

Data Encryption Workshop

FAQs

Issue 20
Date 2025-03-04



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 KMS Related	1
1.1 What Is Key Management Service?	1
1.2 What Is a Customer Master Key?	1
1.3 What Is a Default Key?	2
1.4 What Are the Differences Between a Custom Key and a Default Key?	2
1.5 What Is a Data Encryption Key?	3
1.6 Why Cannot I Delete a CMK Immediately?	3
1.7 Which Cloud Services Can Use KMS for Encryption?	3
1.8 How Do Huawei Cloud Services Use KMS to Encrypt Data?	5
1.9 What Are the Benefits of Envelope Encryption?	6
1.10 Is There a Limit on the Number of Custom Keys That I Can Create on KMS?	7
1.11 Can I Export a CMK from KMS?	7
1.12 Can I Decrypt My Data if I Permanently Delete My Custom Key?	7
1.13 How Do I Use the Online Tool to Encrypt or Decrypt Small Volumes of Data?	8
1.14 Can I Update CMKs Created by KMS-Generated Key Materials?	9
1.15 When Should I Use a CMK Created with Imported Key Materials?	9
1.16 What Should I Do When I Accidentally Delete Key Materials?	10
1.17 How Are Default Keys Generated?	10
1.18 What Should I Do If I Do Not Have the Permissions to Perform Operations on KMS?	11
1.19 Why Can't I Wrap Asymmetric Keys by Using -id-aes256-wrap-pad in OpenSSL?	11
1.20 Key Algorithms Supported by KMS	13
1.21 What Should I Do If KMS Failed to Be Requested and Error Code 401 Is Displayed?	13
1.22 What Is the Relationship Between the Ciphertext and Plaintext Returned by the encrypt-data API?	14
1.23 How Does KMS Protect My Keys?	15
1.24 How Do I Use an Asymmetric Key to Verify the Signature Result of a Public Key Pair?	15
1.25 Does an Imported Key Support Rotation?	17
1.26 Does KMS Support Offline Data Encryption and Decryption?	17
1.27 How Do I Convert an Original EC Private Key into a Private Key in PKCS8 Format?	18
2 CSMS Related	22
2.1 Why Cannot I Delete the Version Status of a Secret?	22
2.2 Why Is the Rotation Period Set for RDS Secrets Inconsistent with the Actual Rotation Period?	22

2.3 What Can I Do If "The API does not exist or has not been published in the environment" Is Displayed When I Rotate TaurusDB Secrets?.....	22
3 KPS Related.....	25
3.1 How Do I Create a Key Pair?.....	25
3.2 What Are a Private Key Pair and an Account Key Pair?.....	30
3.3 How Do I Handle an Import Failure of a Key Pair Created Using PuTTYgen?.....	31
3.4 What Should I Do When I Fail to Import a Key Pair Using Internet Explorer 9?.....	34
3.5 How Do I Log In to a Linux ECS with a Private Key?.....	34
3.6 How Do I Use a Private Key to Obtain the Password to Log In to a Windows ECS?.....	36
3.7 How Do I Handle the Failure in Binding a Key Pair?.....	37
3.8 How Do I Handle the Failure in Replacing a Key Pair?.....	39
3.9 How Do I Handle the Failure in Resetting a Key Pair?.....	40
3.10 How Do I Handle the Failure in Unbinding a Key Pair?.....	41
3.11 Do I Need to Restart Servers After Replacing Its Key Pair?.....	42
3.12 How Do I Enable the Password Login Mode for an ECS?.....	42
3.13 How Do I Handle the Failure in Logging In to ECS After Unbinding the Key Pair?.....	44
3.14 What Should I Do If My Private Key Is Lost?.....	46
3.15 How Do I Convert the Format of a Private Key File?.....	46
3.16 Can I Change the Key Pair of a Server?.....	48
3.17 Can a Key Pair Be Shared by Multiple Users?.....	48
3.18 How Do I Obtain the Public or Private Key File of a Key Pair?.....	48
3.19 What Can I Do If an Error Is Reported When an Account Key Is Created or Upgraded for the First Time?.....	49
3.20 Will the Account Key Pair Quota Be Occupied After a Private Key Pair Is Upgraded to an Account Key Pair?.....	49
3.21 Why Is the Private Key Pair Invisible After It Is Upgraded to an Account Key Pair When Logging in as a Federated User?.....	49
4 Dedicated HSM Related.....	51
4.1 What Is Dedicated HSM?.....	51
4.2 How Does Dedicated HSM Ensure the Security for Key Generation?.....	51
4.3 Do Equipment Room Personnel Has the Super Administrator Role to Steal Information by Using a Privileged UKey?.....	51
4.4 What HSMs Are Used for Dedicated HSM?.....	52
4.5 What APIs Does Dedicated HSM Support?.....	52
4.6 How Do I Enable Public Access to a Dedicated HSM Instance?.....	52
5 Pricing.....	54
5.1 How Is DEW Charged?.....	54
5.2 How Do I Renew DEW?.....	54
5.3 How Do I Unsubscribe from DEW?.....	56
5.4 Will a CMK Be Charged After It Is Disabled?.....	56
5.5 Are Credentials Scheduled to Be Deleted Billed?.....	56
5.6 Will a CMK Be Charged After It Is Scheduled to Delete?.....	56
5.7 How Is Rotation Charged for a CMK?.....	57

6 General.....	58
6.1 What Functions Does DEW Provide?.....	58
6.2 What Cryptography Algorithms Does DEW Use?.....	59
6.3 In Which Regions Are DEW Services Available?.....	60
6.4 What Is a Quota?.....	60
6.5 What Is the Resource Allocation Mechanism of DEW?.....	62
6.6 What Are Regions and AZs?.....	62
6.7 Can DEW Be Shared Across Accounts?.....	63
6.8 How Do I Access the Functions of DEW?.....	64
6.9 Why Do DEW Permissions Fail to Take Effect Immediately?.....	64

1 KMS Related

1.1 What Is Key Management Service?

KMS is a secure, reliable, and easy-to-use cloud service that helps users create, manage, and protect keys in a centralized manner.

It uses Hardware Security Modules (HSMs) to protect keys. All keys are protected by root keys in HSMs to avoid key leakage. The HSMs meet the FIPS 140-2 Level 3 security requirements.

It also controls access to keys and records all operations on keys with traceable logs. In addition, it provides use records of all keys, meeting your audit and regulatory compliance requirements.

1.2 What Is a Customer Master Key?

A Customer Master Key (CMK) is a Key Encryption Key (KEK) created by a user on KMS. It is used to encrypt and protect DEKs. One CMK can be used to encrypt one or more DEKs.

CMKs are categorized into custom keys and default keys.

- Custom keys
Keys created or imported by users on the KMS console.
- Default keys

When a user uses KMS for encryption in a cloud service for the first time, the cloud service automatically creates a key with the alias suffix **/default**.

You can use the management console to query but cannot disable or schedule the deletion of Default Master Keys.

Table 1-1 Default Master Keys

Alias	Cloud Service
obs/default	Object Storage Service (OBS)

Alias	Cloud Service
evs/default	Elastic Volume Service (EVS)
ims/default	Image Management Service (IMS)
kps/default	Key Pair Service (KPS)
csms/default	Cloud Secret Management Service (CSMS)

1.3 What Is a Default Key?

A default key is automatically created by another cloud service using KMS, such as Object Storage Service (OBS). The alias of a default key ends with **/default**.

You can use the management console to query but cannot disable or schedule the deletion of default keys.

Default keys are hosted for free, and are charged based on the number of the API requests for them. If API requests exceed the free limit, the excess part will be charged.

Table 1-2 Default Master Keys

Alias	Cloud Service
obs/default	Object Storage Service (OBS)
evs/default	Elastic Volume Service (EVS)
ims/default	Image Management Service (IMS)
vbs/default	Volume Backup Service (VBS)
sfs/default	Scalable File Service (SFS)
kps/default	Key Pair Service (KPS)
csms/default	Cloud Secret Management Service (CSMS)

NOTE

A default key is automatically created when a user employs the KMS encryption function for the first time in another cloud service.

1.4 What Are the Differences Between a Custom Key and a Default Key?

The following table describes the differences between a custom key and a default key.

Table 1-3 Differences between a custom key and a default key

Item	Definition	Difference
Custom key	A Key Encryption Key (KEK) created using KMS. The key is used to encrypt and protect DEKs. A custom key can be used to encrypt multiple DEKs.	<ul style="list-style-type: none">• It can be disabled and scheduled for deletion.• It is billed per use after the being created or imported.
Default key	Automatically generated by the system when you use KMS to encrypt data in another cloud service for the first time. The suffix of the key is / default . Example: evs/default	<ul style="list-style-type: none">• It cannot be disabled or scheduled for deletion.• You are not charged when you use the cloud service automatically generated by the system. If the number of API requests exceeds 20,000, you will be billed.

1.5 What Is a Data Encryption Key?

A data encryption key (DEK) is used to encrypt data.

1.6 Why Cannot I Delete a CMK Immediately?

The decision to delete a CMK should be considered with great caution. Before deletion, confirm that the CMK's encrypted data has all been migrated. As soon as the CMK is deleted, you will not be able to decrypt data with it. Therefore, KMS offers a user-specified period of 7 to 1096 days for the deletion to finally take effect. On the scheduled day of deletion, the CMK will be permanently deleted. However, prior to the scheduled day, you can still cancel the pending deletion. This is a means of precaution within KMS.

1.7 Which Cloud Services Can Use KMS for Encryption?

Object Storage Service (OBS), Elastic Volume Service (EVS), Image Management Service (IMS), and Relational Database Service (RDS) can use KMS for encryption.

Table 1-4 List of cloud services that use KMS encryption

Service Name	Description
Object Storage Service (OBS)	<p>You can upload objects to and download them from Object Storage Service (OBS) in common mode or server-side encryption mode. When you upload objects in encryption mode, data is encrypted at the server side and then securely stored on OBS in ciphertext. When you download encrypted objects, the data in ciphertext is decrypted at the server side and then provided to you in plaintext. OBS supports the server-side encryption with KMS-managed keys (SSE-KMS) mode. In SSE-KMS mode, OBS uses the keys provided by KMS for server-side encryption.</p> <p>For details about how to upload objects to OBS in SSE-KMS mode, see the Object Storage Service Console Operation Guide.</p>
Elastic Volume Service (EVS)	<p>If you enable the encryption function when creating an EVS disk, the disk will be encrypted with the DEK generated by using your CMK. Data stored in the EVS disk will be automatically encrypted.</p> <p>For details about how to use the encryption function of EVS, see Elastic Volume Service User Guide.</p>
Image Management Service (IMS)	<p>When creating a private image using an external image file, you can enable the private image encryption function and select a CMK provided by KMS to encrypt the image.</p> <p>For details about how to use the private image encryption function of Image Management Service (IMS), see Image Management Service User Guide.</p>
Scalable File Service (SFS)	<p>When creating a file system on SFS, the CMK provided by KMS can be selected to encrypt the file system, so that files stored in the file system are automatically encrypted.</p> <p>For details about how to use the file system encryption function of SFS, see Scalable File Service User Guide.</p>
Relational Database Service (RDS)	<p>When purchasing a database instance, you can enable the disk encryption function of the database instance and select a CMK created on KMS to encrypt the disk of the database instance. Enabling the disk encryption function will enhance data security.</p> <p>For details about how to use the disk encryption function of RDS, see Relational Database Service User Guide.</p>
Document Database Service (DDS)	<p>When purchasing a DDS instance, you can enable the disk encryption function of the instance and select a CMK created on KMS to encrypt the disk of the instance. Enabling the disk encryption function will enhance data security.</p> <p>For details about how to use the disk encryption function of DDS, see Document Database Service Getting Started.</p>

1.8 How Do Huawei Cloud Services Use KMS to Encrypt Data?

Generally, **Huawei Cloud services** use KMS envelope encryption to protect user data.

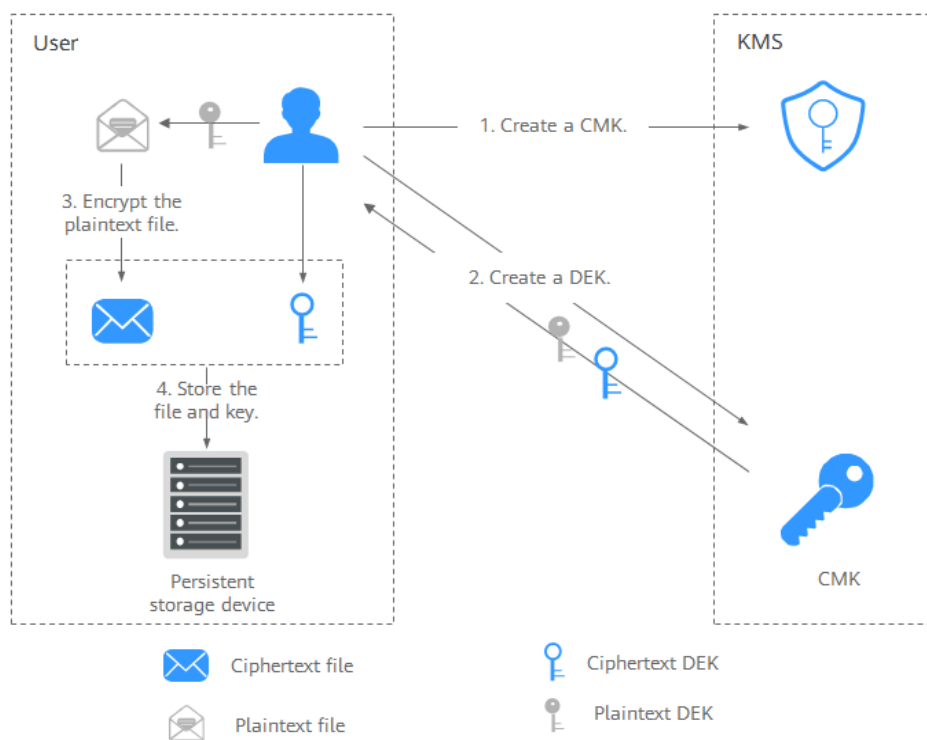
NOTE

Envelope encryption is the practice of encrypting data with a DEK and then encrypting the DEK with a root key that you can fully manage. In this case, CMKs are not required for encryption or decryption.

Envelope Encryption and Decryption Principles

- **Figure 1-1** illustrates the process for encrypting a local file.

Figure 1-1 Encrypting a local file

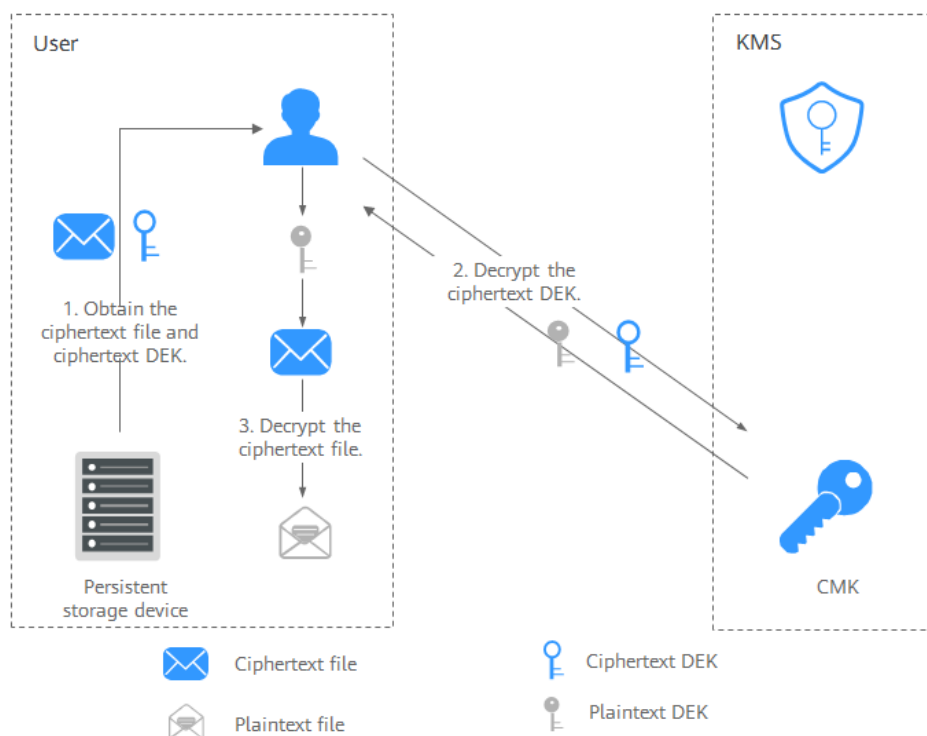


The procedure is as follows:

- Create a CMK on KMS.
- Call the **create-datakey** API of KMS to create a DEK. Then you get a plaintext DEK and a ciphertext DEK. The ciphertext DEK is generated when you use a CMK to encrypt the plaintext DEK.
- Use the plaintext DEK to encrypt the file. A ciphertext file is generated.
- Save the ciphertext DEK and the ciphertext file together in a persistent storage device or a storage service.

