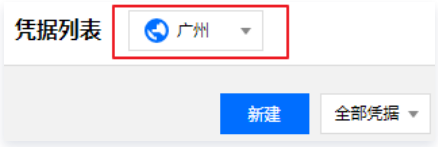
Use Limits

For restrictions on using tags (tag keys and tag values), please refer to Tag Usage Restrictions.

Operation

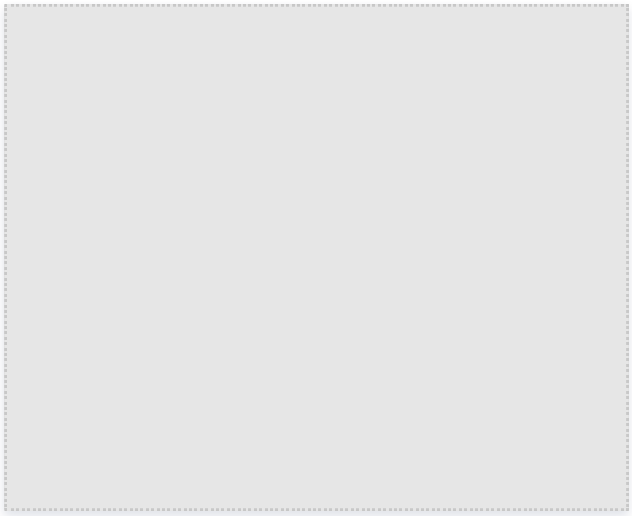
Setting Tags

1. log in to the SSM Console, and in the left navigation pane, click **Credentials List**.
2. Switch between different regions at the top left of the credential list to view and edit the credentials tags of the desired region



3. Find the credential for which you need to edit the tag, and in the right operation column, click **Edit Tag**.

4. In the pop-up "Edit Tag" window, click **Add**, and set the tag as shown below:



5. Click **Confirm** and the system will prompt that the modification was successful.

Filtering credentials by tags

1. log in to the SSM Console, and in the left navigation pane, click **Credentials List**.
2. Switch between different regions at the top left of the credential list to view and edit the credentials of the desired region.

3. In the search box above the credential list, choose " Tag " as the filter condition, enter the content to filter, click Enter to proceed. For example, if you wish to filter the keys where owner is alex , you can enter Tag :owner:alex, click Enter to proceed.

Database Credential Overview

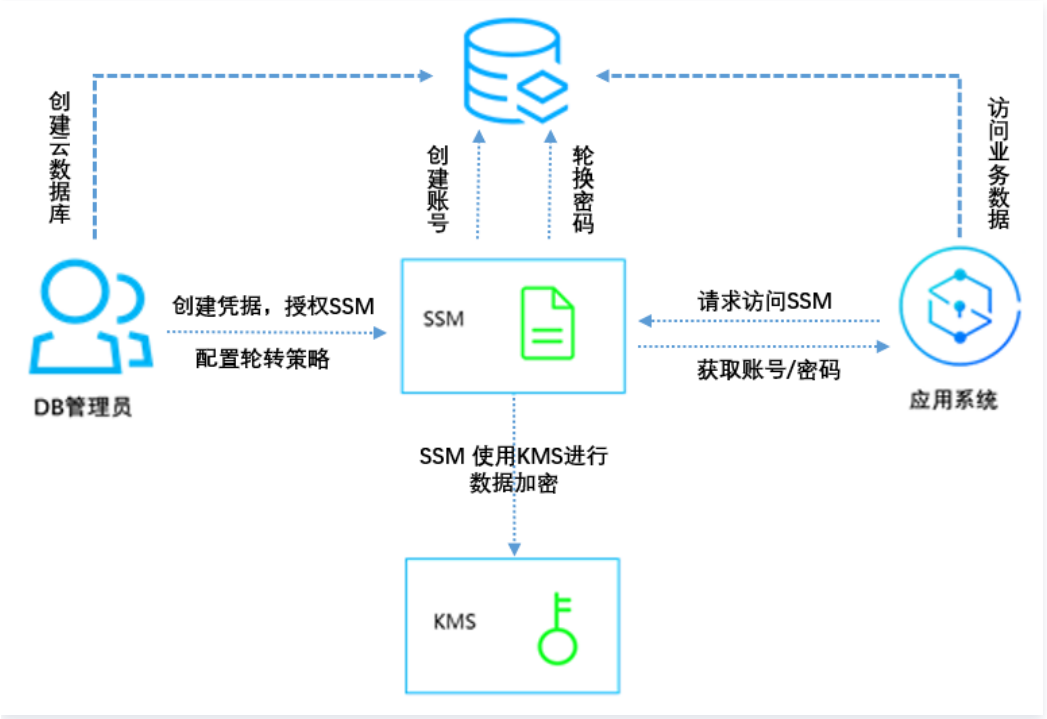
Last updated：2024-08-23 11:20:10

Currently, cloud product accounts face issues with improper management of administrative privileges, passwords remaining unchanged for long periods, and plaintext storage of key configuration information, leading to digital asset loss. To mitigate these risks, **database credentials** are rotated regularly, automatically creating strong passwords and managing sensitive configuration information. This approach not only reduces the risk and security threats to accounts but also enhances the security of business data.

Main Feature

- SSM allows the application and distribution of database accounts on the console.
- In conjunction with Tencent KMS, encryption protection is provided for sensitive information configurations.
- 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

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 application systems need to access databases, they can request access credentials from SSM. For details on the interface request, please refer to Obtaining Credential Plaintext.
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.

Use Limits

Automatic credential rotation currently supports **TencentDB for MySQL, TDSQL-C for MySQL, TDSQL for MySQL, Redis.**

Usage guide

Use Instructions

Last updated: 2024-08-23 11:20:29

Prerequisites

- Database credential created. If not created, see Creating a Database Credential.
- Credential rotation enabled. For disabled rotation, see Enable Database Credentials.

Rotation Effect

SSM will update the account password information stored in the credentials according to the rotation period preset by the user. Clients can obtain the latest valid account and password information by calling Get Plain Text Credentials. The account and password information for the same credentials will change, but the access permissions to the corresponding database remain the same. SSM will be responsible for synchronously creating or updating accounts or password with the same permissions in the database.

