

Data Encryption Workshop

Getting Started

Issue 05
Date 2025-07-22



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.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

1 Creating a Key for Cloud Service Encryption..... 1

2 Creating a Secret for Data Storage Rotation.....7

3 Binding a Key Pair and Logging In to an ECS Using a Private Key.....13

4 Using a Key to Encrypt Data in OBS..... 22

5 Getting Started with Common Practices..... 29

1 Creating a Key for Cloud Service Encryption

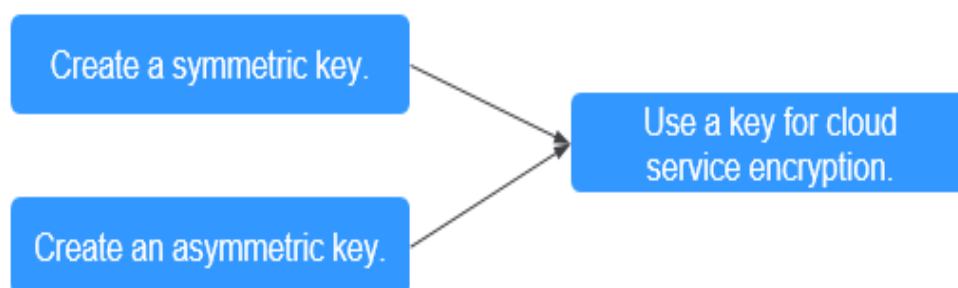
A key can be symmetric or asymmetric.

- For symmetric keys, the same key is used to encrypt and decrypt data, which is fast and efficient, suitable for encrypting a large amount of data.
- For asymmetric keys, a key pair, that is, a public key and a private key, are used for encryption and decryption. Public keys can be distributed to anyone, while private keys must be kept secure and provided for only trusted users. These keys are used for digital signature verification and encrypted transmission of sensitive information.

Procedure

This section uses the AES-256 symmetric key and RSA-2048 asymmetric key as examples to describe how to create a key and bind it to a cloud service. The following figure shows the process.

Figure 1-1 Creating a key for cloud service encryption



Procedure	Description
Preparations	Register a Huawei ID, enable Huawei Cloud services, top up the account, and grant KMS permissions to the account.
Step 1: Creating a Key	Create a key and select the key algorithm type.
Step 2: Cloud Service Encryption	After the key is created, bind the key to the instance when you create or use a cloud service instance for encryption.

Preparations

1. Before creating key, register a Huawei Cloud account and enable Huawei Cloud services. For details, see [Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services](#).
If you have enabled Huawei Cloud, skip this step.
2. You have obtained KMS CMKFullAccess or higher permissions. For details, see [Creating a User and Authorizing the User the Permission to Access DEW](#).

Table 1-1 KMS system roles

Role	Description	Type	Dependencies
KMS administrator	All permissions of KMS	System-defined role	None
KMS CMKFullAccess	All permissions for KMS keys. Users with these permissions can perform all the operations allowed by policies.	System-defined policy	None
KMS CMKReadOnlyAccess	Read-only permissions for KMS keys. Users with these permissions can perform all the operations allowed by policies.	System-defined policy	None

Step 1: Creating a Key

This section describes how to create an AES-256 symmetric key and an RSA-2048 asymmetric key.

Creating a Symmetric Key

The created key can be used only in the current region. To use it in other regions, switch to the target region and create a key or use a regional key.

1. Log in to the [DEW console](#).
2. On the **Key Management Service** page, click **Create Key** in the upper right corner.
3. On the displayed page, configure the parameter as shown in the following and retain default settings for other parameters. For details about the parameters, see [Table 1-2](#).

Figure 1-2 Creating a key

Basic Information

Name

1

KMS-335c

Key Algorithm

?

AES_256

2

Usage

?

ENCRYPT_DECRYPT

3

Enterprise Project

default

Create Enterprise Project

You can organize cloud resources and users by enterprise project for more convenient management.

Keystore

default

Create Keystore

Source

4

Key Management Service

External

Table 1-2 Mandatory parameters

Parameter	Example Value	Description
Name	KMS-335c	Custom key name, which cannot be empty.
Key Algorithm	AES-256	Supported key algorithm types and description. For details, see Key algorithms supported by KMS .