- **Figure 1-2** illustrates the process for decrypting a local file.

Figure 1-2 Decrypting a local file



The procedure is as follows:

- Obtain the ciphertext DEK and file from the persistent storage device or the storage service.
- Call the **decrypt-datakey** API of KMS and use the corresponding CMK (the one used for encrypting the DEK) to decrypt the ciphertext DEK. Then you get the plaintext DEK.
If the CMK is deleted, the decryption fails. Therefore, properly keep your CMKs.
- Use the plaintext DEK to decrypt the ciphertext file.

For details about how to use KMS to encrypt and decrypt data, see [Using KMS to Encrypt and Decrypt Data for Cloud Services](#).

1.9 What Are the Benefits of Envelope Encryption?

Envelope encryption is the practice of encrypting data with a DEK and then encrypting the DEK with a root key that you can fully manage. In this case, CMKs are not required for encryption or decryption.

Benefits:

- Advantages over CMK encryption in KMS
Users can use CMKs to encrypt and decrypt data on the KMS console or by calling KMS APIs.

A CMK can encrypt and decrypt data no more than 4 KB. An envelope can encrypt and decrypt larger volumes of data.

Data encrypted using envelopes does not need to be transferred. Only the DEKs need to be transferred to the KMS server.

- Advantages over encryption by using cloud services
 - Security

Data transferred to the cloud for encryption is exposed to risks such as interception and phishing.

During envelope encryption, KMS uses Hardware Security Modules (HSMs) to protect keys. All CMKs are protected by root keys in HSMs to avoid key leakage.
 - Trustworthiness

You will worry about data security on the cloud. It is also difficult for cloud services to prove that they never misuse or disclose such data.

If you choose envelope encryption, KMS will control access to keys and record all usages of and operations on keys with traceable logs, meeting your audit and regulatory compliance requirements.
 - Performance and cost

To encrypt or decrypt data using a cloud service, you have to send the data to the encryption server and receive the processed data. This process seriously affects your service performance and incurs high costs.

Envelope encryption allows you to generate DEKs online by calling KMS cryptographic algorithm APIs, and to encrypt a large amount of local data with the DEKs.

1.10 Is There a Limit on the Number of Custom Keys That I Can Create on KMS?

There is a limit on the number of custom keys that can be created on KMS.

You can create a maximum of 100 custom keys, including those in enabled, disabled, and pending deletion states. Default keys are not included.

1.11 Can I Export a CMK from KMS?

No.

To ensure CMK security, users can only create and use CMKs in KMS.

1.12 Can I Decrypt My Data if I Permanently Delete My Custom Key?

No.

If you have permanently deleted your custom key, the data encrypted using it cannot be decrypted. Before the scheduled deletion date of the custom key, you can cancel the scheduled deletion.

1.13 How Do I Use the Online Tool to Encrypt or Decrypt Small Volumes of Data?

You can use the online tool to encrypt or decrypt data in the following procedures:

Encrypting Data



- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation on the left, choose  > **Security & Compliance > Data Encryption Workshop.**
- Step 4** Click the name of the target custom key to access the key details page. Click the **Tool** tab.
- Step 5** Click **Encrypt**. In the text box on the left, enter the data to be encrypted, as shown in [Figure 1-3](#).

Figure 1-3 Encrypting data



- Step 6** Click **Execute**. Ciphertext of the data is displayed in the text box on the right.

NOTE

- Use the current CMK to encrypt the data.
- You can click **Clear** to clear the entered data.
- You can click **Copy to Clipboard** to copy the ciphertext and save it in a local file.

----End


NOTE

Enter the plaintext on the console, the text will be encoded to Base64 format before encryption.

The decryption result returned via API will be in Base64 format. Perform Base64 decoding to obtain the plaintext entered on the console.

Decrypting Data

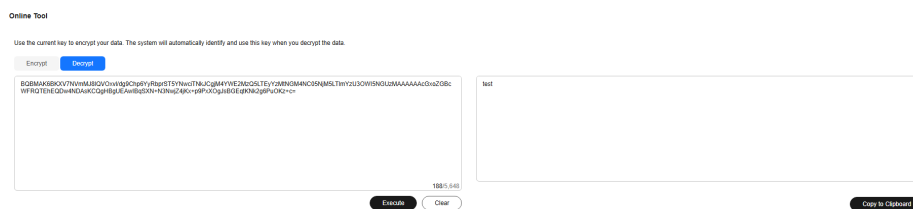
- Step 1** [Log in to the management console.](#)

- Step 2** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 3** You can click any non-default key in **Enabled** status to go to the encryption and decryption page of the online tool.
- Step 4** Click **Decrypt**. In the text box on the left, enter the data to be decrypted. For details, see [Figure 1-4](#).

 **NOTE**

- The tool will identify the original encryption CMK and use it to decrypt the data.
- If the key has been deleted, the decryption will fail.

Figure 1-4 Decrypting data



- Step 5** Click **Execute**. Plaintext of the data is displayed in the text box on the right.

 **NOTE**

- You can click **Copy to Clipboard** to copy the plaintext and save it in a local file.
- Enter the plaintext on the console, the text will be encoded to Base64 format before encryption.

The decryption result returned via API will be in Base64 format. Perform Base64 decoding to obtain the plaintext entered on the console.

----End

1.14 Can I Update CMKs Created by KMS-Generated Key Materials?

No.

Keys created using KMS-generated materials cannot be updated. You can only use KMS to create new CMKs to encrypt and decrypt data.

1.15 When Should I Use a CMK Created with Imported Key Materials?

- If you do not want to use KMS-generated key materials, you can import your own key materials to create a CMK. Such a CMK allows deletion of only the key materials when you do not need it. In addition, when you find that the key materials are mis-deleted, you can import the same materials to the CMK.

- You can also import off-cloud key materials to KMS when you want to use the same keys on and off the cloud. This practice has proved useful when users migrate local encrypted data onto cloud.

1.16 What Should I Do When I Accidentally Delete Key Materials?

You can import the backup key materials from your local device again.

NOTICE

Before importing key materials, you are advised to back up the materials. The materials to be re-imported must be consistent with the mis-deleted materials.

1.17 How Are Default Keys Generated?

Default keys are automatically generated.

When a user uses KMS for encryption in a cloud service for the first time, the cloud service automatically creates a key with the alias suffix **/default**.

You can use the management console to query but cannot disable or schedule the deletion of Default Master Keys.

Default keys are hosted for free, and are charged based on the number of the API requests for them. If API requests exceed the free limit, the excess part will be charged.

Table 1-5 Default Master Keys

Alias	Cloud Service
obs/default	Object Storage Service (OBS)
evs/default	Elastic Volume Service (EVS)
ims/default	Image Management Service (IMS)
kps/default	Key Pair Service (KPS)
csms/default	Cloud Secret Management Service (CSMS)

1.18 What Should I Do If I Do Not Have the Permissions to Perform Operations on KMS?

Symptom

A message indicating lack of permissions is displayed when you attempt to perform operations on keys, such as view, create, or import keys.

Possible Causes

Your account is not associated with the required KMS system policies.

Solution

Step 1 Check whether your account has been associated with **KMS Administrator** and **KMS CMKFullAccess** policies.

For details about how to check your user groups and permissions, see [User Groups and Authorization](#).

If your account has been associated with required KMS system policies, go to [Step 2](#).

Step 2 Associate your account with required system policies.

- For details about how to add administrator permissions, see [User Groups and Authorization](#).
- For details about how to add a custom policy, see [Creating a Custom DEW Policy](#).

----End

1.19 Why Can't I Wrap Asymmetric Keys by Using -id-aes256-wrap-pad in OpenSSL?

Symptom

By default, the -id-aes256-wrap-pad algorithm is not enabled in OpenSSL. To wrap a key, upgrade OpenSSL to the latest version and patch it first.

Solution

Use bash commands to create a local copy of the existing OpenSSL. You do not need to delete or modify the default OpenSSL client installation configurations.

Step 1 Switch to the **root** user.

```
sudo su -
```

Step 2 Run the following command and record the OpenSSL version:

openssl version

Step 3 Run the following commands to create the **/root/build** directory. This directory will be used to store the latest OpenSSL binary file.

```
mkdir $HOME/build
```

```
mkdir -p $HOME/local/ssl
```

```
cd $HOME/build
```

Step 4 Download the latest OpenSSL version from <https://www.openssl.org/source/>.

Step 5 Download and decompress the binary file.

Step 6 Replace **openssl-1.1.1d.tar.gz** with the latest OpenSSL version downloaded in [step 4](#).

```
curl -O https://www.openssl.org/source/openssl-1.1.1d.tar.gz
```

```
tar -zxf openssl-1.1.1d.tar.gz
```

Step 7 Use the **gcc** tool to patch the version, and compile the downloaded binary file.

```
yum install patch make gcc -y
```

 **NOTE**

If you are using a version other than OpenSSL-1.1.1d, you may need to change the directory and commands used, or this patch may not work properly.

Step 8 Run the following commands:

```
sed -i "/BIO_get_cipher_ctx(benc, &ctx);/a\ EVP_CIPHER_CTX_set_flags(ctx, EVP_CIPHER_CTX_FLAG_WRAP_ALLOW);" $HOME/build/openssl-1.1.1d/apps/enc.c
```

Step 9 Run the following commands to compile the OpenSSL **enc.c** file:

```
cd $HOME/build/openssl-1.1.1d/
```

```
./config --prefix=$HOME/local --openssldir=$HOME/local/ssl
```

```
make -j$(grep -c ^processor /proc/cpuinfo)
```

```
make install
```

Step 10 Configure the environment variable **LD_LIBRARY_PATH** to ensure that required libraries are available for OpenSSL. The latest version of OpenSSL has been dynamically linked to the binary file in the **\$HOME/local/ssl/lib/** directory, and cannot be directly executed in shell.

Step 11 Create a script named **openssl.sh** to load the **\$HOME/local/ssl/lib/** path before running the binary file.

```
cd $HOME/local/bin/
```

```
echo -e '#!/bin/bash \nenv LD_LIBRARY_PATH=$HOME/local/lib/ $HOME/local/bin/openssl "$@"' > ./openssl.sh
```

Step 12 Run the following command to configure an execute bit on the script:

```
chmod 755 ./openssl.sh
```

Step 13 Run the following command to start the patched OpenSSL version:

```
$HOME/local/bin/openssl.sh
```

```
----End
```

1.20 Key Algorithms Supported by KMS

Table 1-6 Key algorithms supported by KMS

Key Type	Algorithm Type	Key Specifications	Description	Usage
Symmetric key	AES	<ul style="list-style-type: none">• AES_256	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.
Digest key	SHA	<ul style="list-style-type: none">• HMAC_256• HMAC_384• HMAC_512	SHA digest key	<ul style="list-style-type: none">• Data tampering prevention• Data integrity verification
Digest key	SM3	<ul style="list-style-type: none">• HMAC_SM3	SM3 digest key	<ul style="list-style-type: none">• Data tampering prevention• Data integrity verification
Asymmetric key	RSA	<ul style="list-style-type: none">• RSA_2048• RSA_3072• RSA_4096	RSA asymmetric password	Encrypts and decrypts a small amount of data or creates digital signatures.
	ECC	<ul style="list-style-type: none">• EC_P256• EC_P384	Elliptic curve recommended by NIST	Digital signature

1.21 What Should I Do If KMS Failed to Be Requested and Error Code 401 Is Displayed?

Symptom

An error is reported when KMS is requested or the cloud service encryption function is enabled.

Error information: **httpcode=401,code=APIGW.0301,Msg=Incorrect IAM authentication information: current ip:xx.xx.xx.xx refused**

Possible Causes

Access control is configured in IAM.


By default, IAM allows access from any IP addresses. If you configure ACL, the IP addresses and network segments out of the specified range cannot access KMS or use the cloud encryption feature.

Solution

- To access KMS through the cloud service console (for example, for OBS encryption purposes), allow access from network segments 10.0.0.0/8, 11.0.0.0/8, and 26.0.0.0/8.
- To call KMS via API, allow access from the source IP addresses.

Allowing Access from Specific IP Addresses

Step 1 [Log in to the management console](#).

Step 2 Click  on the left of the page and choose **Management & Governance > Identity and Access Management**. The **Users** page is displayed.

Step 3 Choose **Security Settings** and click the **ACL** tab. Check whether **IP Address Ranges** and **IPv4 CIDR Blocks** are properly configured.

NOTE

The source IP address you use must be specified on both the **Console Access** and **API Access** tabs.

----End

1.22 What Is the Relationship Between the Ciphertext and Plaintext Returned by the encrypt-data API?

The basic length of the ciphertext returned by the encrypt-data API is 124 bytes. The ciphertext consists of multiple fields, including the key ID, encryption algorithm, key version, and ciphertext digest.

The plaintext has 16 bytes in each block. A block with fewer than 16 bytes will be padded. Ciphertext length = 124 + Ceil(plaintext length/16) x 16. The conversion result is encoded using Base64.

Take 4-byte plaintext input as an example. The calculation result is 124 + Ceil(4/16) x 16 = 140. The 140 bytes are converted into 188 bytes after Base64 encoding.

NOTE

Ceil is a round-up function. Ceil(a) = 1. The value range of **a** is (0,1].

1.23 How Does KMS Protect My Keys?

The mechanism of KMS prevents anyone from accessing your keys in plaintext. KMS relies on hardware security modules (HSMs) that safeguard the confidentiality and integrity of your keys. Plaintext KMS keys are always encrypted by HSMs and are never stored on any disk. These keys are only utilized within the volatile memory of the HSMs for as long as necessary to perform the cryptographic operation you have requested.

1.24 How Do I Use an Asymmetric Key to Verify the Signature Result of a Public Key Pair?

In scenarios where public and private key pairs are used, the private key is used for signature and the public key is used for signature verification. The public key can be distributed to the service subject that needs to use the public key. The service subject verifies the signature of the key data. KMS provides the API **get-publickey** for obtaining public keys.