Integrating Application with SSM

The application only needs to call Retrieve Credential Plaintext to obtain the latest valid 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 database access failures, **do not automatically save password information on the client and avoid using third-party SDKs with database connection pool features**. Refer to Application of Database Credentials for details and use the official Tencent Cloud-provided **SSM SDK** (Go and Python) in the **Practice Tutorial** to connect to the database

Creating a Database Credential

Last updated: 2024-08-23 11:20:52

Operation scenarios

In the SSM console, create a database credential, enable credential rotation, and select encryption for the database credential to reduce account leakage risks and security threats, and improve the security of business data.

Prerequisites

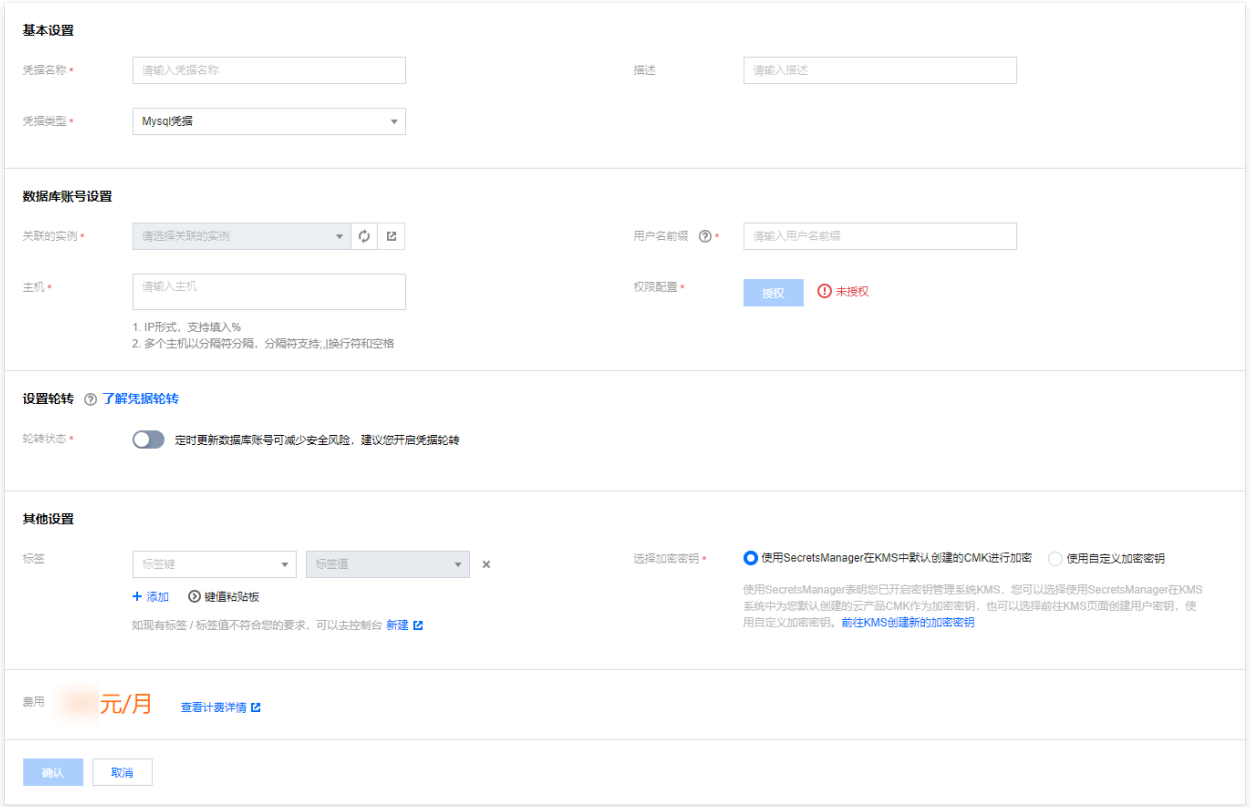
Before using database credentials, please note the following prerequisites:

- Confirm that you have activated the KMS service, and SSM encrypts using KMS-managed keys.
- Ensure you have created the relevant database instances. For specific operations, please refer to Creating MySQL Instance, Creating TDSQL Instance, Creating TDSQL-C for MySQL cluster, Creating Redis Instance.

Operation step

1. log in to SSM Console, in the left navigation bar, click **Database Credentials**.
2. In the credential list page, select the region and the **Database Type** you need to add.

3. In the credential list page, click New to enter the new credential page.
4. In the new credential page, enter the corresponding information, then click **Confirm** to return to the credential list. The newly created credential will appear at the top of the list.



Field description

Basic settings

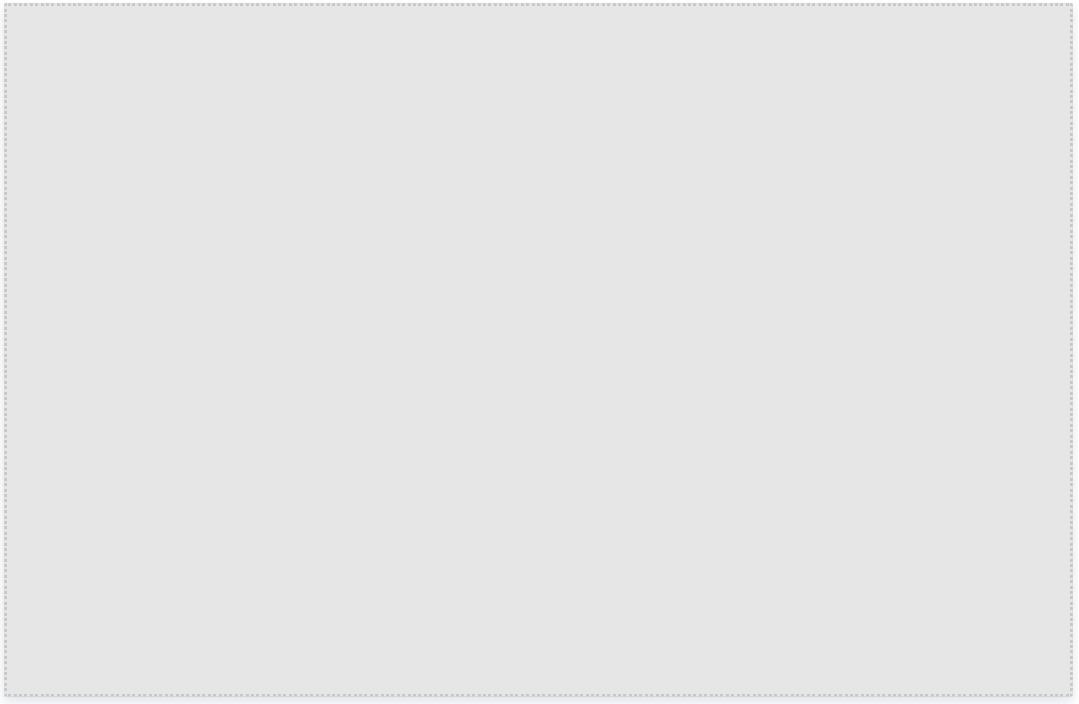
- **Credential Name:** The name length is 1–128 bytes, using letters, numbers, hyphens (-), and underscores (_). **The first character must be a letter or digit.**
- **Description:** Credential description for detailed description of usage, up to 2048 bytes. (Optional)