Parameter	Example Value	Description
Usage	ENCRYPT_DECRYPT	The value cannot be changed after the key is created. For AES_256 symmetric keys, the default value is ENCRYPT_DECRYPT .
Source	Key Management Service	The following key material sources are supported: <ul style="list-style-type: none">• Key Management Service: KMS generates key materials.• External: Import local key materials to KMS.

4. Click **OK**. A message is displayed in the upper right corner of the page, indicating that the key is created. In the key list, you can view the created keys, which are in the **Enabled** state by default.

Creating an Asymmetric Key

The created key can be used only in the current region. To use it in other regions, switch to the target region and create a key or use a regional key.

1. Log in to the [DEW console](#).
2. On the displayed **Key Management Service** page, click **Create Key** in the upper right corner.
3. On the displayed page, configure the parameter as shown in the following and retain default settings for other parameters. For details about the parameters, see [Table 1-2](#).

Figure 1-3 Creating a key

Basic Information

Name 1

Key Algorithm ? 2

Usage ? 3

Enterprise Project
 Q [Create Enterprise Project](#)

You can organize cloud resources and users by enterprise project for more convenient management.

Keystore
 Q [Create Keystore](#)

Source 4

☒ Key Management Service ☐ External

Table 1-3 Mandatory parameters

Parameter	Example Value	Description
Name	KMS-335c	Custom key name, which cannot be empty.
Key Algorithm	RSA-2048	Supported key algorithm types and description. For details, see Key algorithms supported by KMS .
Usage	SIGN_VERIFY	The value cannot be changed after the key is created. For RSA asymmetric keys, the value can be ENCRYPT_DECRYPT or SIGN_VERIFY .

Parameter	Example Value	Description
Source	Key Management Service	The following key material sources are supported: <ul style="list-style-type: none">• Key Management Service: KMS generates key materials.• External: Import local key materials to KMS.

4. Click **OK**. A message is displayed in the upper right corner of the page, indicating that the key is created. In the key list, you can view the created keys, which are in the **Enabled** state by default.

Step 2: Cloud Service Encryption

Currently, KMS interconnects with services such as OBS and EVS to implement instance encryption. For details about the principles and operations, see the following.

- [Encrypting Data in ECS](#)
- [Encrypting Data in OBS](#)
- [Encrypting Data in EVS](#)
- [Encrypting Data in IMS](#)
- [Encrypting an RDS DB Instance](#)
- [Encrypting a DDS DB Instance](#)

2

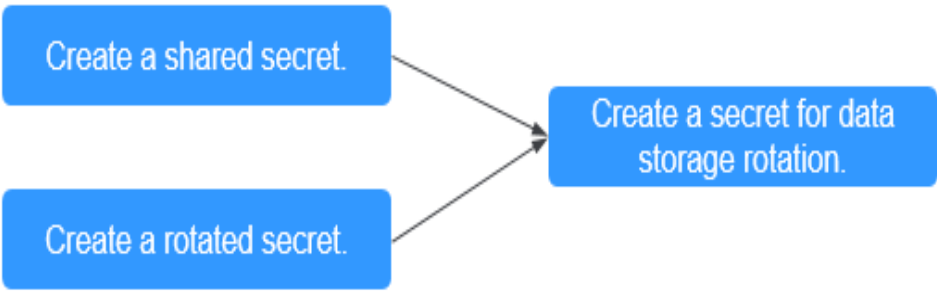
Creating a Secret for Data Storage Rotation

Applications and business systems have a large number of secrets and are difficult to manage. Cloud Secret Management Service (CSMS) can store, retrieve, and use secrets in a unified manner throughout their lifecycles.

Procedure

This section uses a shared secret and a rotated secret as examples to describe how to create a secret and rotate data. The following figure shows the process.

Figure 2-1 Creating a secret for data storage rotation



Procedure	Description
Preparations	Register a Huawei ID, enable Huawei Cloud services, top up the account, and grant CSMS permissions to the account.
Step 1: Creating a Secret	Create a secret and choose the secret type.
Step 2: Rotating Data	After the secret is created, you can configure FunctionGraph to complete data rotation within the secret.

Preparations

1. Before creating a secret, register a Huawei Cloud account and enable Huawei Cloud services. For details, see [Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services](#).
If you have enabled Huawei Cloud, skip this step.
2. Before purchasing an instance, ensure that your account balance is sufficient. For details, see [Top-Up and Payment](#).
3. Before using a rotated secret, you need to create a database instance and database account.
 - RDS secret: Create an RDS instance. For details, see [Buying an RDS for MySQL DB Instance](#).
 - TaurusDB secret: Only TaurusDB instances are supported. For details, see [Buying a DB Instance](#).