The **RSA_3072** CMK in this case is used to verify signatures. You can use KMS to sign APIs. The request body is as follows:

```
{
  "key_id": "key_id_value",
  "message": "MTlzNA==",
  "signing_algorithm": "RSASSA_PSS_SHA_256",
  "message_type": "RAW"
}
```

The result is as follows:

```
{
  "key_id": "key_id_value",
  "signature": "xxx"
}
```

After the public key is obtained, ensure that the signature is verified.

```
public class RawDataVerifyExample {
    /**
     * Basic authentication information:
     * - ACCESS_KEY: access key of the Huawei Cloud account
     * - SECRET_ACCESS_KEY: Huawei Cloud account secret access key, which is sensitive information. Store
     this in ciphertext.
     * - IAM_ENDPOINT: endpoint for accessing IAM. For details, see https://developer.huaweicloud.com/intl/en-us/endpoint?IAM.
     * - KMS_REGION_ID: regions supported by KMS. For details, see https://developer.huaweicloud.com/intl/en-us/endpoint?DEW.
     * - KMS_ENDPOINT: endpoint for accessing KMS. For details, see https://developer.huaweicloud.com/intl/en-us/endpoint?DEW.
     */
    private static final String ACCESS_KEY = System.getenv("HUAWEICLOUD_SDK_AK");
    private static final String SECRET_ACCESS_KEY = System.getenv("HUAWEICLOUD_SDK_SK");
    private static final String IAM_ENDPOINT = "https://<IamEndpoint>";
    private static final String KMS_REGION_ID = "<RegionId>";
    private static final String KMS_ENDPOINT = "https://<KmsEndpoint>";

    private static final int SALT_LENGTH = 32;
    private static final int TRAILER_FIELD = 1;
    public static final String RSA_PUBLIC_KEY_BEGIN = "-----BEGIN PUBLIC KEY-----\n";
}
```

```
public static final String RSA_PUBLIC_KEY_END = "-----END PUBLIC KEY-----";

// Sample signature data in Base64 encoding format. The original text is 1234.
private static final String RWA_DATA = "MTIzNA==";

// Signature value obtained through the sign API of KMS
private static final String SIGN = "xxx";
public static void main(String[] args) throws Exception {

    final String keyId = args[0];

    publicKeyVerify(keyId);
}
public static void publicKeyVerify(String keyId) throws Exception {

    // 1. Prepare the authentication information for accessing HUAWEI CLOUD.
    final BasicCredentials auth = new BasicCredentials()
        .withIamEndpoint(IAM_ENDPOINT).withAk(ACCESS_KEY).withSk(SECRET_ACCESS_KEY);

    // 2. Initialize the SDK and transfer the authentication information and the address for the KMS to
    access the client.
    final KmsClient kmsClient = KmsClient.newBuilder()
        .withRegion(new Region(KMS_REGION_ID, KMS_ENDPOINT)).withCredential(auth).build();

    // 3. Obtain the public key information. The returned information is in PKCS8 format.
    final ShowPublicKeyRequest showPublicKeyRequest = new ShowPublicKeyRequest()
        .withBody(new OperateKeyRequestBody().withKeyId(keyId));
    final ShowPublicKeyResponse showPublicKeyResponse =
kmsClient.showPublicKey(showPublicKeyRequest);

    // 4. Obtain the public key string.
    final String publicKeyStr = showPublicKeyResponse.getPublicKey().replace(RSA_PUBLIC_KEY_BEGIN, "")
        .replaceAll("\n", "").replace(RSA_PUBLIC_KEY_END, "");

    // 5. Parse the public key.
    final X509EncodedKeySpec keySpec = new
X509EncodedKeySpec(Base64.getDecoder().decode(publicKeyStr));
    final KeyFactory keyFactory = KeyFactory.getInstance("RSA", new BouncyCastleProvider());
    final PublicKey publicKey = keyFactory.generatePublic(keySpec);

    // 6. Verify the signature.
    final Signature signature = getSignature();
    signature.initVerify(publicKey);
    signature.update(commonHash(Base64.getDecoder().decode(RWA_DATA)));

    // 7. Obtain the verification result.
    assert signature.verify(Base64.getDecoder().decode(SIGN));

}
private static Signature getSignature() throws Exception {
    Signature signature= Signature.getInstance("NONEwithRSASSA-PSS", new BouncyCastleProvider());
    MGF1ParameterSpec mgfParam = new MGF1ParameterSpec("SHA256");
    PSSParameterSpec pssParam = new PSSParameterSpec("SHA256", "MGF1", mgfParam, SALT_LENGTH,
TRAILER_FIELD);
    signature.setParameter(pssParam);
    return signature;
}
private static byte[] commonHash(byte[] data) {
    byte[] digest;
    try {
        MessageDigest md = MessageDigest.getInstance("SHA256",
BouncyCastleProvider.PROVIDER_NAME);
        md.update(data);
        digest = md.digest();
    } catch (Exception e) {
        throw new RuntimeException("Digest failed.");
    }
    return digest;
}
```

```
}  
}
```

1.25 Does an Imported Key Support Rotation?

Imported keys do not support rotation. After the imported key materials are deleted, ensure that the same key materials are imported.

1.26 Does KMS Support Offline Data Encryption and Decryption?

Generally, KMS provides open APIs **encrypt-data** and **decrypt-data** for encrypting and decrypting a small volume of data. The calculation of the APIs is based on KMS, which wraps the ciphertext. So offline data encryption and decryption are not supported.

However, for asymmetric keys, KMS does not wrap the ciphertext. So public keys can be encrypted offline while private keys are decrypted online.

The following shows an example:

RSA_3072 is used for **ENCRYPT_DECRYPT**. After a public key is used to encrypt "*hello world!*" offline, **decrypt-data** is called to decrypt the message using a private key. The RSA/ECB/OAEPWithSHA-256AndMGF1Padding algorithm is used.

```
public class RsaEncryptDataExample {  
    /**  
     * Basic authentication information:  
     * - ACCESS_KEY: Access key of the Huawei Cloud account. For details, see How Do I Obtain an Access Key \(AK/SK\)?.  
     * - SECRET_ACCESS_KEY: Secret access key of the Huawei Cloud account. This is sensitive information. Store it in ciphertext. For details, see How Do I Obtain an Access Key \(AK/SK\)?.  
     * - IAM_ENDPOINT: Endpoint for accessing IAM. For details, see Regions and Endpoints.  
     * - KMS_REGION_ID: Regions supported by KMS. For details, see Regions and Endpoints.  
     * - KMS_ENDPOINT: Endpoint for accessing KMS. For details, see Regions and Endpoints.  
     * - There will be security risks if the AK/SK used for authentication is directly written into code. Encrypt the AK/SK in the configuration file or environment variables for storage.  
     * - In this example, the AK/SK stored in the environment variables are used for identity authentication. Configure the environment variables HUAWEICLOUD_SDK_AK and HUAWEICLOUD_SDK_SK in the local environment first.  
     */  
    private static final String ACCESS_KEY = System.getenv("HUAWEICLOUD_SDK_AK");  
    private static final String SECRET_ACCESS_KEY = System.getenv("HUAWEICLOUD_SDK_SK");  
    private static final String IAM_ENDPOINT = "https://<IamEndpoint>";  
    private static final String KMS_REGION_ID = "<RegionId>";  
    private static final String KMS_ENDPOINT = "https://<KmsEndpoint>";  
  
    private static final String RSA_PUBLIC_KEY_BEGIN = "-----BEGIN PUBLIC KEY-----\n";  
    private static final String RSA_PUBLIC_KEY_END = "-----END PUBLIC KEY-----";  
  
    private static final String RSAES_OAEP_SHA_256 = "RSA/ECB/OAEPWithSHA-256AndMGF1Padding";  
  
    private static final String SHA_256 = "SHA-256";  
  
    private static final String MGF1 = "MGF1";  
  
    private static final String HELLO_WORLD = "hello world!";  
  
    public static void main(String[] args) throws Exception {  
        final String keyId = args[0];
```

```
        publicKeyEncrypt(keyId);
    }

    private static void publicKeyEncrypt(String keyId) throws NoSuchAlgorithmException,
InvalidKeySpecException,
        NoSuchPaddingException, InvalidAlgorithmParameterException, InvalidKeyException,
        IllegalBlockSizeException, BadPaddingException {

        // 1. Prepare the authentication information for accessing Huawei Cloud.
        final BasicCredentials auth = new BasicCredentials()
            .withIamEndpoint(IAM_ENDPOINT).withAk(AccessKey.ACCESS_KEY).withSk(SecretKey.ACCESS_KEY);

        // 2. Initialize the SDK and transfer the authentication information and the address for the KMS to
        // access the client.
        final KmsClient kmsClient = KmsClient.newBuilder()
            .withRegion(new Region(KMS_REGION_ID, KMS_ENDPOINT)).withHttpConfig(new HttpConfig()
                .withIgnoreSSLVerification(true)).withCredential(auth).build();

        // 3. Obtain the public key information. The returned information is in PKCS8 format.
        final ShowPublicKeyRequest showPublicKeyRequest = new ShowPublicKeyRequest()
            .withBody(new OperateKeyRequestBody().withKeyId(keyId));
        final ShowPublicKeyResponse showPublicKeyResponse =
            kmsClient.showPublicKey(showPublicKeyRequest);

        // 4. Obtain the public key string.
        final String publicKeyStr = showPublicKeyResponse.getPublicKey().replace(RSA_PUBLIC_KEY_BEGIN, "")
            .replaceAll("\n", "").replace(RSA_PUBLIC_KEY_END, "");

        // 5. Obtain the binary public key.
        final X509EncodedKeySpec keySpec = new
X509EncodedKeySpec(Base64.getDecoder().decode(publicKeyStr));
        final KeyFactory keyFactory = KeyFactory.getInstance("RSA", new BouncyCastleProvider());
        final PublicKey publicKey = keyFactory.generatePublic(keySpec);

        // 6. Encrypt the string "hello world!" offline using a public key.
        final Cipher cipher = Cipher.getInstance(RSAES_OAEP_SHA_256);
        final OAEPParameterSpec oaepParameterSpec = new OAEPParameterSpec(SHA_256, MGF1,
            new MGF1ParameterSpec(SHA_256), PSource.PSpecified.DEFAULT);
        cipher.init(Cipher.ENCRYPT_MODE, publicKey, oaepParameterSpec);
        final byte[] cipherData = cipher.doFinal(HELLO_WORLD.getBytes(StandardCharsets.UTF_8));

        // 7. Decrypt the ciphertext online using a private key.
        final DecryptDataRequest decryptDataRequest = new DecryptDataRequest()
            .withBody(new DecryptDataRequestBody().withKeyId(keyId)
                .withEncryptionAlgorithm(DecryptDataRequestBody.EncryptionAlgorithmEnum.RSAES_OAEP
                _SHA_256)
                .withCipherText(Base64.getEncoder().encodeToString(cipherData)));

        final DecryptDataResponse decryptDataResponse = kmsClient.decryptData(decryptDataRequest);

        assert HELLO_WORLD.equals(decryptDataResponse.getPlainText());
    }
}
```

1.27 How Do I Convert an Original EC Private Key into a Private Key in PKCS8 Format?

Scenario

The EC private key is a large integer. However, in the key pair import scenario, the private key must be ASN.1-encoded and then the data must be encoded in binary

mode to obtain the DER format, which cannot be obtained by running the OpenSSL command.

This section describes how to convert a 256-bit EC private key into a private key in PKCS8 format.

Environment Preparations

- Create a Java environment and import bouncycastle 1.78 or later.
- Install OpenSSL 1.1.1m or later.

Converting a Private Key to a PKCS8 Object

The following uses a secp256k1 private key as an example. The original private key in hexadecimal format is as follows:

```
``DC23DA6E913444ABADCE2F42A3B7DC3958569948633EE80AEC46ACCA02523495``
```

NOTE

The private key is used as an example only. Do not use it in the actual environment.

Use the following code to convert the private key into a PKCS8 object:

```
``java
import org.bouncycastle.jcajce.provider.asymmetric.ec.BCECPrivateKey;
import org.bouncycastle.jcajce.provider.asymmetric.ec.BCECPublicKey;
import org.bouncycastle.jce.ECNamedCurveTable;
import org.bouncycastle.jce.interfaces.ECPrivateKey;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.bouncycastle.jce.spec.ECNamedCurveParameterSpec;
import org.bouncycastle.jce.spec.ECPrivateKeySpec;
import org.bouncycastle.jce.spec.ECPublicKeySpec;
import org.bouncycastle.math.ec.ECPoint;

import java.math.BigInteger;
import java.security.KeyFactory;
import java.security.NoSuchAlgorithmException;
import java.security.PublicKey;
import java.security.Security;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.InvalidParameterSpecException;
import java.util.Base64;

public class RawEcPrivateKeyToPKCS8Object {
    public static void main(String[] args)
        throws InvalidParameterSpecException, NoSuchAlgorithmException, InvalidKeySpecException {

        Security.addProvider(new BouncyCastleProvider());

        KeyFactory keyFactory = KeyFactory.getInstance("ECDSA", new BouncyCastleProvider());

        ECNamedCurveParameterSpec ecSpec = ECNamedCurveTable.getParameterSpec("secp256k1");
        BigInteger d = new
        BigInteger("DC23DA6E913444ABADCE2F42A3B7DC3958569948633EE80AEC46ACCA02523495", 16);
        ECPrivateKeySpec ecPrivateKeySpec = new ECPrivateKeySpec(d, ecSpec);
        BCECPrivateKey ec = new BCECPrivateKey("EC", ecPrivateKeySpec,
        BouncyCastleProvider.CONFIGURATION);

        ECPoint q = ecSpec.getG().multiply(((ECPrivateKey) ec).getD());
        ECPublicKeySpec pubSpec = new ECPublicKeySpec(q, ecSpec);
        PublicKey publicKey = keyFactory.generatePublic(pubSpec);

        BCECPrivateKey ec2 = new BCECPrivateKey("EC", ec.engineGetKeyParameters(), (BCECPublicKey)
```



```
publicKey,  
    ecPrivateKeySpec.getParams(), BouncyCastleProvider.CONFIGURATION);  
  
    System.out.println(Base64.getEncoder().encodeToString(ec2.getEncoded()));  
}  
}  
...
```

The output is as follows:

```
````ignorelang  
MIGNAgEAMBAGByqGSM49AgEGBSuBBAAKBHYwdAIBAQQg3CPabpE0RKutzi9Co7fcOVhWmUhjPugK7Easyg
JSNJWgBwYFK4EEAAqhRANCAAQWiYvQT8cyVJx3wN85fXw0c2Ppv3SEsgnDaB96rWlz6G2bf2WhBJVD/jf5zb
+5/oxgVIOYDe8EwqYtBwhIJ3Yh
````
```

Use the ASN.1 decoding tool:

```
````  
<SEQUENCE>
<INTEGER/>
<SEQUENCE>
<OBJECT_IDENTIFIER Comment="ANSI X9.62 public key type"
Description="ecPublicKey">1.2.840.10045.2.1</OBJECT_IDENTIFIER>
<OBJECT_IDENTIFIER Comment="SECG (Certicom) named elliptic curve"
Description="secp256k1">1.3.132.0.10</OBJECT_IDENTIFIER>
</SEQUENCE>
<OCTET_STRING>
<SEQUENCE>
<INTEGER>1</INTEGER>
<OCTET_STRING>0xDC23DA6E913444ABADCE2F42A3B7DC3958569948633EE80AEC46ACCA02523495</
OCTET_STRING>
<NODE Sign="a0">
<OBJECT_IDENTIFIER Comment="SECG (Certicom) named elliptic curve"
Description="secp256k1">1.3.132.0.10</OBJECT_IDENTIFIER>
</NODE>
<NODE Sign="a1">
<BIT_STRING
Bits="520">0x000416898BD04FC732549C77C0DF397D7C347363E9BF7484B209C3681F7AAD6973E86D9B7F6
5A1049543FE3179CDBFB9FE8C605483980DEF04C2A62D070848277621</BIT_STRING>
</NODE>
</SEQUENCE>
</OCTET_STRING>
</SEQUENCE>
````
```

Add the following content to the `ec_private_key.pem` file:

```
````ignorelang  
-----BEGIN PRIVATE KEY-----
MIGNAgEAMBAGByqGSM49AgEGBSuBBAAKBHYwdAIBAQQg3CPabpE0RKutzi9Co7fcOVhWmUhjPugK7Easyg
JSNJWgBwYFK4EEAAqhRANCAAQWiYvQT8cyVJx3wN85fXw0c2Ppv3SEsgnDaB96rWlz6G2bf2WhBJVD/jf5zb
+5/oxgVIOYDe8EwqYtBwhIJ3Yh
-----END PRIVATE KEY-----
````
```

Run the following commands to view the EC key information:

```
````shell  
openssl ec -in ec_private_key.pem -text
````  
````ignorelang  
read EC key
Private-Key: (256 bit)
priv:
dc:23:da:6e:91:34:44:ab:ad:ce:2f:42:a3:b7:dc:
39:58:56:99:48:63:3e:e8:0a:ec:46:ac:ca:02:52:
34:95
pub:
04:16:89:8b:d0:4f:c7:32:54:9c:77:c0:df:39:7d:
````
```

```
7c:34:73:63:e9:bf:74:84:b2:09:c3:68:1f:7a:ad:
69:73:e8:6d:9b:7f:65:a1:04:95:43:fe:31:79:cd:
bf:b9:fe:8c:60:54:83:98:0d:ef:04:c2:a6:2d:07:
08:48:27:76:21
ASN1 OID: secp256k1
writing EC key
-----BEGIN EC PRIVATE KEY-----
MHQCAQEEINwj2m6RNESrrc4vQqO33DlYVplIYz7oCuxGrMoCUjSVoAcGBSuBBAK
oUQDQgAEFomL0E/HMlScd8DfOX18NHnj6b90hLIJw2gfeq1pc+htm39loQSVQ/4x
ec2/uf6MYFSDmA3vBMKmLQclSCd2IQ==
-----END EC PRIVATE KEY-----

...