Database account settings

- **Associated Instances:** Select the instance you created for the selected database type.
- **Username Prefix:** Username prefix length is 1–8 bytes, using letters, digits, or _ combination. The first character must be a letter.

> **Note**
> The generated username is the username prefix + suffix. Each rotation replaces the two different usernames.

- **Host:**
  - Must be in IP format. % is supported.
  - Multiple hosts are separated by delimiters. Delimiters support newline characters and spaces.
- **Authorization:** Set database-related permissions.



Rotation settings

- **Rotation Status:** After enabling rotation, SSM will periodically update the database account's password; **It is recommended to enable it for increased security.**
- **Rotation Cycle:** Cycle interval ranges from 30 to 365 days.
- **Next Rotation Start Time:** Set the next rotation start time based on your needs. The unit is **seconds**.

Other settings

- **Tag :** Optional item.
- **Select Encryption Key:**
  - Use the default CMK that SSM has created in KMS.
  - Use a custom encryption key.

> **Note**
> If you use SSM it indicates that you have enabled KMS . You can create encryption keys in the following two ways:
> - Use the default Tencent Cloud managed CMK created in KMS as the encryption key and store it using the envelope encryption scheme.

- Use a custom key created in KMS as the encryption key for encrypted storage of credentials.

Editing a Database Credential

Last updated: 2024-08-23 11:21:14

Operation scenarios

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

- Successfully obtained control of the console's log in to account and password.
- A database credential has been created; for cases where a database credential has not been created, you can consult 'Create Database Credential' to proceed with creation.

Operation step

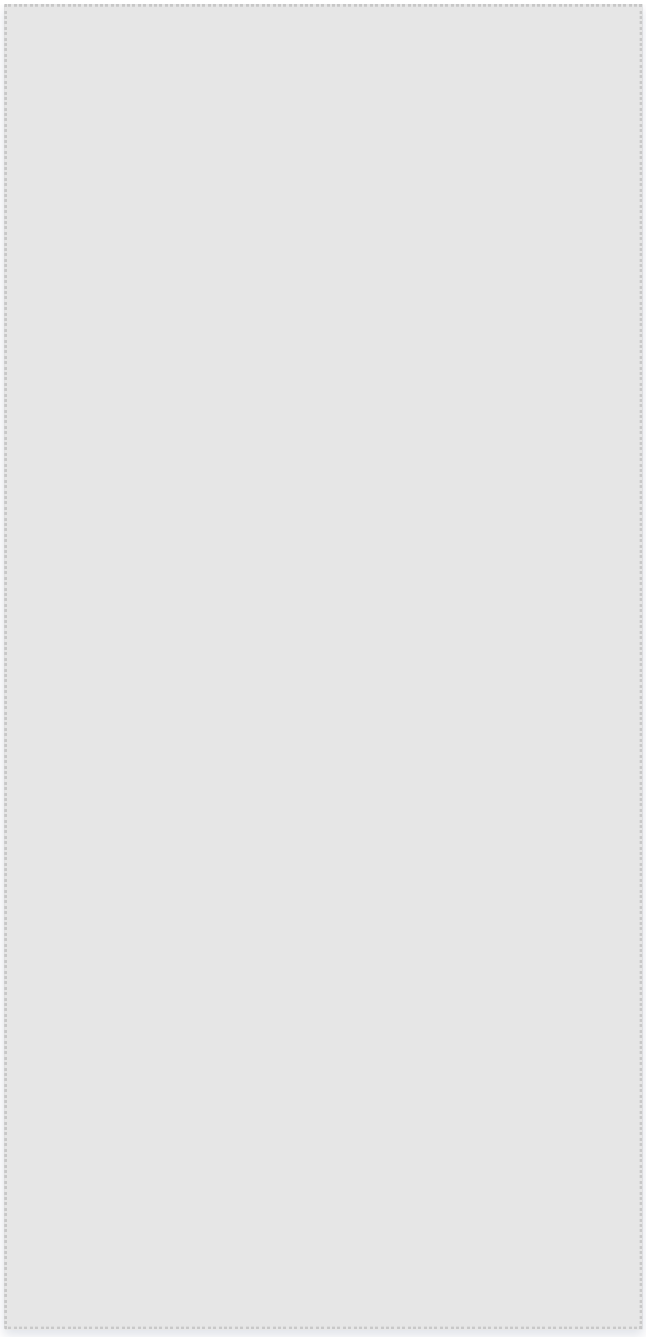
1. Log in to the SSM console, in the left navigation bar, click **Database Credentials** to enter the credentials list page.

2. On the credentials list page, click the "Region dropdown" at the top left to switch regions.

3. In the search box on the right side of the page, click the search box. You can search for credentials using keywords such as "Tag and credential name".

4. Click on 'Credential Name' to view the detailed information of the credential.

> **Note:**
> In the credential list, clicking 'Rotation Status' enables or disables rotation, where for the details of the credential rotation settings, you can view 'Modify Rotation Information'.