Step 1: Creating a Secret

The following describes how to create a shared secret and a rotated secret.


Creating a Shared Secret

Full lifecycle management is supported for customized secrets in different scenarios. You can use CSMS to centrally manage, retrieve, and securely store various types of secrets, such as database account passwords, server passwords, SSH keys, and access keys. Multiple versions can be managed, so you can rotate secrets.

1. Log in to the [DEW console](#).
2. In the navigation pane on the left, choose **Cloud Secret Management Service > Secrets**. On the displayed page, click **Create Secret** in the upper left corner.
3. On the displayed page, configure the parameters as shown in [Figure 2-2](#).

Figure 2-2 Creating a shared secret

Basic Information




Type  **1**

Shared secret Rotated secret

Secret Name

test

Enterprise Project


default   [Create Enterprise Project](#) 

You can organize cloud resources and users by enterprise project for more convenient management.

Secret Value **2**

Secret key/value Plaintext




test 001 [Delete](#)

 [Add](#)

KMS Encryption Key

Select from List Enter

Use this if the current account key is used or a key is shared.

csms/default **3**   [Create Key](#) 

By default, the master key csms/default is used for encryption.

4. Click **Next**.
5. Click **Next** and confirm the creation information.
6. Click **OK**. In the secret list, you can view the created secrets, which are in the **Enabled** state by default.

Creating a Rotated Secret

Database secret leakage is the main cause of data leakage. CSMS supports RDS and TaurusDB secrets hosting, as well as automatic and manual rotation, meeting various database secret management scenarios and reducing security risks faced by service data.

1. Log in to the [DEW console](#).
2. In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**. On the displayed page, click **Create Secret** in the upper left corner.
3. On the displayed page, configure the parameter as shown in the following and retain default settings for other parameters. For details about the parameters, see [Table 2-1](#).

Figure 2-3 Creating a rotated secret

Basic Information

Type ⓘ

1

Shared secretRotated secret

RDS secret

2

Secret Name

test

Enterprise Project

default

Create Enterprise Project

You can organize cloud resources and users by enterprise project for more convenient management.

Database

TaurusDB

3

RDS DB Instance

taurus_test_01

4

View RDS DB Instance

5

Secret Value

Dual accountSingle account

The simplest rotation strategy. Program access will be interrupted the moment the password is rotated. Exercise caution when selecting this.

Account Name

Select

Password

Enter a value.

KMS Encryption Key

Select from ListEnter

Use this if the current account key is used or a key is shared.

csms/default

6

Create Key

By default, the master key csms/default is used for encryption.

Table 2-1 Parameters for creating a rotated secret

Parameter	Example Value	Description
Type	Rotated secret > RDS secret	CSMS supports the following secret types: <ul style="list-style-type: none">● Shared secret: Automatic secret rotation is not supported.● Rotated secret: Automatic secret rotation is supported. The secret type can be RDS secret or TaurusDB secret.
Database	TaurusDB	RDS secrets support MySQL, PostgreSQL, SQLServer, MariaDB, and TaurusDB databases.

Issue 05 (2025-07-22)

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

10

Parameter	Example Value	Description
RDS DB Instance	taurus_test_01	Select the RDS instance corresponding to the target database type.
Secret Value	Single account Set Account Name and Password as required.	Account name and password to be encrypted. <ul style="list-style-type: none">• If Single account is selected, you need to enter an available database account.• If Dual account is selected, after you enter an available database account, a cloned account with the same permissions will be created. Select I understand the risks.

Parameter	Example Value	Description
KMS Encryption Key	csms/default	<p>The following modes are supported:</p> <ul style="list-style-type: none">• Select from list: Select this if you want to use the key used or shared by the current account. Select the default key csms/default or a custom key created on KMS.• Enter: Enter the ID of the authorized key. Enter an encryption key if an authorized key is used. Only symmetric algorithm key IDs are supported. Do not enter an asymmetric key ID. <p>NOTE</p> <ul style="list-style-type: none">• CSMS encrypts secret values using the encryption key provided by KMS. When you use the KMS encryption function, KMS creates a default key csms/default for you to use.• For details about how to create a custom key on KMS, see Creating a Key.• After a grant is created, you can switch to the manual input mode, and enter the key ID to use the granted key for encryption. For details, see .