```

If the commands can be executed properly, the following **DER** command is generated:

```
```shell
openssl pkcs8 -topk8 -inform PEM -outform DER -in ec_private_key.pem -out ec_private_key.der -nocrypt```

```

# 2 CSMS Related

---

## 2.1 Why Cannot I Delete the Version Status of a Secret?

`SYSCURRENT` and `SYSPREVIOUS` are preconfigured statuses and cannot be deleted.

## 2.2 Why Is the Rotation Period Set for RDS Secrets Inconsistent with the Actual Rotation Period?

When RDS secret rotation is added, the scheduled task is triggered once an hour and does not take effect immediately. Therefore, the rotation time may be one hour later than the expected time.

## 2.3 What Can I Do If "The API does not exist or has not been published in the environment" Is Displayed When I Rotate TaurusDB Secrets?

### Symptom



When the TaurusDB secret rotation is enabled, the error message "The API does not exist or has not been published in the environment" is displayed.

### Possible Causes

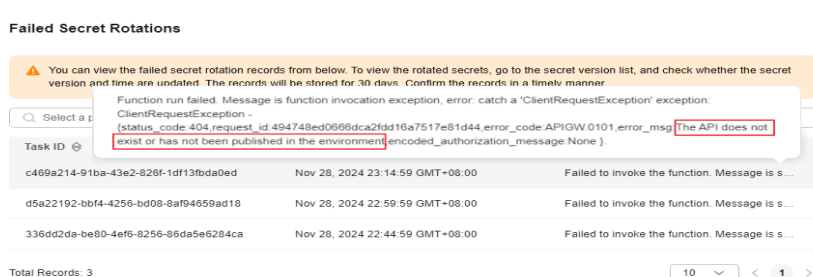
The domain name address in the FunctionGraph rotation function is incorrect.

### Solution

**Step 1** [Log in to the management console.](#)

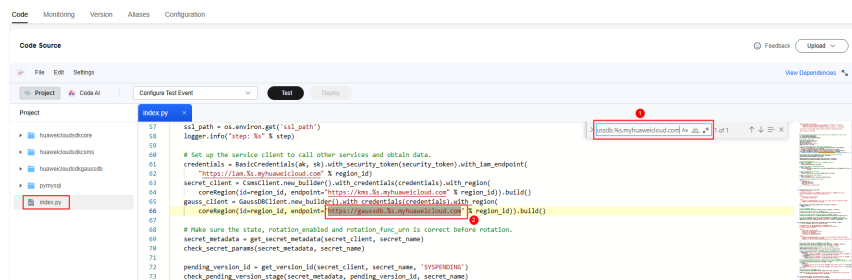
- Step 2** Click  in the upper left corner and select a region or project.
- Step 3** Click  on the left of the page and choose **Security & Compliance > Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service > Secrets**.
- Step 5** In the **Secrets**, locate the target secret and click the secret name to go to the secret details page.
- Step 6** In the **Version** area, click the number next to **Failed rotations** and check whether the secret rotation failure record contains **The API does not exist or has not been published in the environment**. If yes, go to the next step.

**Figure 2-1** Viewing the cause of the secret rotation failure



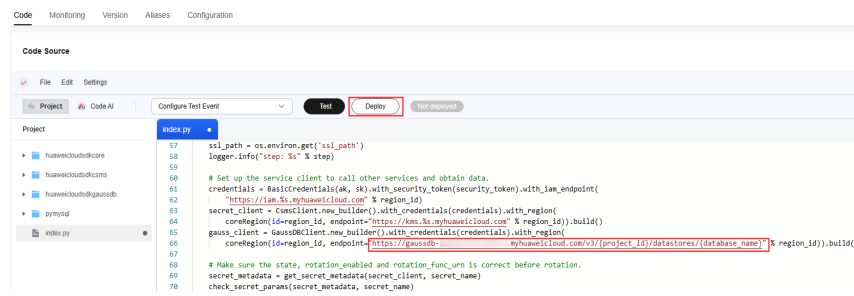
- Step 7** Return to the secret details page. In the secret information area, click the FunctionGraph rotate function to go to the FunctionGraph console.
- Step 8** Locate the **index.py** file and search for **https://gaussdb.%s.myhuaweicloud.com** in the code source.

**Figure 2-2** Editing the index.py file



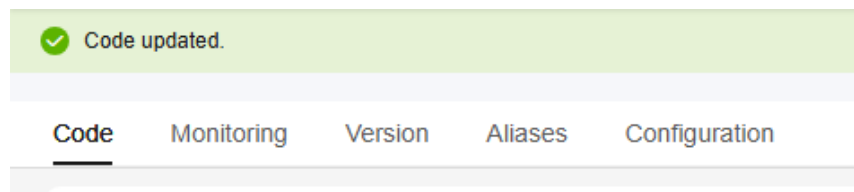
- Step 9** Call the TaurusDB API to **obtain the database engine version** and copy the TaurusDB database domain name in the current region.
- Step 10** Replace **https://gaussdb.%s.myhuaweicloud.com** in the **Step 8 index.py** file with the copied domain name and click **Deploy**.

**Figure 2-3** Changing the domain name



When the message **Code updated** is displayed on the FunctionGraph console, the modification is successful.

**Figure 2-4** Code updated



----End

## Follow-up Operations



**Log in to the management console**, choose **Cloud Secret Management Service** > **Secrets**, locate the target **TaurusDB secret**, and enable the rotation function again to check whether the operation is successful.

# 3 KPS Related

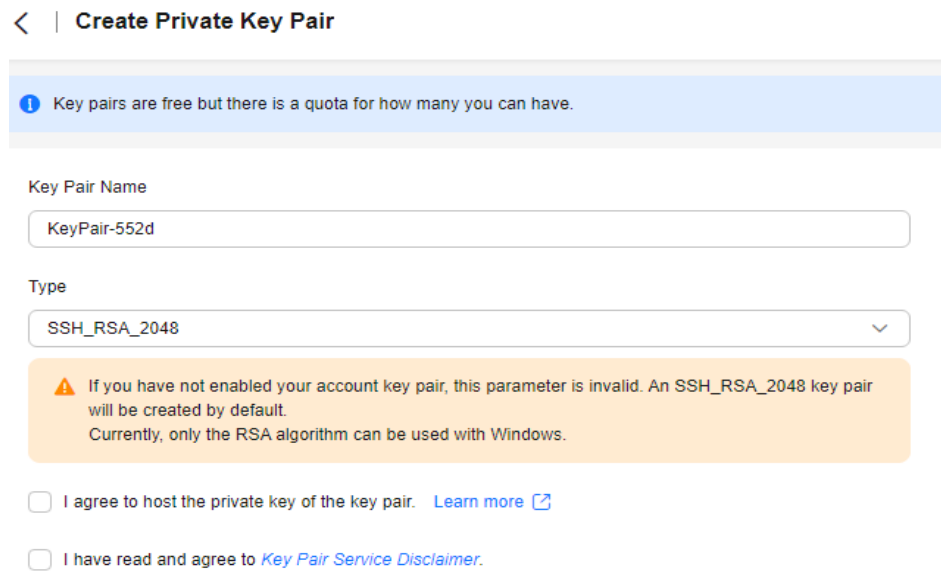
---

## 3.1 How Do I Create a Key Pair?

### Creating a Key Pair Using the Management Console

- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, click **Key Pair Service**.
- Step 5** In the displayed **Private Key Pairs** tab, create a private key pair or an account key pair as required.
- Step 6** Click **Create Key Pair**. In the displayed dialog box, enter the key pair name, as shown in [Figure 3-1](#).

**Figure 3-1** Creating a key pair



**Step 7** (Optional) Select a key pair type. If no key pair is enabled for your account, an SSH\_RSA\_2048 key pair will be created by default.

**NOTE**

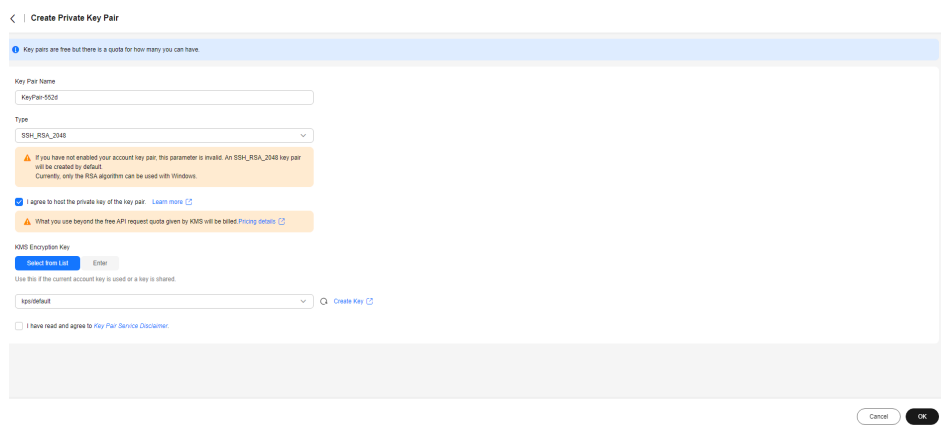
Currently, only the RSA algorithm can be used with Windows.

**Step 8** Read and select **I agree to host the private key of the key pair** if needed. Select an encryption key from the **KMS encryption** drop-down list box. Skip this step if not needed.

**NOTE**

- KPS encrypts private keys using the encryption key provided by KMS. When you use the KMS encryption function of the key pair, KMS creates a default key **kps/default** for you to use.
- For details about the custom keys created on KMS, see [Creating a Key](#).

**Figure 3-2** Managing private keys



**Step 9** Read the *Key Pair Service Disclaimer* and select **I have read and agree to the Key Pair Service Disclaimer**.

- Step 10** Click **OK**. The browser automatically downloads the private key. When the private key is downloaded, a dialog box is displayed.
- Step 11** Save the private key as prompted by the dialog box.

---

**NOTICE**

- If the private key is not managed, it can be downloaded only once. Keep it properly. If the private key is lost, you can bind a key pair to the ECS again by resetting the password or key pair. For details, see [How Do I Handle the Failure in Logging In to ECS After Unbinding the Key Pair?](#)
- If you have authorized Huawei Cloud to manage the private key, you can export the private key anytime as required.

- 
- Step 12** Click **OK**. After the key pair is created, you can view the information in the key pair list, including name, fingerprint, status, and private key.

 **NOTE**

After the key pair is created, download the private key to your local host and keep it securely.

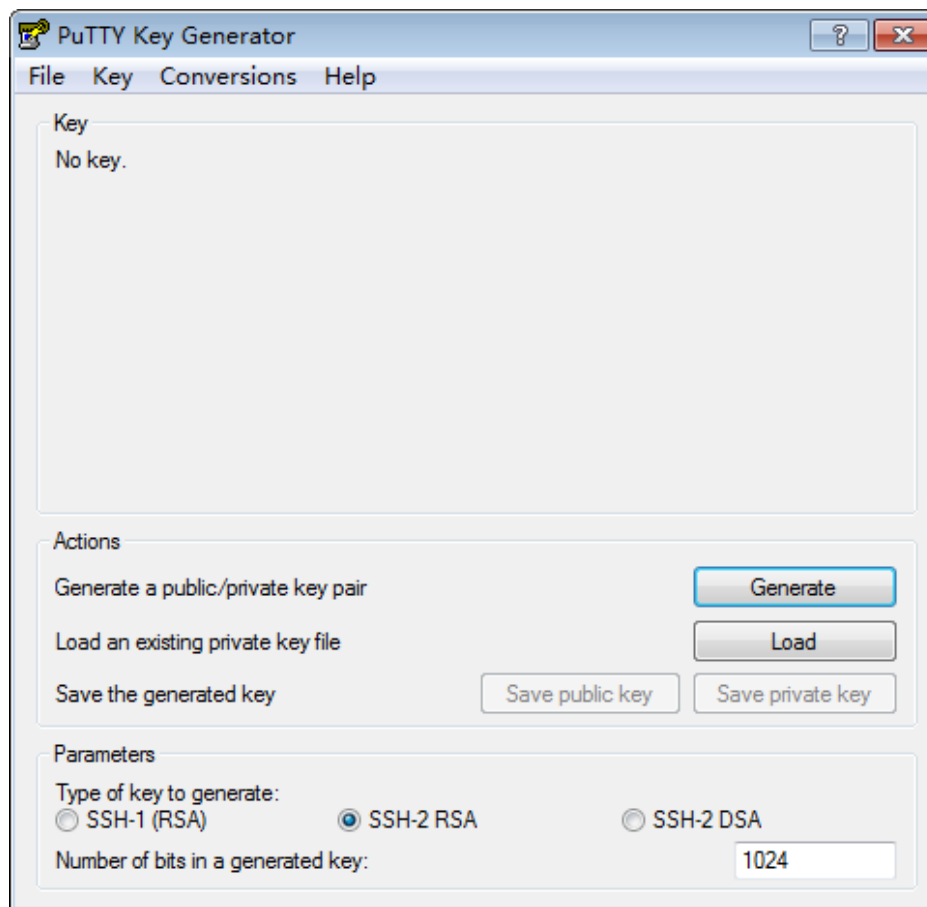
----End

## Creating a Key Pair Using PuTTYgen

- Step 1** Generate the public and private keys. Double-click **PuTTYgen.exe**. The **PuTTY Key Generator** page is displayed, as shown in [Figure 3-3](#).



**Figure 3-3** PuTTY Key Generator



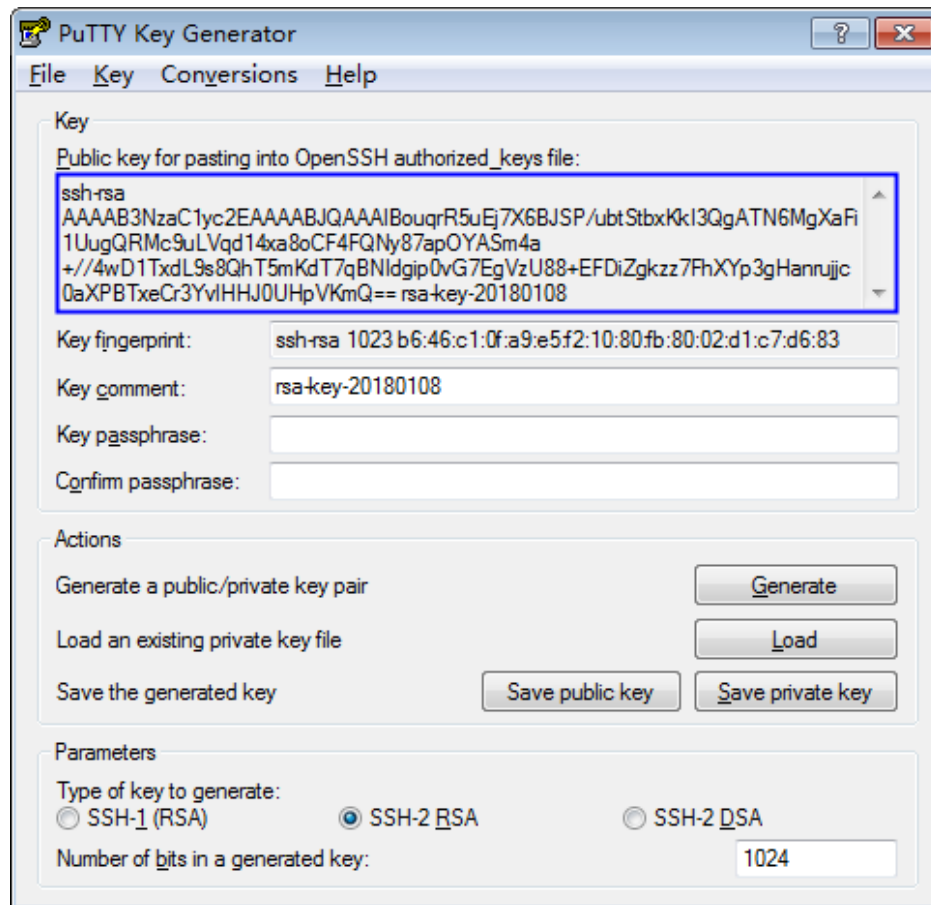
**Step 2** Configure the parameters as described in [Table 3-1](#).

**Table 3-1** Parameter description

Parameter	Description
Type of key to generate	Encryption and decryption algorithm of key pairs to be imported to the management console. Currently, only <b>SSH-2 RSA</b> is supported.
Number of bits in a generated key	Length of a key pair to be imported to the management console. Currently, the following length values are supported: <b>1024, 2048, and 4096</b> .

**Step 3** Click **Generate** to generate a public key and a private key. See [Figure 3-4](#). Contents highlighted by the blue-line box show a generated public key.

Figure 3-4 Obtaining the public and private keys



**Step 4** Copy the information in the blue square and save it in a local .txt file.

---

**NOTICE**

Do not save the public key by clicking **Save public key**. If you save a public key using **Save public key**, the public key format will be changed and cannot be imported to the management console directly.