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

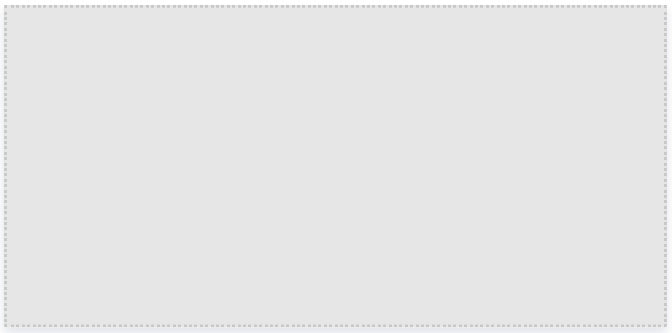
Modifying basic information

- Change Credential State: Turning on the 'Credential Switch' button toggles it, where gray indicates disabled.
- **Modify description information:** Description information is used to detail its purpose, supporting up to 2,048 bytes. (Optional)

Modifying rotation information

In this information bar, you can view the rotation status, cycle, last rotation end time, and next rotation start time (this information is available only when rotation is enabled).

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



- Immediate Rotation: After clicking 'Immediate Rotation', a pop-up will inform you of the precautions after credential rotation, clicking 'Confirm' completes the rotation operation.

> **Note:**
> The prerequisite for enabling credential rotation is that the credential must be in the enabled state.

Version Information

This information bar will display the credential's version number, clicking 'View' allows you to see the account name and account password.

> **Note:**
> The plaintext of the password is automatically obtained and updated by the SSM API. For security considerations, it is generally not recommended to check the values of the managed credentials on the console.

Enable/Disable Database Credentials

Last updated：2024-08-23 11:21:41

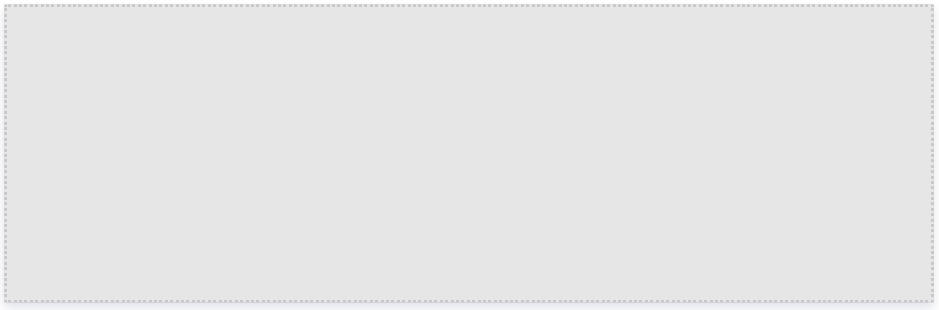
Prerequisites

- You have created your account and password in the SSM Console.
- You have created a database credential. If you haven’t, see Creating a Database Credential.

Operation step

1. Log in to the SSM Console, and in the left navigation bar, click **Database Credentials** to enter the credentials list page.

2. On the credentials list page, click the "Region dropdown" at the top left to switch regions.



3. In the search box on the right, click **Search Box**. You can find the credentials by keywords such as "Tag and Credential Name".

4. On the row of the desired credential, click **Enable** or **Disable** to enable or disable the feature of the credential.

> **Note:**
> Click the **Credential Name** to switch the credential status on the details page. For details, click Editing a Database Credential.

Deleting a Database Credential

Last updated: 2024-08-23 11:22:08

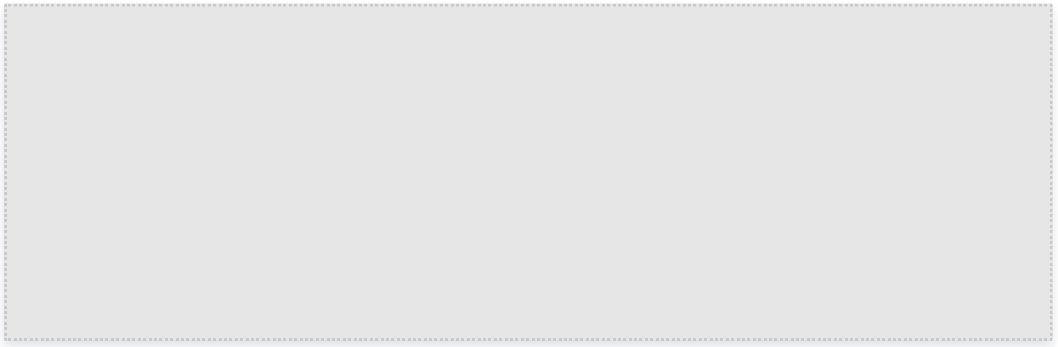
Notes

- To avoid accidental deletions, SSM uses a planned deletion mechanism, that is, **each deletion has a mandatory waiting period of 0 – 30 days**, and after confirmation of deletion, there will be an additional 0 – 30 days before the credential is permanently deleted.
- Once deleted, a credential **cannot be restored**, and all its content **cannot be invoked**.

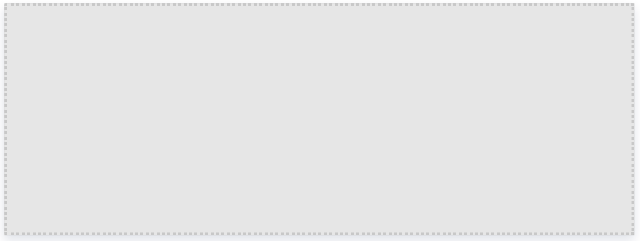
Operation step

1. Log in to SSM Console. In the left navigation bar, click **Database Credentials** to enter the Credentials List page.

2. On the credentials list page, click the "Region dropdown" at the top left to switch regions.



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

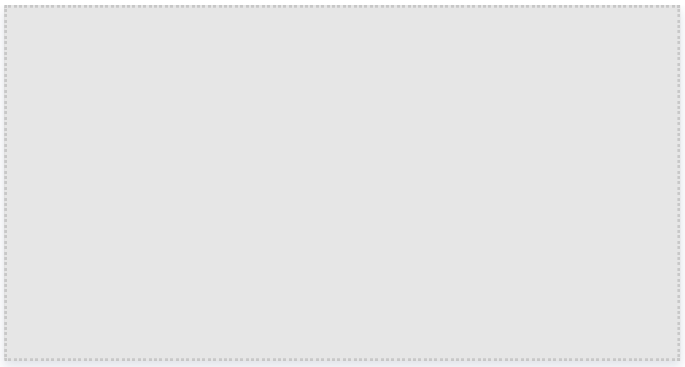


4. Select the credentials you need to schedule for deletion, and in the scheduled deletion operation column, click **Schedule for Deletion**.