4. Click **Next**. On the displayed page, enable automatic rotation and set the rotation period as required.
5. Under **Rotation function**, click **Create one**, enter the function name, select **I understand the risks**, and click **Next**.
6. Click **OK**. In the secret list, you can view the created secrets, which are in the **Enabled** state by default.

Step 2: Rotating Data

You need to configure FunctionGraph to use shared secrets for data rotation. For details, see the following content.

- [Rotating IAM Secrets Using FunctionGraph](#)
- [Using CSMS to Automatically Rotate Security Passwords](#)

3 Binding a Key Pair and Logging In to an ECS Using a Private Key

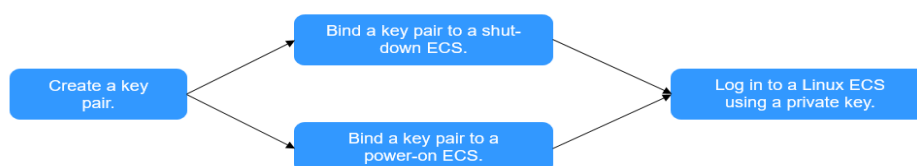
A key pair, including one public key and one private key, are generated based on a cryptographic algorithm. The public key is automatically saved in Key Pair Service (KPS), while the private key can be saved to the user's local host. If you have configured the public key in a Linux ECS, you can use the private key to log in to the ECS for better security.

This section describes how to bind a key pair and log in to an ECS using a private key.

Procedure

The following uses an SSH_RSA_2048 key pair as an example to describe how to create a key pair and use the key to log in to an ECS. The following figure shows the process.

Figure 3-1 Creating a key pair and using it to log in to an ECS



Procedure	Description
Preparations	Register a Huawei ID, enable Huawei Cloud services, top up the account, and grant KPS permissions to the account.
Step 1: Creating a Key Pair	Create a key pair and select the key pair type.

Procedure	Description
Step 2: Binding a Key Pair to an ECS <ul style="list-style-type: none">• Step 2: Binding a Key Pair to a Shut-down ECS• Step 2: Binding a Key Pair to a Running ECS	Bind a key pair to the ECS.
Step 3: Logging in to an ECS Using a Private Key	After the key pair is bound, use the private key to log in to the ECS.

Preparations

1. Before creating key pair, register a Huawei Cloud account and enable Huawei Cloud services. For details, see [Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services](#).
If you have enabled Huawei Cloud, skip this step.
2. An ECS has been created. For details, see [Purchasing an ECS in Custom Config Mode](#).
The SSH port (22 by default) of the ECS security group must allow traffic from the **100.125.0.0/16** CIDR block in advance. For details about ports and CIDR blocks, see [Enhancing Security for SSH Logins to Linux ECSs](#).
3. The KPS permission has been granted to the account. For details, see [Creating a User and Authorizing the User the Permission to Access DEW](#).

Table 3-1 KPS system policies

Role/Policy Name	Description	Type	Dependency
DEW KeypairFull Access	Full permissions for KPS in DEW. Users with these permissions can perform all the operations allowed by policies.	System-defined policy	None
DEW KeypairRead OnlyAccess	Read-only permissions for KPS in DEW. Users with this permission can only view KPS data.	System-defined policy	None

Step 1: Creating a Key Pair

1. Log in to the [DEW console](#).
2. In the navigation pane on the left, choose **Key Pair Service**.

3. In the **Private Key Pairs** tab, click **Create Key Pair**, and configure the parameters as shown in **Figure 3-2**. For details about the parameters, see **Table 3-2**.

Figure 3-2 Creating a private key pair

Key Pair Name

KeyPair-108b

Type ?

SSH_RSA_2048

⚠ If you have not enabled your account key pair, this parameter is invalid. An SSH_RSA_2048 key pair will be created by default. Currently, only the RSA algorithm can be used with Windows.

☒ I agree to host the private key of the key pair. [Learn more](#)

⚠ What you use beyond the free API request quota given by KMS will be billed.[Pricing details](#)

KMS Encryption Key

Select from List

Enter

Use this if the current account key is used or a key is shared.

kps/default

🔍

Create Key

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

Table 3-2 Parameters for creating a private key pair

Parameter	Example Value	Description
Type	SSH_RSA_2048	Signature algorithm of the SSH key pair. RSA, ECDSA, and EdDSA are supported.