**Step 5** Save the private key in PPK or PEM format.

---

**NOTICE**

For security purposes, the private key can only be downloaded once. Keep it secure.

---

**Table 3-2** Format of a private key file

Private Key File Format	Private Key Usage Scenario	Saving Method
PEM	<ul style="list-style-type: none"><li>• Use the Xshell tool to log in to the cloud server running the Linux operating system.</li><li>• Manage the private key on the management console.</li></ul>	<ol style="list-style-type: none"><li>1. Choose <b>Conversions &gt; Export OpenSSH key</b>.</li><li>2. Save the private key, for example, <b>kp-123.pem</b>, to a local directory.</li></ol>
	Obtain the password of a cloud server running the Windows operating system.	<ol style="list-style-type: none"><li>1. Choose <b>Conversions &gt; Export OpenSSH key</b>. <b>NOTE</b> Do not enter the <b>Key passphrase</b> information. Otherwise, the password fails to be obtained.</li><li>2. Save the private key, for example, <b>kp-123.pem</b>, to a local directory.</li></ol>
PPK	Use the PuTTY tool to log in to the cloud server running the Linux operating system.	<ol style="list-style-type: none"><li>1. On the <b>PuTTY Key Generator</b> page, choose <b>File &gt; Save private key</b>.</li><li>2. Save the private key, for example, <b>kp-123.ppk</b>, to a local directory.</li></ol>

After the public key and private key are correctly saved, you can import the key pair to the management console.

----End

## 3.2 What Are a Private Key Pair and an Account Key Pair?

A private key pair can be viewed or used only by the current account.

An account key pair can be viewed or used by all users under the account.

A private key pair can be upgraded to an account key pair. For details, see [Upgrading a Key Pair](#).

## 3.3 How Do I Handle an Import Failure of a Key Pair Created Using PuTTYgen?

### Symptom

When a key pair created using PuTTYgen was imported to the management console, the system displayed a message indicating that importing the public key failed.

### Possible Causes

The format of the public key content does not meet system requirements.

Storing a public key by clicking **Save public key** will change the format of the public key content. Importing such a public key will fail because the key does not pass the format verification by the system.

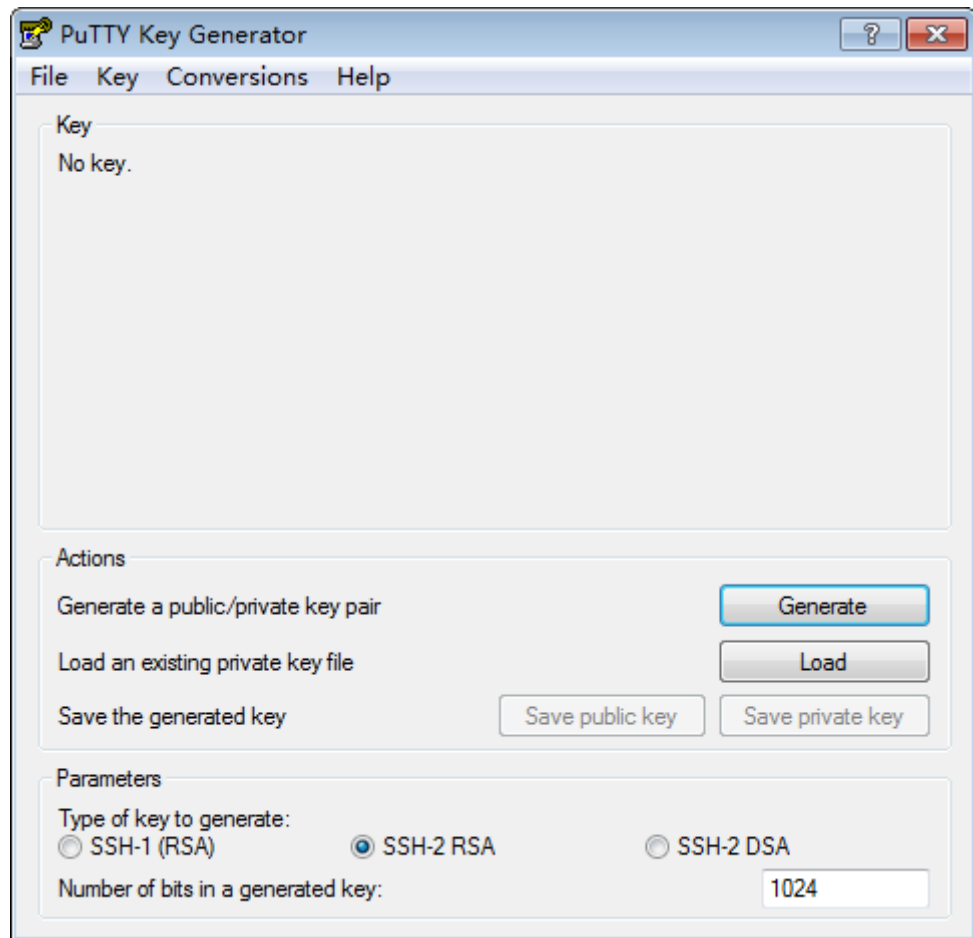
### Procedure

Use the locally stored private key and **PuTTY Key Generator** to restore the format of the public key content. Then, import the public key to the management console.

**Step 1** Restore the public key file in the correct format.

1. Double-click **PuTTYgen.exe**. The **PuTTY Key Generator** page is displayed, as shown in [Figure 3-5](#).

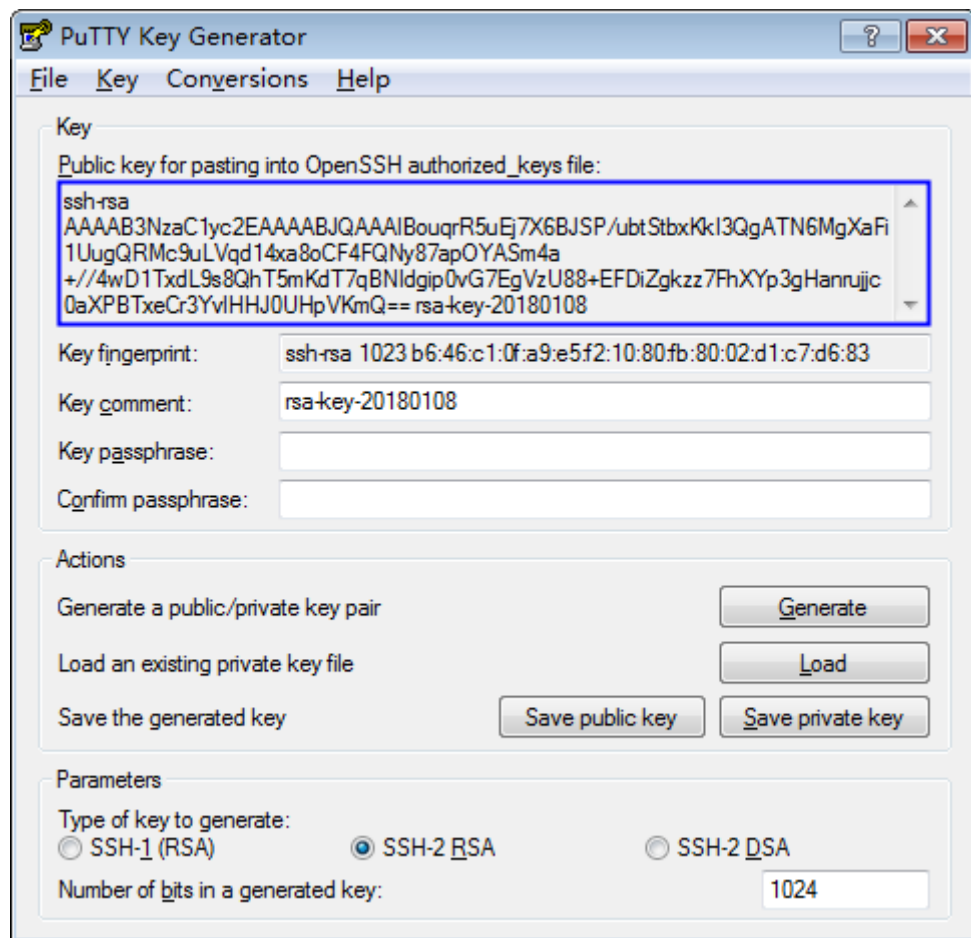
**Figure 3-5** Main interface of the PuTTY Key Generator



2. Click **Load** and select the private key.

The system automatically loads the private key and restores the format of the public key content in **PuTTY Key Generator**. The content in the red box in **Figure 3-6** is the public key with the format meeting system requirements.

**Figure 3-6** Restoring the format of the public key content




3. Copy the information in the blue square and save it in a local **.txt** file.

#### NOTICE

Do not save the public key by clicking **Save public key**. If you save a public key using **Save public key**, the public key format will be changed and cannot be imported to the management console directly.

**Step 2** Import the public key file in the correct format to the KPS console.

1. Log in to the management console.
2. Click  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.
3. In the navigation pane, click **Key Pair Service**.
4. On the **Key Pair Service** page, click **Import Key Pair**.
5. Click **Select File**, select the **.txt** public key file, or copy and paste the public key content to the text box of the public key content.
6. Click **OK** to import the public key file.


----End

## 3.4 What Should I Do When I Fail to Import a Key Pair Using Internet Explorer 9?

### Symptom

Importing a key pair may fail if Internet Explorer 9 is used.

### Procedure

- Step 1** Click  in the upper right corner of the browser.
  - Step 2** Select **Internet Options**.
  - Step 3** Click the **Security** tab in the displayed dialog box.
  - Step 4** Click **Internet**.
  - Step 5** If the security level indicates **Custom**, click **Default Level** to restore to the default settings.
  - Step 6** Move the scroll bar to set the security level to **Medium** and click **Apply**.
  - Step 7** Click **Custom Level**.
  - Step 8** Set **Initialize and script ActiveX controls not marked as safe for scripting** to **Prompt**.
  - Step 9** Click **Yes**.
- End

## 3.5 How Do I Log In to a Linux ECS with a Private Key?

### Scenario

After you create or import a key pair on the KMS console, set login mode to **Key Pair** when purchasing an ECS, and select the created or imported key pair.

After purchasing an ECS, you can use the private key of the key pair to log in to the ECS.

### Prerequisites

- The network connection between the login tool (such as PuTTY and XShell) and the target ECS is normal.
- You have bound an EIP to the ECS.
- You have obtained the private key file of the ECS.

### Logging In from a Windows Computer

To log in to the Linux ECS from a Windows computer, perform the operations described in this section.

### Method 1: Use PuTTY to log in to the ECS.

The following operations use PuTTY to log in to the ECS. Before logging in, you must obtain the private key format in the .ppk format.

**Step 1** Double-click **PuTTY.EXE**. The **PuTTY Configuration** page is displayed.

**Step 2** Choose **Connection > Data**. Enter the image username in **Auto-login username**.

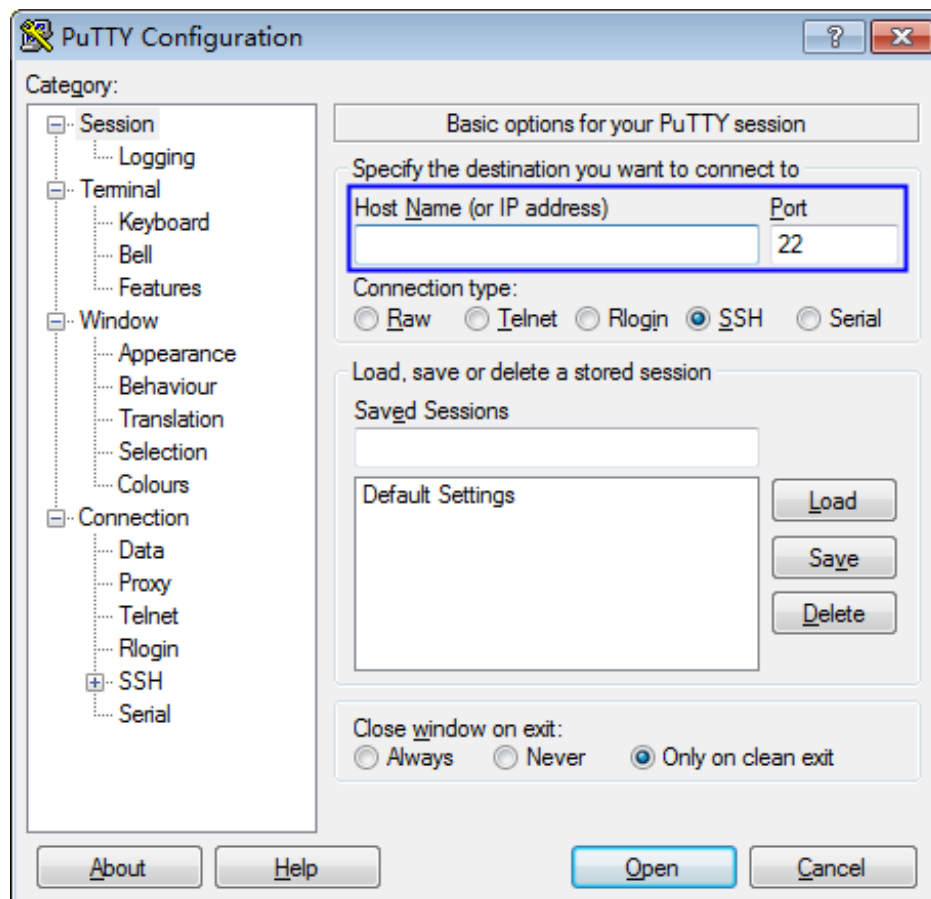
**NOTE**

- If the public image of the **CoreOS** is used, the username of the image is **core**.
- For a **non-CoreOS** public image, the username of the image is **root**.

**Step 3** Choose **Connection > SSH > Auth**. In **Private key file for authentication**, click **Browse** and select a private key file (in the .ppk format).

**Step 4** Click **Session** and enter the EIP of the ECS under **Host Name (or IP address)**.

**Figure 3-7** Configuring the EIP



**Step 5** Click **Open** to log in to the ECS.

----End

### Method 2: Use Xshell to log in to the ECS.

**Step 1** Start the Xshell tool.



**Step 2** Run the following command to remotely log in to the ECS through SSH:

```
ssh Username@EIP
```

An example command is provided as follows:

```
ssh root@192.168.1.1
```

**Step 3** (Optional) If the system displays the **SSH Security Warning** dialog box, click **Accept & Save**.

**Step 4** Select **Public Key** and click **Browse** next to the CMK text box.

**Step 5** In the displayed dialog box, click **Import**.

**Step 6** Select the locally stored key file (in the **.pem** format) and click **Open**.

**Step 7** Click **OK** to log in to the ECS.

----End

## Logging In from a Linux Computer

To log in to the Linux ECS from a Linux computer, perform the operations described in this section. The following procedure uses private key file **kp-123.ppk** as an example to log in to the ECS. The name of your private key file may differ.

**Step 1** On the Linux CLI, run the following command to change operation permissions:

```
chmod 600 /path/kp-123.ppk
```

 **NOTE**

In the preceding command, **path** is the path where the key file is saved.

**Step 2** Run the following command to log in to the ECS:

```
ssh -i /path/kp-123 root@EIP
```

 **NOTE**

- In the preceding command, **path** is the path where the key file is saved.
- *EIP* is the EIP bound to the ECS.

----End

## 3.6 How Do I Use a Private Key to Obtain the Password to Log In to a Windows ECS?

### Scenario

A password is required when you log in to a Windows ECS. First, obtain the administrator password generated during the initial installation of the ECS from the private key file downloaded when you create the ECS. The administrator password is the password of account **Administrator** or an account set in Cloudbase-init. This password is randomly generated, offering high security.

You can obtain the password for logging in to a Windows ECS through the management console

 **NOTE**


- After obtaining the initial password, you are advised to clear the password information recorded in the system to increase system security.  
Clearing the initial password information does not affect ECS operation or login. Once cleared, the password cannot be restored. Before deleting a password, record the password information. For details, see *Elastic Cloud Server User Guide*.
- You can also call the API to obtain the initial password of the Windows ECS. For details, see *Elastic Cloud Server API Reference*.

## Prerequisites

You have obtained the private key file in the .pem format for logging in to the ECS.

## Obtaining a Password

**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click . Under **Computing**, click **Elastic Cloud Server**.

**Step 4** In the ECS list, click the ECS whose password is to be obtained.

**Step 5** In the **Operation** column, click **More** and choose **Get Password**.

**Step 6** Use either of the following methods to obtain the password:

- Click **Select File** and upload the key file from a local directory.
- Copy the key file content to the text field.

**Step 7** Click **Get Password** to obtain a new random password.

----End

## 3.7 How Do I Handle the Failure in Binding a Key Pair?

### Symptom

Failed to bind the key pair to the ECS.

 **NOTE**

- The **Failed Key Pair Task** dialog box only records and displays failed key pair operations on ECSs, which do not affect the ECS status and subsequent operations. You can click **Delete** in the row of the failure record to delete it, or you can click **Delete All** to delete all failure records.
- Click **Learn more** to view related documents.

## Possible Causes

- An incorrect or invalid password has been provided.
- The permission or owner group of the public key file has been changed.
- SSH configuration of the ECS has been modified.
- The inbound direction of port 22 of the ECS security group is not open to 100.125.0.0/16.
- The ECS has been shut down, started, or a disk has been detached during the process of binding the key pair to the ECS.
- The network connection is faulty.
- Firewall rules have been configured for the ECS.

## Handling Procedure

**Step 1** Check the ECS status.

- If it is running, go to [Step 2](#).
- If it is shut down, go to [Step 5](#).

**Step 2** Use the password to log in to the ECS to check whether the password is correct.

- If it is correct, go to [Step 4](#).
- If it is incorrect, use the correct password to bind the key pair again.

**Step 3** Check whether the permission path and owner group of the `/root/.ssh/authorized_keys` file on the ECS have been modified.

- If yes, restore the permission to the following:
  - The owner group of each level has the `root:root` permission.
  - The permission for the `.ssh` file is 700.
  - The permission for `authorized_keys` is 600.
- If no, go to [Step 4](#).

**Step 4** Check whether the `/root/.ssh/authorized_keys` file of the ECS has been modified.

- If yes, restore the original content of the `/root/.ssh/authorized_keys` file based on the site requirements.
- If no, go to [Step 5](#).

**Step 5** Check whether the inbound direction of port 22 of the ECS security group is open to 100.125.0.0/16. That is, 100.125.0.0/16 can remotely connect to Linux ECSs through SSH.

- If yes, go to [Step 6](#).
- If no, add the following security group rule and bind the key pair again. For details about how to add a security group, see [Adding a Security Group Rule](#).

Direction	Protocol/ Application	Port	Source
Inbound	SSH (22)	22	100.125.0.0/16

**Step 6** Check whether the ECS can be powered on, shut down, and logged in to.

- If yes, bind the key pair again.
- If no, go to [Step 7](#).

**Step 7** Check whether the network is faulty.

- If yes, contact technical support to check and locate the fault.
- If no, bind the key pair again.

----End

## 3.8 How Do I Handle the Failure in Replacing a Key Pair?

### Symptom

Failed to replace the key pair on the ECS.

#### NOTE

The **Failed Key Pair Task** dialog box only records and displays failed key pair operations on ECSs, which do not affect the ECS status and subsequent operations. You can click **Delete** in the row of the failure record to delete it, or you can click **Delete All** to delete all failure records.

### Possible Causes

- An incorrect or invalid private key has been provided.
- The inbound direction of port 22 of the ECS security group is not open to 100.125.0.0/16.
- SSH configuration of the ECS has been modified.
- The ECS has been shut down, started, or a disk has been detached during the process of replacing the key pair.
- The network connection is faulty.
- Firewall rules have been configured for the ECS.

### Handling Procedure

**Step 1** Use the SSH key pair to log in to the ECS and check whether the private key is correct.

- If it is correct, go to [Step 2](#).
- If it is incorrect, use the correct private key to replace the key pair again.

**Step 2** Check whether the `/root/.ssh/authorized_keys` file of the ECS has been modified.

- If yes, restore the original content of the `/root/.ssh/authorized_keys` file based on the site requirements.
- If no, go to [Step 3](#).

**Step 3** Check whether the inbound direction of port 22 of the ECS security group is open to 100.125.0.0/16. That is, 100.125.0.0/16 can remotely connect to Linux ECSs through SSH.

- If yes, go to [Step 4](#).
- If no, add the following security group rule and replace the key pair again.

Direction	Protocol/ Application	Port	Source
Inbound	SSH (22)	22	100.125.0.0/16

**Step 4** Check whether the ECS can be powered on, shut down, and logged in to.

- If yes, replace the key pair again.
- If no, go to [Step 5](#).

**Step 5** Check whether the network is faulty.

- If yes, contact technical support to check and locate the fault.
- If no, replace the key pair again.

----End

## 3.9 How Do I Handle the Failure in Resetting a Key Pair?

### Symptom

Failed to reset the key pair on the ECS.

#### NOTE

The **Failed Key Pair Task** dialog box only records and displays failed key pair operations on ECSs, which do not affect the ECS status and subsequent operations. You can click **Delete** in the row of the failure record to delete it, or you can click **Delete All** to delete all failure records.

### Possible Causes

- The inbound direction of port 22 of the ECS security group is not open to 100.125.0.0/16.
- The ECS has been shut down, started, or a disk has been detached during the process of resetting the key pair.
- The network connection is faulty.
- Firewall rules have been configured for the ECS.

### Handling Procedure

**Step 1** Check whether the inbound direction of port 22 of the ECS security group is open to 100.125.0.0/16. That is, 100.125.0.0/16 can remotely connect to Linux ECSs through SSH.

- If yes, go to [Step 2](#).
- If no, add the following security group rule and reset the key pair again.

Direction	Protocol/ Application	Port	Source
Inbound	SSH (22)	22	100.125.0.0/16

**Step 2** Check whether the ECS can be powered on, shut down, and logged in to.

- If yes, reset the key pair again.
- If no, go to [Step 3](#).

**Step 3** Check whether the network is faulty.

- If yes, contact technical support to check and locate the fault.
- If no, reset the key pair again.

----End

## 3.10 How Do I Handle the Failure in Unbinding a Key Pair?

### Symptom

Failed to unbind the key pair from the ECS.

#### NOTE

The **Failed Key Pair Task** dialog box only records and displays failed key pair operations on ECSs, which do not affect the ECS status and subsequent operations. You can click **Delete** in the row of the failure record to delete it, or you can click **Delete All** to delete all failure records.

### Possible Causes

- An incorrect or invalid private key has been provided.
- The inbound direction of port 22 of the ECS security group is not open to 100.125.0.0/16.
- SSH configuration of the ECS has been modified.
- The ECS has been shut down, started, or a disk has been detached during the process of unbinding the key pair from the ECS.
- The network connection is faulty.
- Firewall rules have been configured for the ECS.

### Handling Procedure

**Step 1** Check the ECS status.

- If it is running, go to [Step 2](#).
- If it is shut down, go to [Step 4](#).

**Step 2** Use the SSH key pair to log in to the ECS and check whether the private key is correct.

- If it is correct, go to [Step 4](#).
- If it is incorrect, use the correct private key to unbind the key pair again.

**Step 3** Check whether the `/root/.ssh/authorized_keys` file of the ECS has been modified.

- If yes, restore the original content of the `/root/.ssh/authorized_keys` file.
- If no, go to [Step 4](#).

**Step 4** Check whether the inbound direction of port 22 of the ECS security group is open to 100.125.0.0/16. That is, 100.125.0.0/16 can remotely connect to Linux ECSs through SSH.

- If yes, go to [Step 5](#).
- If no, add the following security group rule and unbind the key pair again.

Direction	Protocol/ Application	Port	Source
Inbound	SSH (22)	22	100.125.0.0/16

**Step 5** Check whether the ECS can be powered on, shut down, and logged in to.

- If yes, unbind the key pair again.
- If no, go to [Step 6](#).

**Step 6** Check whether the network is faulty.

- If yes, contact technical support to check and locate the fault.
- If no, unbind the key pair again.

----End

## 3.11 Do I Need to Restart Servers After Replacing Its Key Pair?

No. Key pair replacement does not affect services.

## 3.12 How Do I Enable the Password Login Mode for an ECS?

If you disable the password login mode when binding a key pair to an ECS, you can enable the password login mode again later when you need to.

### Procedure

The following example describes how to log in to the ECS using PuTTY and enable the password login mode.

**Step 1** Double-click **PuTTY.EXE**. The **PuTTY Configuration** page is displayed.

**Step 2** Choose **Connection > Data**. Enter the image username in **Auto-login username**.

 NOTE

- If the public image of the **CoreOS** is used, the username of the image is **core**.
- For a **non-CoreOS** public image, the username of the image is **root**.

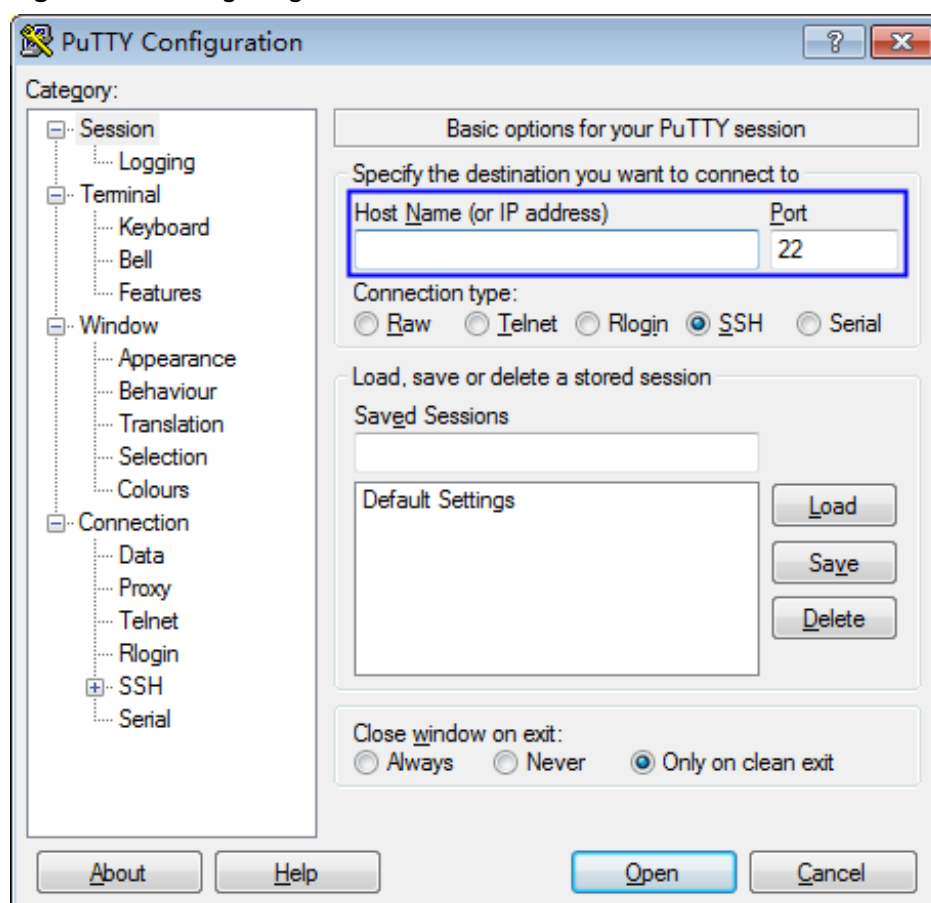
**Step 3** Choose **Connection > SSH > Auth**. In **Private key file for authentication**, click **Browse** and select a private key file (in the **.ppk** format).

 NOTE

If the file is in the **.pem** format, convert it by referring to [Converting the Private Key File in the .pem Format to the .ppk Format](#).

**Step 4** Click **Session** and enter the EIP of the ECS under **Host Name (or IP address)**.

**Figure 3-8** Configuring the EIP



**Step 5** Click **Open** to log in to the ECS.

**Step 6** Run the following command to open the **/etc/ssh/sshd\_config** file:

```
vi /etc/ssh/sshd_config
```

**Step 7** Press **i** to enter the editing mode and enable the password login mode.

- For a non-SUSE operating system, change the value of **PasswordAuthentication** to **yes**.  
PasswordAuthentication yes
- For a SUSE operating system, change the values of **PasswordAuthentication** and **UsePAM** to **yes**.