> **Note:**
> If the credential is enabled, please first click **Disable** to disable the credential.

5. Enter the number of days for scheduled deletion, click **Confirm**, and the credential will be deleted as scheduled.

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



6. During the 1–30 day waiting period, you can cancel the deletion of the scheduled credentials. To cancel the deletion of credentials, click **Cancel Deletion** to cancel the deletion of the credentials.

7. After confirming the cancellation of deletion, the credential key will be reset to the "Enabled" status, and you can disable, modify, or delete the credential.

Managing Resource with Tag

Last updated: 2024-08-23 11:22:34

This document will guide you on how to set and edit Tag, and filter credentials by Tag.

Operation scenarios

- Tags are used to classify and manage resources and permissions from different dimensions.
- In SSM, tags are mainly used for managing user credentials.
- Adding tags to credentials makes it easy for users to classify and track credentials, and also allows them to analyze the usage of credentials based on tags.

Use Limits

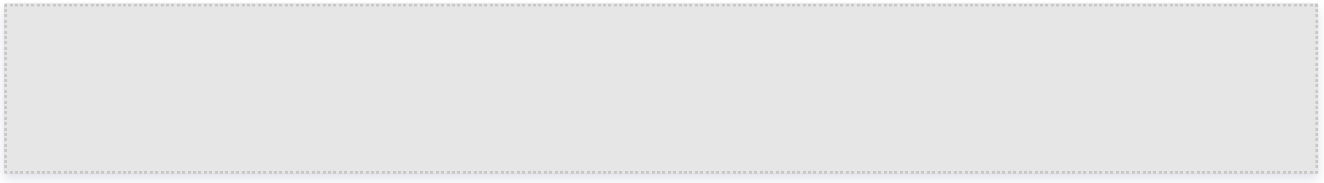
For restrictions on using tags (tag keys and tag values), please refer to Tag Usage Restrictions.

Add Tag

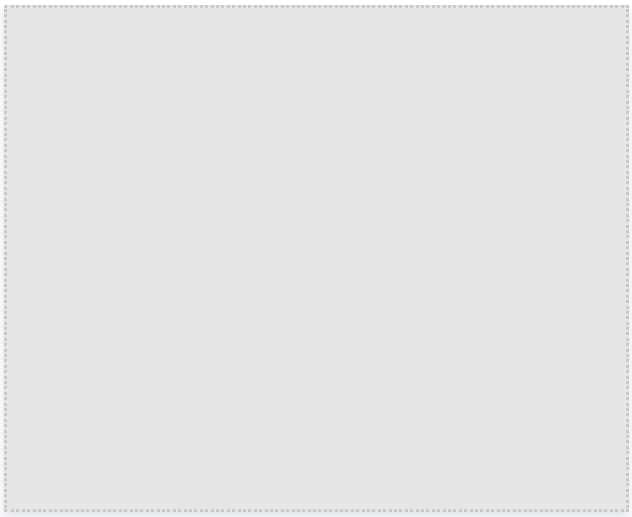
1. Log in to the SSM Console, and in the left navigation bar, click **Database Credentials** to enter the credentials list page.

2. On the credentials list page, click the "Region dropdown" at the top left to switch regions.

3. Find the credential you need to edit, and in the operation column on the right, click **Edit Tag**.



4. In the pop-up "Edit Tag" window, click **Add** to set the tag, as shown below:

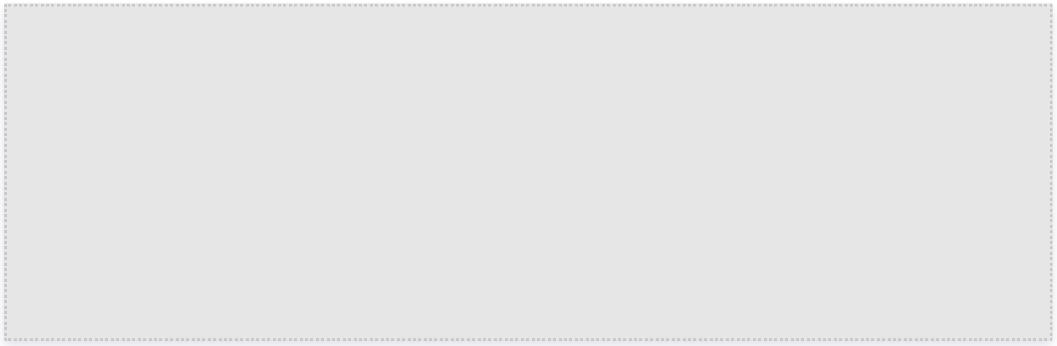


5. Click **Confirm** and the system will prompt that the modification was successful.

Edit tag

1. Log in to the SSM Console, and in the left navigation bar, click **Database Credentials** to enter the credentials list page.

2. On the credentials list page, click the "Region dropdown" at the top left to switch regions.



3. In the credential list page, both single and batch Tag editing are supported.

- **Edit Individual Credential Tags**

  3.1 Find the credential you need to edit, and in the operation column on the right, click **Edit Tag**.

  3.2 In the pop-up "Edit Tag" window, add or delete tags as needed.

> **Note**
> For information on how to use tags, please see Example of Tag Management.

- **Bulk Edit Tags**

  3.1 Select the credentials that need to edit the tag, and click **Edit Tag** above the credentials list.

3.2 In the pop-up "Edit Tag" window, add or delete tags as needed.

Filtering credentials by tags

1. Log in to the SSM Console, and in the left navigation bar, click **Database Credentials** to enter the credentials list page.