Parameter	Example Value	Description
KMS Encryption Key NOTE Select I agree to host the private key of the key pair and select an encryption key.	kps/default	KMS supports the following encryption modes: <ul style="list-style-type: none">• Select from List: Select this if you want to use the key used or shared by the current account. Select the default key kps/default or a custom key created on KMS.• Enter: Enter the ID of the authorized key. Enter an encryption key if an authorized key is used. Only symmetric algorithm key IDs are supported. Do not enter an asymmetric key ID.

4. Select **I have read and agree to Key Pair Service Disclaimer** and click **OK**. The private key file will be automatically downloaded. You need to save the file as prompted.

Step 2: Binding a Key Pair to an ECS

After a key pair is bound to an ECS, you can use the private key to log in to the ECS.

Step 2: Binding a Key Pair to a Shut-down ECS

1. In the navigation pane on the left, choose **Key Pair Service**. On the displayed page, click the **ECS List** tab.
2. Locate the target shut-down ECS and click **Bind** in the **Operation** column.
3. On the displayed page, select a key pair. Then, select **Disable the password login mode** and **I have read and agree to Key Pair Service Disclaimer**.

Figure 3-3 Binding a key pair to a shut-down ECS

Bind Key Pair

• Check whether the preparations are complete before binding the key pairs, which will take 3 to 5 minutes. [View preparations.](#)
• The key pair bound to the server can be used for login. For security reasons, disable password login for this server.

⚠ A temporary ECS needs to be created. It will be automatically deleted after the key pair is bound. This will cost you only a few cents. [Pricing details](#)

ECS

ECS Name	Private IP Address	Status
ecs-default	192.168.1.1	Shut down

Key Pair

KeyPair-ea512

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

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

4. Click **OK**.

Step 2: Binding a Key Pair to a Running ECS

1. In the navigation pane on the left, choose **Key Pair Service**. On the displayed page, click the **ECS List** tab.
2. Locate the target running ECS and click **Bind** in the **Operation** column.
3. On the displayed page, configure the parameters as shown in **Figure 3-4**.
 - Set **New Key Pair** and **Root Password**.
 - The default port is **22**.
 - Select **Disable the password login mode** and **I have read and agree to Key Pair Service Disclaimer**.

Figure 3-4 Binding a key pair

Bind Key Pair

• Check whether the preparations are complete before binding the key pair, which will take 1 to 3 minutes. [View preparations.](#)
• The key pair bound to the server can be used for login. For security reasons, disable password login for this server.

ECS

ECS Name	Private IP Address	Status
ecs-liyuan-test	10.0.0.1	Running

Key Pair 1

123

Root Password 2

Port

22

The default port number is 22, but you can change it if your server uses another port.

☒ Disable the password login mode. [Learn more](#) 3

☒ I have read and agree to [Key Pair Service Disclaimer](#). 4

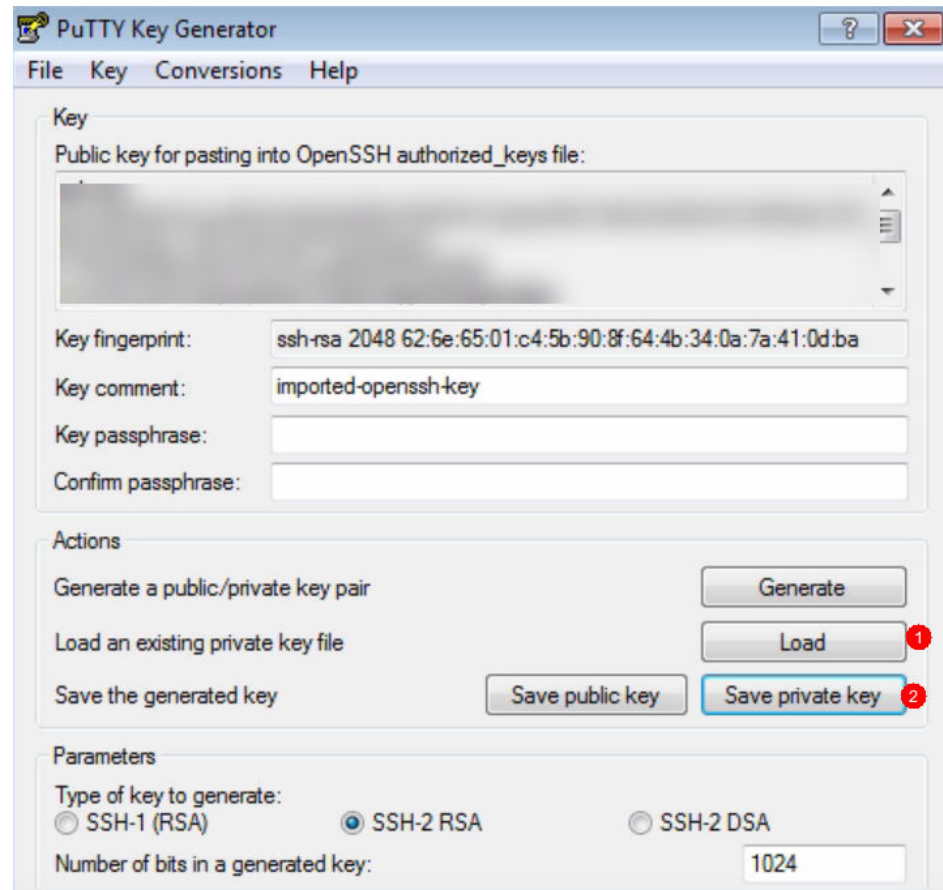
4. Click **OK**.