```
PasswordAuthentication yes
UsePAM yes
```

**NOTE**

- Non-SUSE OS  
To disable password login, change the value of **PasswordAuthentication** to **no**. If the **PasswordAuthentication** parameter is not contained in the `/etc/ssh/sshd_config` file, add it and set it to **no**.
- SUSE OS  
To disable password login, change the values of **PasswordAuthentication** and **UsePAM** to **no**. If the file does not contain the **PasswordAuthentication** and **UsePAM** parameters, add the parameters and set the values to **no**.

**Step 8** Press **Esc** to exit the editing mode.

**Step 9** Enter `:wq` and press **Enter** to save and exit.

**Step 10** Run the following command to restart the SSH service for the configuration to take effect:

- Non-Ubuntu14.xx OS  
**service sshd restart**
- Ubuntu14.xx OS  
**service ssh restart**

----End

## 3.13 How Do I Handle the Failure in Logging In to ECS After Unbinding the Key Pair?

### Symptom

- If the login mode is set to **Key Pair** when purchasing an ECS, after I unbind the initial password, I do not have the password or key pair to log in to the ECS. How can I solve this problem?
- When I bind a key pair to the ECS on the KPS management console, I disabled the password login mode. After the key pair is unbound, I have no password and key pair to log in to the ECS. How can I solve this problem?

### Procedure



#### Method 1: resetting the password

Reset the password on the ECS console and log in to the ECS using the password. For details, see *Elastic Cloud Server User Guide*.

#### Method 2: resetting the key pair

Shut down the ECS, bind the key pair to the ECS on the KPS console, and use the key pair to log in to the ECS. The procedure is as follows:

**Step 1** [Log in to the management console](#).

- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.
- Step 4** Click **ECS List** to view ECSs. For details, see [Figure 3-9](#).

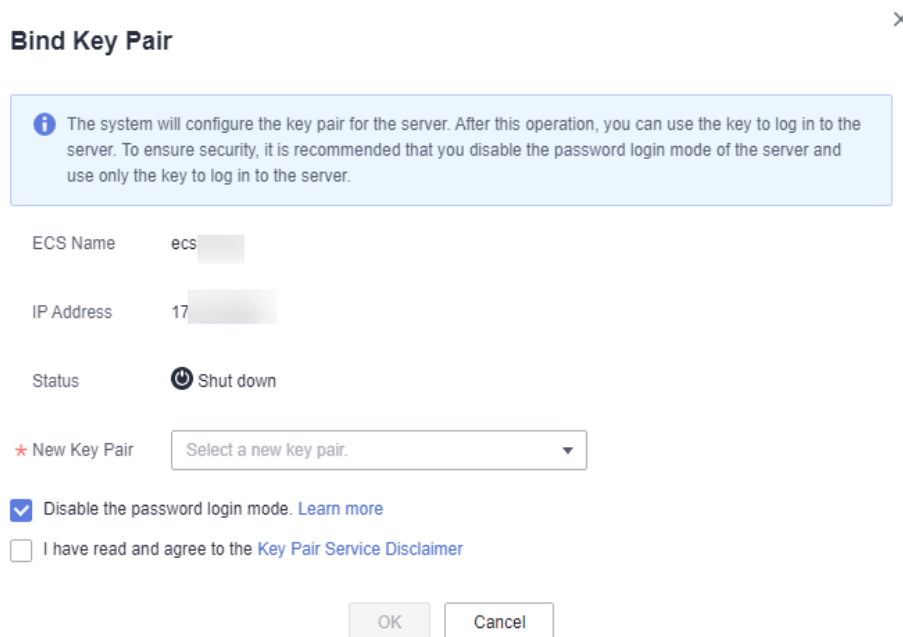
**Figure 3-9** ECS list



ECS Name/ID	Status	Private IP Address	Elastic IP Address	Associated Key Pair	Operation
ecs-windows 0643b313-8b1e-4fe2-873a-1b03053bfc6	Running	192.168.0.231	--	--	Bind
ecs-pwd3 2625c514-7a29-4b50-a13e-a591610ded9c	Shut down	192.168.0.95	--	--	Bind
ecs-euler 984e162e-7f4b-4564-93dc-90043a5dfb8d	Running	192.168.0.27	--	keypair	Replace Reset

- Step 5** Click the target ECS name to go to the details page.
- Step 6** Click **Shut Down** in the upper right corner of the page.
- Step 7** Return to the ECS list page by referring to step [Step 5](#).
- Step 8** Locate the target ECS and click **Bind**.
- Step 9** Select a new key pair from the drop-down list box of **New Key Pair**.

**Figure 3-10** Binding a key pair




**Bind Key Pair** ×

**i** The system will configure the key pair for the server. After this operation, you can use the key to log in to the server. To ensure security, it is recommended that you disable the password login mode of the server and use only the key to log in to the server.

ECS Name: ecs

IP Address: 17

Status:  Shut down

\* New Key Pair:

Disable the password login mode. [Learn more](#)

I have read and agree to the [Key Pair Service Disclaimer](#)

- Step 10** You can choose whether to disable the password login mode as necessary. By default, the password login mode is disabled.

 **NOTE**

- If you do not disable the password login mode, you can use the password or the key pair to log in to the ECS.
- If the password login mode is disabled, you can use only the key pair to log in to the ECS. If you need to use the password login mode later, you can enable the password login mode again. For details, see [How Do I Enable the Password Login Mode for an ECS?](#)

**Step 11** Read and select **I have read and agree to the Key Pair Service Disclaimer**.

**Step 12** Click **OK**. The key pair is bound. You can use the key pair to log in to the ECS.

----End

## 3.14 What Should I Do If My Private Key Is Lost?

### For Private Key Managed in KPS

You can export the private key from KPS again.

### For Private Key Not Managed in KPS

The private key cannot be retrieved.

You can bind a key pair to the ECS again by resetting the password or key pair. For details, see .

## 3.15 How Do I Convert the Format of a Private Key File?

### Converting the Private Key File in the .ppk Format to the .pem Format

The private key to be uploaded or copied to the text box must be in the .pem format. If the file is in the .ppk format, perform the following steps:

**Step 1** Visit the following website and download PuTTY and PuTTYgen:

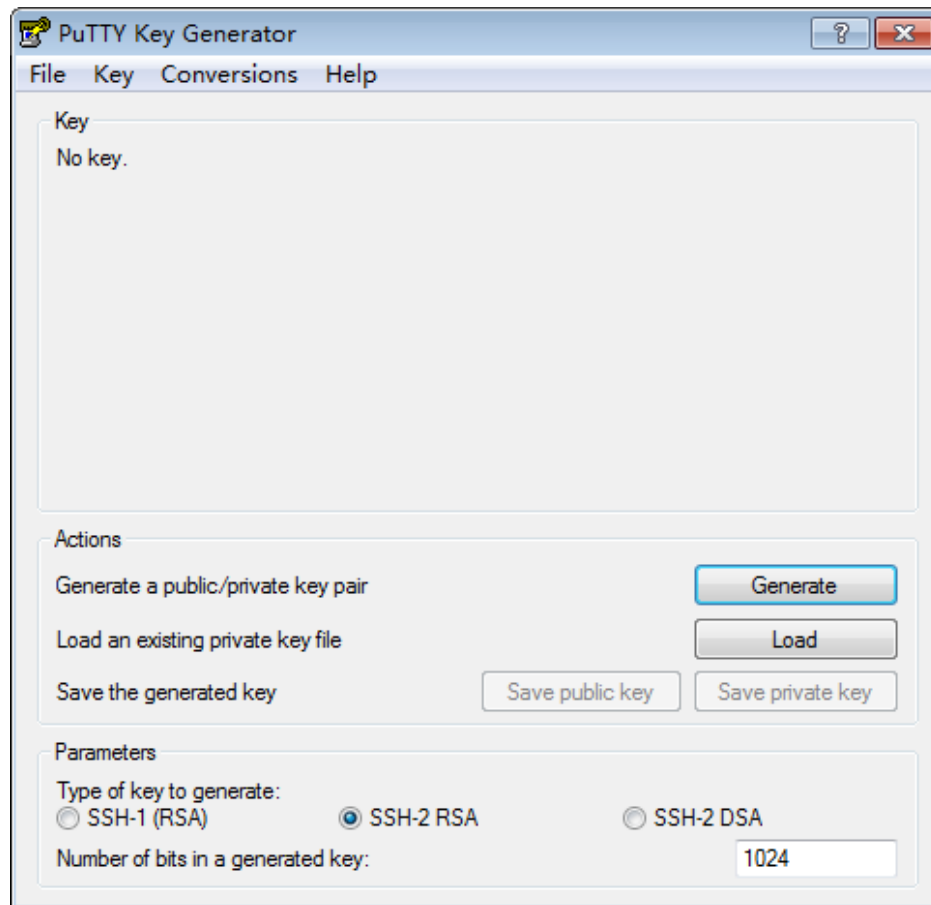
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

 **NOTE**

PuTTYgen is a private key generator, which is used to create a key pair that consists of a public key and a private key for PuTTY.

**Step 2** Double-click **PuTTYGEN.exe**. The **PuTTY Key Generator** page is displayed, as shown in [Figure 3-11](#).

**Figure 3-11** PuTTY Key Generator



- Step 3** Choose **Conversions > Import Key** to import the private key file in the **.ppk** format.
  - Step 4** Choose **Conversions > Export OpenSSH Key**, the **PuTTYgen Warning** dialog box is displayed.
  - Step 5** Click **Yes** to save the file in the **.pem** format.
- End

### Converting the Private Key File in the .pem Format to the .ppk Format

When you use PuTTY to log in to a Linux ECS, the private key must be in the .ppk format. If the file is in .pem format, perform the following steps to convert its format:

- Step 1** Visit the following website and download PuTTY and PuTTYgen:  
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

**NOTE**

PuTTYgen is a private key generator, which is used to create a key pair that consists of a public key and a private key for PuTTY.

- Step 2** Double-click **PuTTYgen.exe**. The **PuTTY Key Generator** window is displayed.

**Step 3** In the **Actions** area, click **Load** and import the private key file that you stored when purchasing the ECS.

Ensure that the private key file format is included in **All files (\*.\*)**.

**Step 4** Click **Save private key**.

**Step 5** Save the converted private key, for example, **kp-123.ppk**, to a local directory.

----End

## 3.16 Can I Change the Key Pair of a Server?

Yes.

You can unbind, reset, and replace the key pair bound to the ECS. For details, see [Managing Key Pairs](#).

## 3.17 Can a Key Pair Be Shared by Multiple Users?

Key pairs cannot be shared across accounts, but can be shared by the IAM users under the same account in either of the following ways:

- Import a key pair. To let multiple IAM users use the same key pair, you can create a key pair (by using PuTTYgen or other tools) and import it as an IAM user resource. For details, see [Importing a Key Pair](#).
- Upgrade a private key pair to an account key pair. You can upgrade a key pair created on the management console by referring to [Creating a Key Pair Using the Management Console](#). Or you can upgrade a created key pair by referring to [Upgrading a Key Pair](#).

## 3.18 How Do I Obtain the Public or Private Key File of a Key Pair?

### Obtaining a Private Key File

When you [create a key pair](#), your private key file will be automatically downloaded.

- If the private key is not managed, it cannot be downloaded later. Keep it properly.
- If you have authorized Huawei Cloud to manage private keys, you can export the managed private keys. For details, see [Exporting a Private Key](#).

### Obtaining a Public Key File

- If a key pair is created on the management console, its public key is automatically stored in Huawei Cloud. You can press **F12** to refresh the key pair list, and make a note of the **public\_key** field in the list.
- If a key pair was created using PuTTYgen, you can find its public key in the storage path on your local PC.

## 3.19 What Can I Do If an Error Is Reported When an Account Key Is Created or Upgraded for the First Time?

### Creating an Account Key Pair for the First Time

When creating an account key pair for the first time, you need to use a user with the Tenant Administrator system role.

### Upgrading an Account Key Pair for the First Time

After you upgrade a key pair to an account key pair, all users under your account can view and use the key pair. If a key pair name is the same as the private key pair name of another sub-user, the upgrade cannot be performed. To upgrade key pairs, users with the Tenant Administrator system role must perform the upgrade at least once. The number of key pairs to be upgraded is not limited.

## 3.20 Will the Account Key Pair Quota Be Occupied After a Private Key Pair Is Upgraded to an Account Key Pair?

Yes.

If a private key pair is upgraded to an account key pair, the account key pair quota is occupied.

## 3.21 Why Is the Private Key Pair Invisible After It Is Upgraded to an Account Key Pair When Logging in as a Federated User?

### Symptom

After logging in as a federated user, some key pairs in the private key pair list are invisible after the account key pair is upgraded on the private key pair page.

### Possible Causes

The user ID of the federated login account is a virtual ID and cannot be obtained in the upgrade scenario. Therefore, after the key pair is upgraded, the key pair in the original private key pair list is invisible.

### Procedure

Before using a federated account, use the master account to upgrade the account key pair.

A private key pair is used to isolate resources based on the user ID of an account, and an account key pair is used to isolate resources based on the domain ID. Therefore, The recommended settings are as follows:

-	<b>Management account</b>	<b>Federated authentication account</b>	<b>Delegated account</b>
Private key pair	Not recommended	Prohibited	Prohibited
Account key pair	Recommended	Recommended	Recommended

# 4 Dedicated HSM Related

---

## 4.1 What Is Dedicated HSM?

Dedicated HSM is a cloud service used for encryption, decryption, signature, signature verification, key generation, and the secure storage of keys.

Dedicated HSM provides encryption hardware, guaranteeing data security and integrity on Elastic Cloud Servers (ECSs) and meeting FIPS 140-2 requirements. Dedicated HSM offers you a secure and reliable management for the keys generated by your instances, and uses multiple algorithms for data encryption and decryption.

## 4.2 How Does Dedicated HSM Ensure the Security for Key Generation?

- A key is created by the user remotely. During the creation, only the UKey owned by the user is involved in the authentication.
- The HSM configuration and preparation of internal keys can be performed only after being authenticated by using the UKey as the credential.

The user has full control over the generation, storage, and access of keys. Dedicated HSM is only responsible for monitoring and managing HSMs and related network facilities.

## 4.3 Do Equipment Room Personnel Has the Super Administrator Role to Steal Information by Using a Privileged UKey?

UKeys are owned only by users who purchased Dedicated HSM instances. Equipment room personnel do not have the super administrator role.

Sensitive data (keys) is stored in chips. Even HSM vendor cannot access the internal key information.



## 4.4 What HSMs Are Used for Dedicated HSM?

Dedicated HSM uses HSMs that have earned China State Cryptography Administration (CSCA) certification and FIPS 140-2 level 3 certification, achieving high security.

## 4.5 What APIs Does Dedicated HSM Support?

Dedicated HSM provides the same functions and interfaces as physical cryptographic devices, helping you easily migrate services to the cloud. Supported APIs include PKCS#11 and CSP.

For details, see [Editions](#).

## 4.6 How Do I Enable Public Access to a Dedicated HSM Instance?

You can binding EIPs to access Dedicated HSM instances from the public network.

### Prerequisites


You have an EIP that can be bound to the Dedicated HSM instance.


### Constraints

- After an EIP is bound to a Dedicated HSM instance, public network attacks may occur. Exercise caution when binding an EIP to a Dedicated HSM instance.
- EIPs are charged resources. You need to configure EIPs as required. If you do not need EIPs, unbind them in a timely manner. For details about how to unbind EIPs, see [Unbinding an EIP from an Instance](#). If the EIP is not released after unbinding, Huawei Cloud will charge the IP address retention fee. If a pay-per-use EIP billed by bandwidth is unbound from an instance, the bandwidth will continue to be billed. For details, see [Why Am I Still Being Billed After My EIP Has Been Unbound or Released?](#)

### Procedure

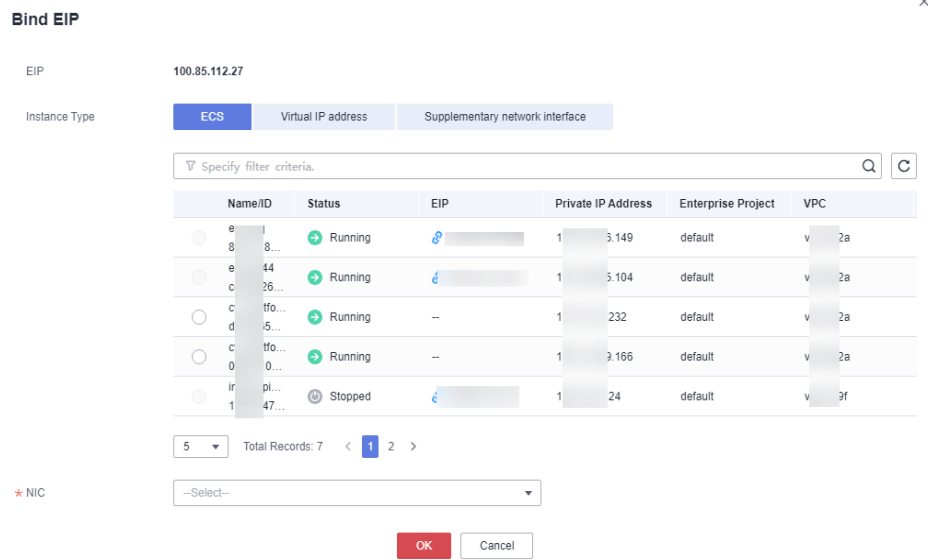
**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click  on the left of the page. Select **Network** > **EIP**. The EIP page is displayed by default.

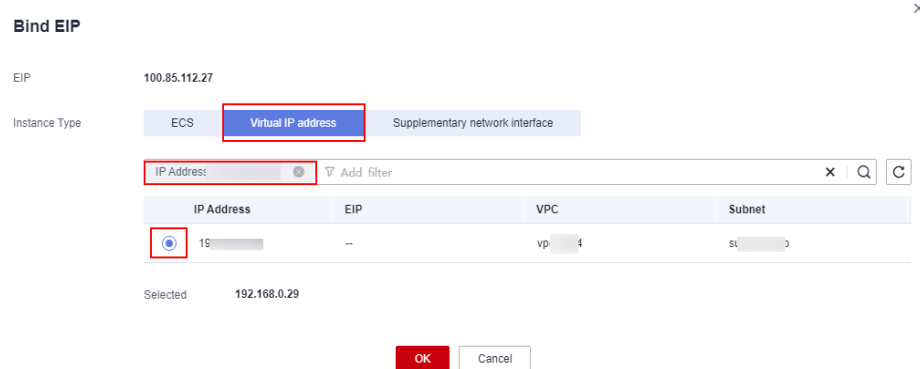
**Step 4** Click **Bind** in the **Operation** column of the target EIP. The Bind page is displayed, as shown in [Figure 4-1](#).

Figure 4-1 Binding an EIP



**Step 5** Click **Virtual IP Address**, enter the IPv4 address of the instance to be bound in the search box, and select the search result, as shown in [Binding a virtual IP address](#).

Figure 4-2 Binding a virtual IP address