2. On the credentials list page, click the "Region dropdown" at the top left to switch regions.

3. In the search box above the credential list, choose " Tag " as the filter condition, enter the content to filter, click Enter to proceed. For example, if you wish to filter the keys where owner is alex , you can enter Tag :owner:alex, click Enter to proceed.

CVM SSH Key Credentials
Creating an SSH Key Secret

Last updated: 2024-08-23 11:23:08

Operation scenarios

Create an SSH key in the SSM console. The SSH key is securely encrypted and managed by SSM, ensuring the secure hosting of the SSH Private Key.

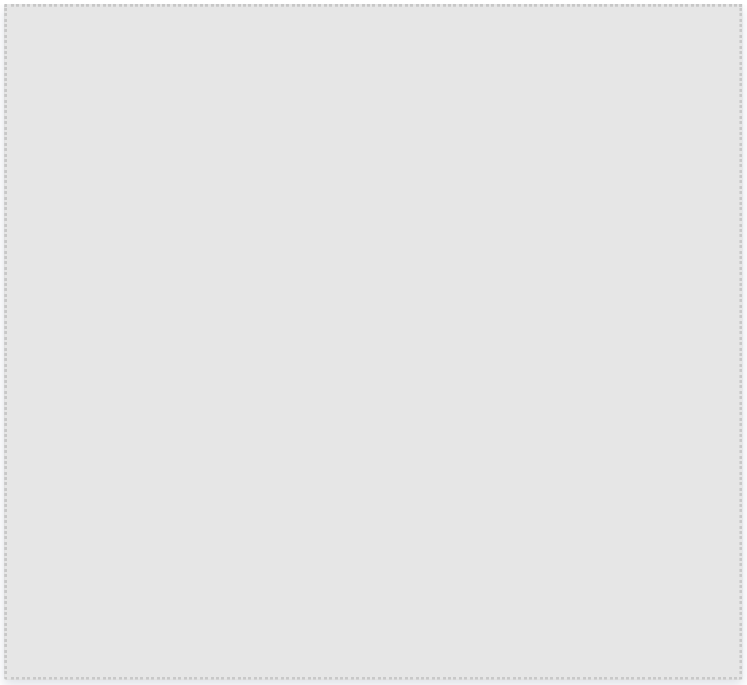
> **Note**
> To better utilize the **CVM SSH Key Management** feature, please prepare the following in advance:
> - Confirm that KMS service is activated. SSM encrypts using KMS managed keys.
> - Ensure you have created a CVM instance. For detailed steps, refer to Create a CVM Instance.

Operation step

1. Log in to SSM console, in the left navigation bar, click **CVM SSH Key Management**, to enter the CVM SSH Key page.

2. In the CVM SSH Key page, click the "Region Dropdown" in the top left corner to switch regions.

3. On the CVM SSH Key page, click **Create** in the top left corner to navigate to the create SSH key page.
4. Enter the corresponding information on the Create SSH Key page, click **OK**, return to the management page, and the newly created secret will appear at the top of the list.



Field Description

- **Credential Name:** The credential name must be unique within the same region, up to 128 bytes long, using a combination of letters, numbers, or - _. The first character must be a letter or number.
- **Description:** Detailed 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.
- **Select Encryption Key:**
  - Use the default CMK that SSM has created in KMS.
  - Use a custom encryption key.

> **Note**
> If you use SSM it indicates that you have enabled KMS. You can create encryption keys in the following two ways:
> - Use the default Tencent Cloud managed CMK created in KMS as the encryption key and store it using the envelope encryption scheme.
> - Use a custom key created in KMS as the encryption key for encrypted storage of credentials.

Deleting an SSH Key Secret

Last updated: 2024-08-23 11:23:34

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

Prerequisites

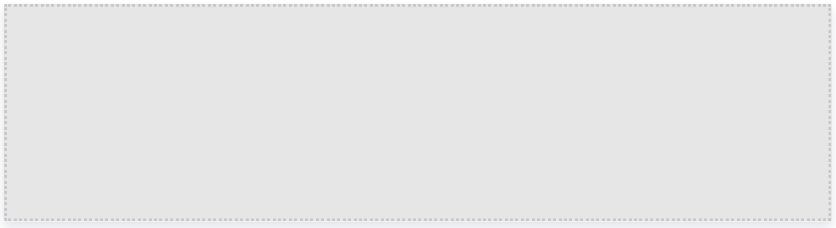
- Credentials for the created CVM SSH key have been established.
- Before deleting a secret, you need to disable it first.
- The secret that is to be deleted does not bound to an instance.

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

Operation step

1. Log in to SSM console, in the left navigation bar, click **CVM SSH Key Management**, to enter the CVM SSH Key page.

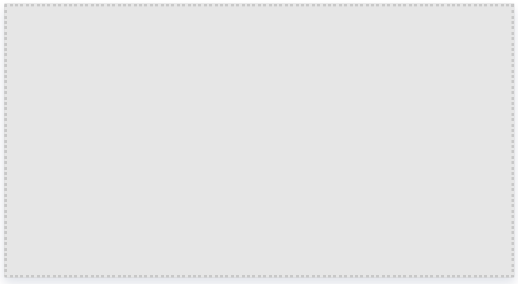
2. In the CVM SSH Key page, click the "Region Dropdown" in the top left corner to switch regions.



3. In the CVM SSH Key page, click the search box, you can search for credentials using keywords such as " Tag and credential name".

4. In the filter results list, select the credential you wish to delete and click delete in the right action column of the credential.

5. In the delete interface, you can choose based on your needs to **only delete the SSH key stored in SSM** or **delete the key stored in both SSM and CVM**. After that, click **OK**.



Download Private Key

Last updated：2024-08-23 11:23:59

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

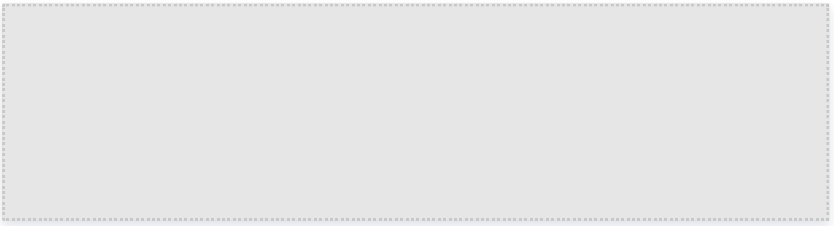
Prerequisites

- Credentials for the created CVM SSH key have been established.