Step 3: Logging in to an ECS Using a Private Key

1. Check whether the private key file has been converted to .ppk format.
 - If yes, log in to the ECS server.
 - If no, perform the following operations to convert the format of the private key file and then log in to ECS.

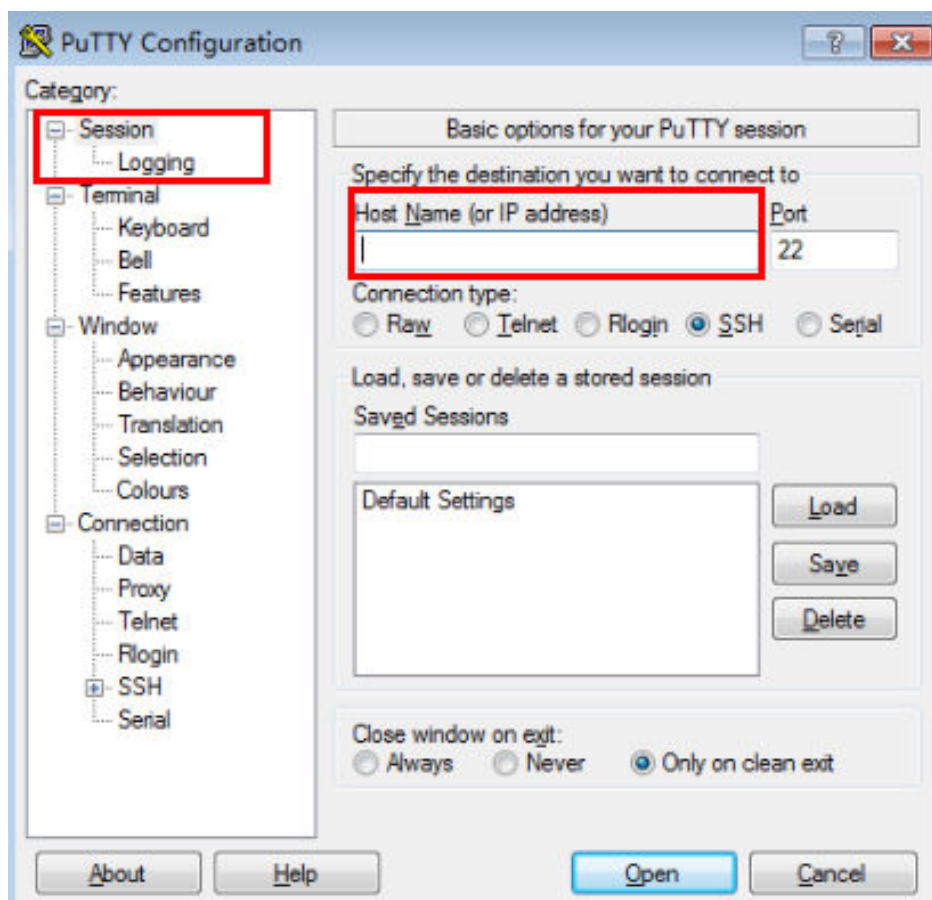
Open the third-party PuTTY, import the .pem private key file, and export the converted .ppk private key file.