**Step 6** Select the corresponding IP address and click **OK**.

----End

# 5 Pricing

---

## 5.1 How Is DEW Charged?

For price details, see [Product Pricing Details](#).

### KMS

KMS is charged per use. No minimum fee is required. Once a CMK is created, it will be charged by hour. You pay for CMKs you created and API requests that are beyond the free-of-charge range.

### KPS

- If you do not choose to let Huawei Cloud manage your private keys when creating or importing them, no cost will be incurred.
- If you have your keys managed by Huawei Cloud, KPS is charged by hour. In the current version, it is free of charge.

### Dedicated HSM

Dedicated HSM offers monthly and yearly packages based on the edition and device models of instances you have purchased.

### CSMS

You are charged based on the number of secrets, usage duration, and number of API requests.

## 5.2 How Do I Renew DEW?

This section describes how to renew KMS or a Dedicated HSM instance. After renewal, you can continue to use the KMS and Dedicated HSM instance.

- Auto-renewal  
If you have selected and agreed to auto renewal of KMS or Dedicated HSM, the system automatically generates a renewal order and renews the

subscription based on the original subscription period before the service expires.

- Manual renewal

Before the service expires, the system will send an SMS message or email to remind you to renew it.

If you do not renew the service before it expires, it will enter the retention period.

 **NOTE**

If you do not renew your subscription before it expires, a retention period will apply. The retention period varies with customer tiers. For details, see [Retention Period](#).

**Table 5-1** Retention period

Service	Edition	Retention Period
KMS	Standard	Keys are frozen. Activate frozen keys by topping up the account.
Dedicated HSM	-	<ul style="list-style-type: none"> <li>• Within the retention period, your Dedicated HSM instances cannot be used but are reserved for you.</li> <li>• If the retention period expires, your Dedicated HSM instances will be released.</li> </ul>

 **NOTE**

- Frozen keys cannot be used for encryption or decryption. To prevent unnecessary losses, it is recommended that you renew the service in time.
- Data related to Dedicated HSM instances will get lost when the instances are released. To prevent unnecessary losses, it is recommended that you renew the service or top up the account in time.

## Prerequisites


You have obtained the login account (with the **BSS Administrator** and **KMS Administrator** permissions) and password for logging in to the management console.


 **NOTE**

An account with the **BSS Administrator** permission can perform any operation on all menu items in the account center, billing center, and resource center.

## Procedure

**Step 1** [Log in to the management console](#).

**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Encryption Workshop**.

**Step 4** In the upper right corner, click **Renew**.

**Step 5** On the renewal management page, complete the renewal as prompted.

For details, see [Manually Renewing a Resource](#).

----End

## 5.3 How Do I Unsubscribe from DEW?

DEW does not support unsubscription.

### NOTE

If you fail to create a Dedicated HSM instance, you can click **Delete** in the row where the failed instance locates to delete it. Then you can submit a service ticket to apply for refund.

### Helpful Links

- [Unsubscription Rules](#)
- [List of Cloud Service Products That You Cannot Unsubscribe From](#)
- [Creating a Service Ticket](#)

## 5.4 Will a CMK Be Charged After It Is Disabled?

Yes.

A disabled CMK is still kept and maintained by KMS. You can enable it whenever you need it. Therefore, a disabled CMK is still billable. Only deleted CMKs are not charged.

## 5.5 Are Credentials Scheduled to Be Deleted Billed?

No.

A credential in pending deletion status does not incur charges.

If you cancel deletion, the charging resumes from the time when the credential was scheduled to be deleted.

## 5.6 Will a CMK Be Charged After It Is Scheduled to Delete?

No.

The pending period of a CMK from its scheduling till its deletion is not charged.

However, if you cancel the scheduled deletion, the charging resumes from the time when the CMK is scheduled to be deleted.

## 5.7 How Is Rotation Charged for a CMK?

After key rotation is enabled, you will be charged for storing the key. Each rotated version is calculated as an independent master key resource. The fees for API calls are irrelevant to the number of rotations.

For example, if rotation is enabled for one CMK, and the rotation period is 30 days, the unit price is \$0.001388 USD (\$ 0.01 USD after erasure) per hour:

First month: the rotation version of a CMK is 0, the fee is \$0.72 USD ( $0.001 \times 24 \times 30 + 0 \times 0.001 \times 24 \times 30$ ).

Second month: the rotation version of a CMK is 1, the fee is \$1.44 USD ( $0.001 \times 24 \times 30 + 1 \times 0.001 \times 24 \times 30$ ).

Third month: the rotation version of a CMK is 2, the fee is \$2.16 USD ( $0.001 \times 24 \times 30 + 2 \times 0.001 \times 24 \times 30$ ).

The other egresses follow the same rule.

Month  $n$ : the rotation version of a CMK is  $n$ , the fee is  $0.001 \times 24 \times 30 + (n-1) \times 0.001 \times 24 \times 30 = \$0.72 \times n$  USD.

# 6 General

## NOTICE

When interconnecting with KMS, retry is required. Error code such as 504, 502, 500, and 429 are included. Retry three to five times. For error codes 502 and 504, the timeout interval should be 5 to 8 seconds. Do not configure a long timeout interval. Otherwise, the client cannot respond.

## 6.1 What Functions Does DEW Provide?

### Key Management Service

- On the KMS console, you can:
  - Create, query, enable, and disable CMKs, as well as schedule and cancel CMK deletion.
  - Modify the alias and descriptions of CMKs.
  - Use the online tool to encrypt and decrypt small-size data.
  - Add, search for, edit, and delete tags.
  - Create, cancel, and query grants.
- You can use the APIs to:
  - Create, encrypt, or decrypt DEKs.
  - Retire grants.
  - Sign or verify the signature of messages or message digests.
  - Generate and verify message authentication codes.

For details, see the *Data Encryption Workshop API Reference*.

- Generate hardware true random numbers.

You can generate 512-bit random numbers based on hardware using the KMS API. The 512-bit true random numbers can be used as basis for key materials and encryption parameters. For details, see the *Data Encryption Workshop API Reference*.

## Key Pair Service

Using the KPS console or APIs, you can perform the following operations on key pairs:

- Creating, importing, viewing, and deleting key pairs
- Resetting, replacing, binding, and unbinding key pairs
- Managing, importing, exporting, and clearing private keys

## Dedicated HSM

On the **Dedicated HSM** page of the management console, you can purchase Dedicated HSM instances

# 6.2 What Cryptography Algorithms Does DEW Use?

## Cryptographic Algorithms Supported by KPS

- The SSH key pairs created on the management console support the following cryptographic algorithms:
  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH\_RSA: The length can be 2048, 3072, and 4096 bits.
- The SSH keys imported to the KPS console support the following cryptographic algorithms:
  - SSH-DSS
  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH\_RSA: The length can be 2048, 3072, 4096 bits.

## Supported Cryptography Algorithms

You can use Chinese cryptographic algorithms and certain international common cryptographic algorithms to meet various user requirements.

**Table 6-1** Supported cryptography algorithms

Category	Common Cryptographic Algorithm
Symmetric cryptographic algorithm	AES
Asymmetric cryptographic algorithm	RSA, DSA, ECDSA, DH, and ECDH



Category	Common Cryptographic Algorithm
Digest algorithm	SHA1, SHA256, and SHA384

## 6.3 In Which Regions Are DEW Services Available?

DEW services are available in the following regions:

- KMS
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore
  - AF-Johannesburg
  - LA-Mexico City1
  - LA-Mexico City2
  - LA-Santiago
  - LA-Sao Paulo1
- KPS
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore
  - LA-Sao Paulo1
- CSMS
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore
  - LA-Sao Paulo1
- Dedicated HSM
  - CN-Hong Kong
  - AP-Bangkok
  - AP-Singapore
  - LA-Santiago

## 6.4 What Is a Quota?

### What Is a Quota?

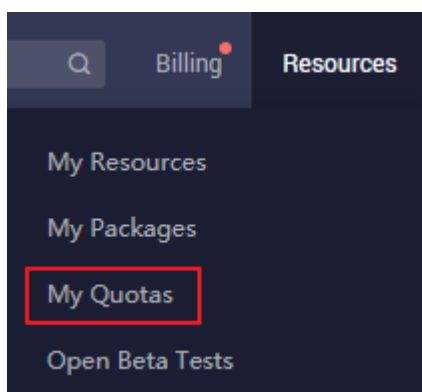
Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users. For example, the maximum number of CMKs that you can create.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

## How Do I View My Quota?

- Step 1** Log in to the management console.
- Step 2** In the upper right corner of the page, choose **Resources > My Quotas**.  
The **Service Quota** page is displayed.

**Figure 6-1** My quotas



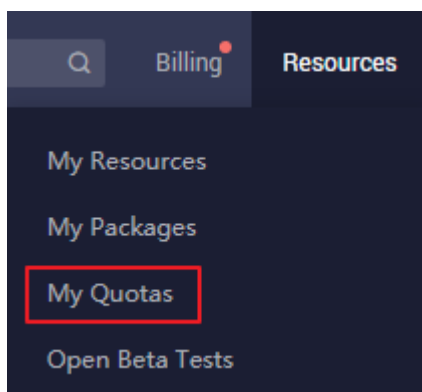
- Step 3** View the used and total quota of each type of resources on the displayed page.
- Step 4** If a quota cannot meet your service requirements, click **Increase Quota** to change it.

----End

## How Do I Increase a Quota?

- Step 1** Log in to the management console.
- Step 2** In the upper right corner of the page, choose **Resources > My Quotas**.  
The **Service Quota** page is displayed.

**Figure 6-2** My quotas



- Step 3** Click **Increase Quota**.

**Step 4** On the **Create Service Ticket** page, configure parameters as required.

In the **Problem Description** area, fill in the content and reason for the increase.

**Step 5** After all mandatory parameters are configured, select **I have read and agree to the Tenant Authorization Letter and Privacy Statement** and click **Submit**.

----End

## 6.5 What Is the Resource Allocation Mechanism of DEW?

DEW uses regions as large resource pools and independent resources or services of each customer as small resource pools. The background has default traffic limits. For a single user, if the traffic exceeds the threshold, the service speed is slow. For customers who have heavy traffic requirements, background resources can be changed based on the actual situation and requirements.

If your traffic volume exceeds the limit, you can submit a service ticket to increase the quota. DEW will adjust your limit in the background to support your provisioning of dedicated configuration clusters and ensure stable service running.

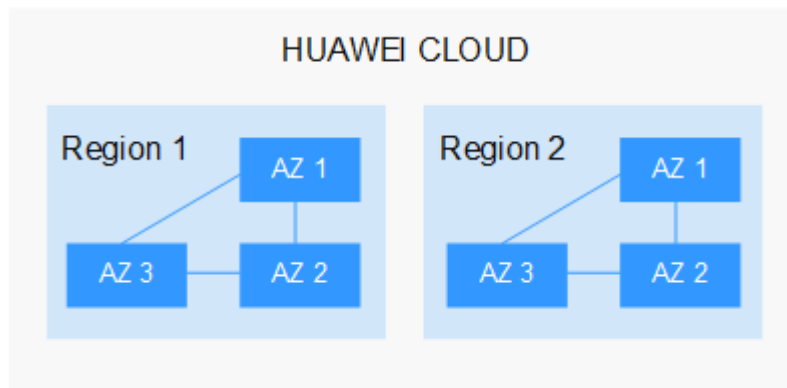
## 6.6 What Are Regions and AZs?

### Concepts

A region or an availability zone (AZ) identifies the location of a data center. You can create resources in a specific region or an AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

**Figure 6-3** shows the relationship between the regions and AZs.

**Figure 6-3** Region and AZ

Huawei Cloud provides services in many regions around the world. You can select a region and AZ as needed.

## Selecting a Region

When selecting a region, consider the following factors:

- Location  
You are advised to select a region close to you or your target users. This reduces network latency and improves access rate.
  - If you or your users are in the Asia Pacific region and outside the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your users are in Africa, select the **AF-Johannesburg** region.
  - If you or your users are in Latin America, select the **LA-Santiago** region.
- Resource price  
Resource prices may vary in different regions. For details, see [Product Pricing Details](#).

## Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

## Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

## 6.7 Can DEW Be Shared Across Accounts?

No. Currently, a user can only use and manage their own keys and key pairs.

## 6.8 How Do I Access the Functions of DEW?

You can use DEW on the web console or call the functions of DEW by using HTTPS-based APIs.

- Console

If you have registered with the public cloud, you can log in to the management console directly. In the upper left corner of the console, click



. Choose **Security & Compliance > Data Encryption Workshop**.

- API

You can access DEW using the API. For details, see the *Data Encryption Workshop API Reference*.

DEW supports REST APIs, allowing you to call APIs by using HTTPS. You can use provided APIs to perform operations on keys and key pairs, such as creating, querying, and deleting keys.

DEW APIs use the HTTPS protocol to encrypt and secure transmission, preventing man-in-the-middle attacks.

## 6.9 Why Do DEW Permissions Fail to Take Effect Immediately?

Generally, DEW permissions such **KMS Administrator** and **KMS CMKFullAccess** take effect immediately.

However, permissions cannot take effect in time in the following scenarios:

1. You did not log out of the console in time and the session is cached. Log in to the console again.
2. You used services that have permissions to cache data, such OBS. In this case, when the permission takes effect depends on the service cache duration.
3. APIG is called. In this case, when the permission take effect depends on the time when IAM broadcasts the permission change to the gateway.