Operation step

1. log in to SSM console, in the left navigation pane, click **CVM SSH Key Management**, to enter CVM SSH Key page.

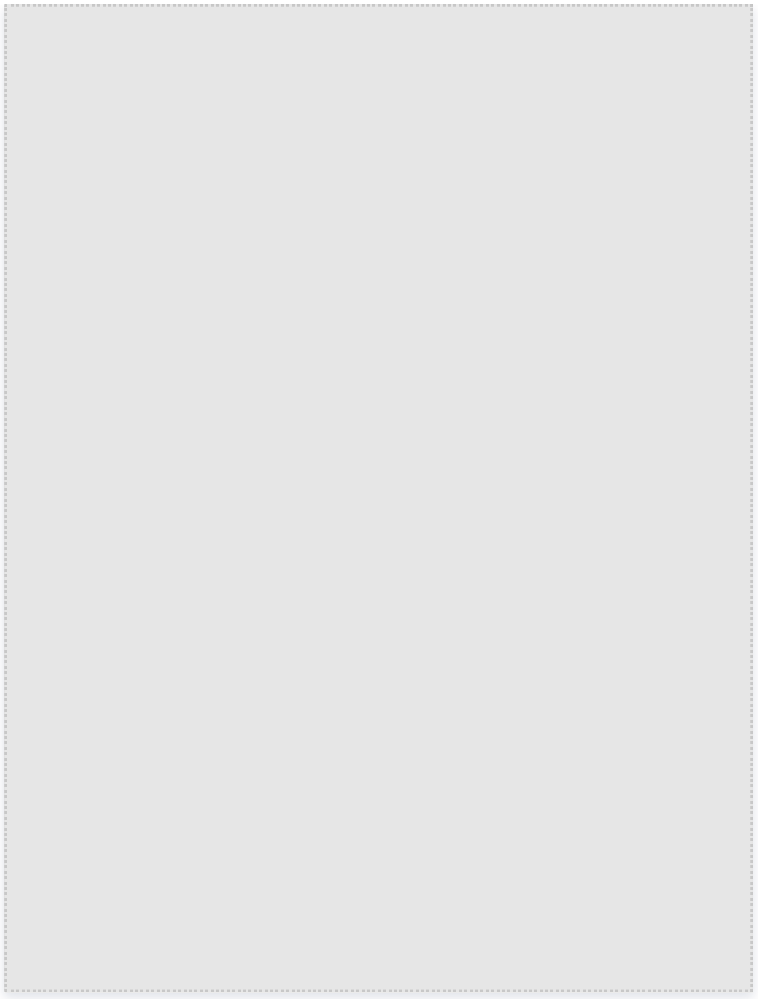
2. In the CVM SSH Key page, click the "Region Dropdown" in the top left corner to switch regions.



3. In the CVM SSH Key page, click the search box, you can search for credentials using keywords such as " Tag and credential name".

4. In the filtered results list, find the credential you wish to view, click **credential name**,to access the credential details page.

5. In the credential details page, the SSH key information displays the key name, ID, and public key content. Click **Download** on the right side of the private key content to complete the download.



Binding Management

Last updated: 2024-08-23 11:24:22

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

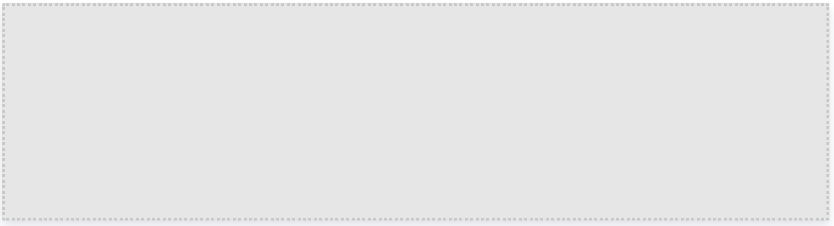
Prerequisites

- Credentials for the created CVM SSH key have been established.
- Ensure you have created a CVM instance. For detailed steps, please refer to Creating a CVM instance.

Operation step

1. log in to SSM console, in the left navigation pane, click **CVM SSH Key Management**, to enter CVM SSH Key page.

2. In the CVM SSH Key page, click the "Region Dropdown" in the top left corner to switch regions.



3. In the CVM SSH Key page, click the search box, you can search for credentials using keywords such as " Tag and credential name".

4. In the filter results list, select the credentials you need to bind and click **Bind Management** in the operation column on the right side of the credentials.

5. This will redirect you to the CVM Console, where you can bind instances in the SSH Key list page corresponding to CVM.

Log audit

Last updated：2024-08-23 11:24:41

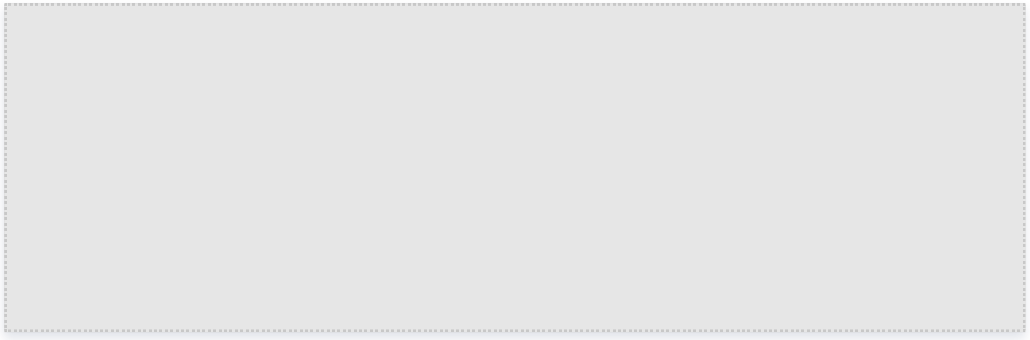
Operation scenarios

SSM integrates with Tencent CloudAudit CloudAudit , to supervise your Tencent Cloud account, conduct compliance checks, operation audits, and risk audits, and can record all credential management operations and usage.