Figure 3-5 Converting the format of the private key file



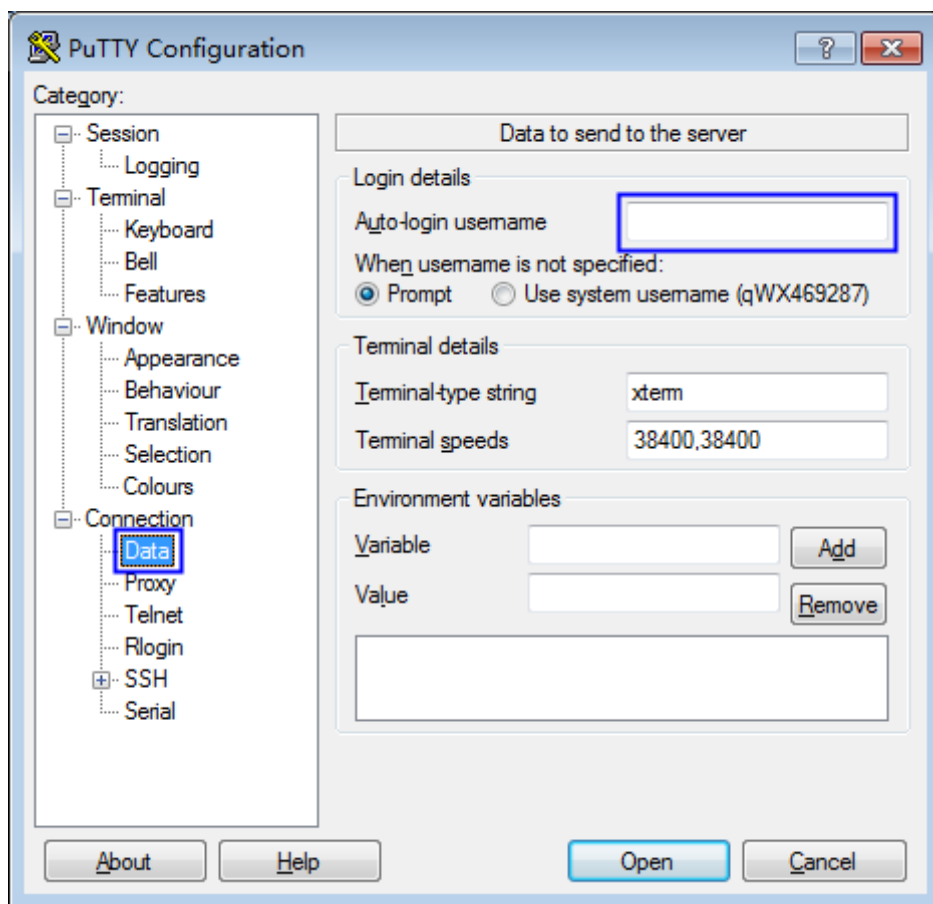
2. Use PuTTY to log in to ECS.
 - Enter the IP address of the ECS. Port **22** is used by default.

Figure 3-6 IP address of ECS



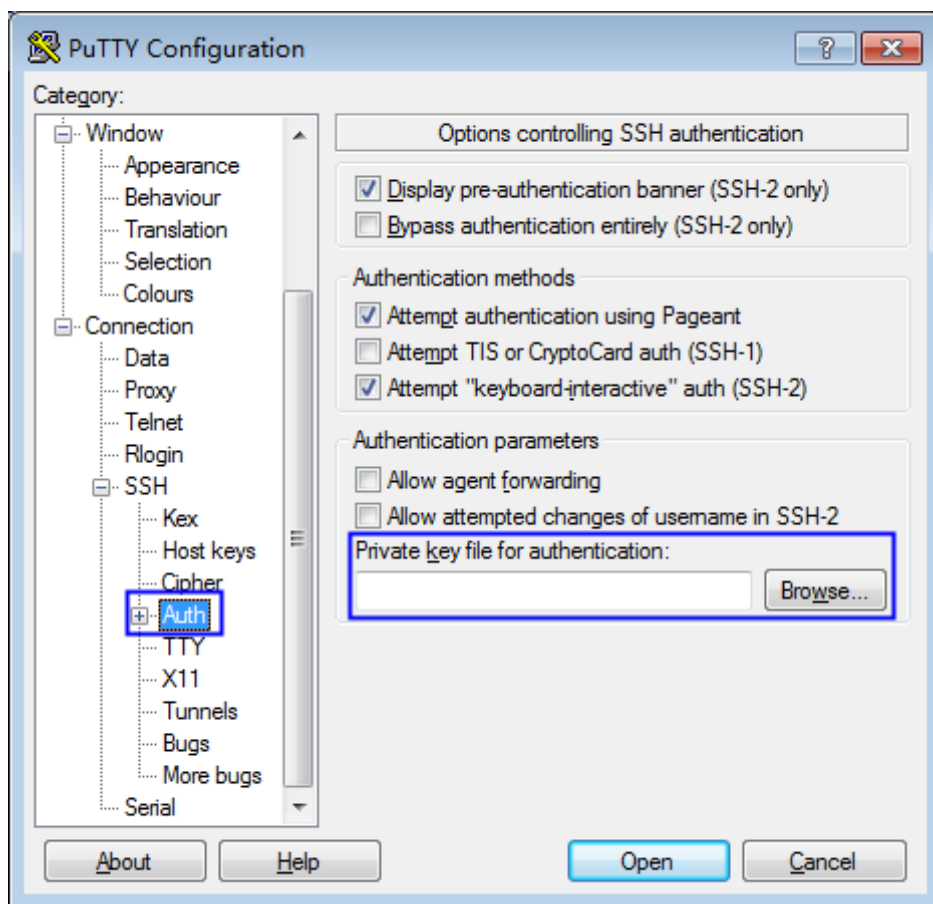
- Enter the username of the ECS image.