Operation step

1. You can log in to CloudAudit Console, and in the left navigation bar, click **Operation Logs**, to view up to the last 30 days of operation logs under your Tencent Cloud account.

2. click the event name of the target event**Event Name**, to view the event details on the right side. For field explanations, refer to Appendix.



Access control
Overview

Last updated: 2024-08-23 11:25:11

If you do not need to control access to resources related to SSM for sub-accounts, you can skip this section. Skipping it will not affect your understanding and use of other documents.
If you use services like SSM, VPC (VPC), CVM (CVM), and databases at the same time, and these services are managed by different people but all share the same cloud account key, there will be issues such as the key being shared by multiple people, high risk of leakage, and an inability to restrict other people's access rights, which can easily lead to misoperations causing security risk issues.

Access control (CAM) is used to manage the access rights to resources under a Tencent Cloud account. With CAM's identity management and policy management, you can control the resource operation permissions for each sub-account. For example, if you have a credential under your main account that you only want sub-account A to use, and not sub-account B, you can control the permissions of the sub-accounts by configuring policies in CAM.

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**
  - **Main account**: The basic entity of Tencent Cloud resource ownership and the usage, metering, billing of resources. Can log in to Tencent Cloud services.
  - **Sub-account**: Created by the main account, has a specific identity ID and credentials, and can log in to the Tencent Cloud console. The main account can create multiple sub-accounts (users). Sub-accounts do not own resources by default and must be authorized by the owning main account.
  - **Credentials**: Includes login credentials and access certificates. Login credentials refer to the username and password, access certificates refer to the TencentCloud API keys (SecretId and SecretKey).
- **Resources and Permissions**
  - **Resources**: Resources are objects operated on in cloud services, like an SSM credential, CVM instance, COS bucket, VPC instance, etc.
  - **Permissions**: Permissions refer to allowing or denying certain users to perform certain actions. By default, the main account has access rights to all its resources, while sub-accounts do not have access rights to any resources under the main account.
  - **Policy**: A policy is a syntax specification that defines and describes one or more permissions. The main account completes authorization by associating policies with users or user groups.

For more information, please see Tencent Cloud Certificate Authority M CAM.

Managing Sub-Accounts

Last updated：2024-08-23 11:25:29

Overview

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

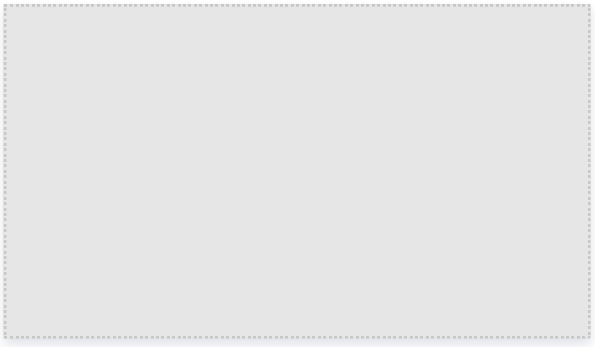
Operation step

1. Create a sub-account. Use the primary account log in to Tencent Cloud CAM CAM Console. In the left navigation, select**User** > **User List**. On the**User List** page, click **Create User** to create a sub-account.

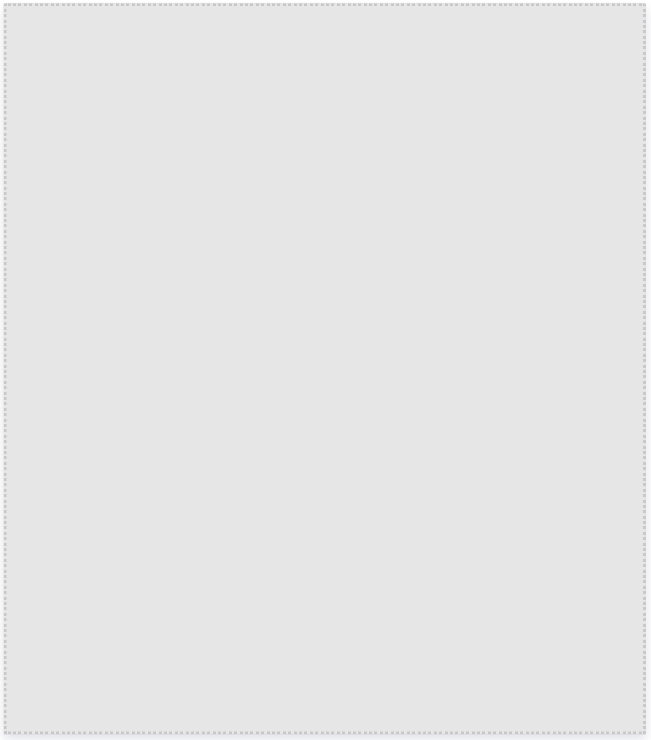
2. Create API key. Click the sub-account name to enter the sub-account details page, select**API Keys** > **Creating key** to create a SecretId and SecretKey. You can use this API key to access SSM.

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

3. Authorize sub-account. For the newly created sub-account, by authorizing SSM policy, the sub-account is allowed access to SSM . On the sub-account details page, select**Permissions** > **Associate Policy** to enter the Add Policy page.



4. Add policy. On the Add Policy page, click **Select Policy from Policy List**, choose the appropriate SSM policy, select **Next** > **Confirm** to authorize the sub-account with SSM permissions.



Creating Access Control Policy

Last updated: 2024-08-23 11:25:56

Type of Manageable Resources

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:

- `$region` : Refers to the region.
- `$uin` : Refers to the main account ID.
- `$creatorUin` : Refers to the ID of the account that created the resource.
- `$secretName` : Refers to the name of the credential to be configured.

Resource-level Authorization APIs

The API interfaces DeleteSecretVersion, UpdateDescription, RestoreSecret, EnableSecret, PutSecretValue, DescribeSecret, UpdateSecret, DeleteSecret, GetSecretValue, DisableSecret, and ListSecretVersionIds have the following resource paths:

```
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	Creating new credentials.
GetRegions	Get the available region list for display in the console.
GetServiceStatus	Get service status to determine whether the service is activated.
ListSecrets	Get information on all credentials.