Figure 3-7 Username



- Upload the private key file in .ppk format.

Figure 3-8 Uploading the private key file



- Click **Open**.

4 Using a Key to Encrypt Data in OBS

DEW is a cloud data encryption service. Key Management Service (KMS) provided by DEW is a secure, reliable, and easy-to-use cloud service that can help you manage and protect keys in a centralized manner.

With KMS, you can create keys and use the keys to encrypt files to be uploaded on the OBS server.

Procedure

Procedure	Description
Preparations	Register a Huawei ID, enable Huawei Cloud services, top up the account, and grant KMS permissions to the account.
Step 1: Creating a Bucket	Buckets are containers that store objects in OBS. Before you can store data, you must create a bucket.
Step 2: Creating a Key	With KMS, you can create keys and use the keys to encrypt files to be uploaded on the OBS server.
Step 3: Uploading Files to an OBS Bucket	Upload files to the OBS bucket and use the KMS key encrypt the files.

Preparations


1. Before encrypting data in OBS, register a Huawei Cloud account and enable Huawei Cloud services. For details, see [Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services](#).
If you have enabled Huawei Cloud, skip this step.
2. Ensure that your account has sufficient balance.
3. You have obtained KMS CMKFullAccess or higher permissions. For details, see [Creating a User and Authorizing the User the Permission to Access DEW](#).

Table 4-1 KMS system roles

Role	Description	Type	Dependencies
KMS administrator	All permissions of KMS	System-defined role	None
KMS CMKFullAccess	All permissions for KMS keys. Users with these permissions can perform all the operations allowed by policies.	System-defined policy	None
KMS CMKReadOnlyAccess	Read-only permissions for KMS keys. Users with these permissions can perform all the operations allowed by policies.	System-defined policy	None

Step 1: Creating a Bucket

Buckets are containers that store objects in OBS. Before you can store data, you must create a bucket.

1. Log in to the [DEW console](#).
2. Click  on the left and choose **Storage > Object Storage Service**.
3. On the displayed page, click **Create Bucket** to store uploaded files. For details, see [Creating a Bucket](#).

Step 2: Creating a Key

The following uses the AES-256 symmetric key as an example.

The created key can be used only in the current region. To use it in other regions, switch to the target region and create a key or use a regional key.

1. Log in to the [DEW console](#).
2. On the **Key Management Service** page, click **Create Key** in the upper right corner.
3. On the displayed page, configure the parameter as shown in the following and retain default settings for other parameters. For details about the parameters, see [Table 4-2](#).

Figure 4-1 Creating a key

Basic Information

Name

KMS-335c

1

Key Algorithm ?

AES_256

2

Usage ?

ENCRYPT_DECRYPT

3

Enterprise Project

default

Q

Create Enterprise Project

Keystore

default

Q

Create Keystore

Source

4

Key Management Service

External

Table 4-2 Mandatory parameters

Parameter	Example Value	Description
Name	KMS-335c	Custom key name, which cannot be empty.
Key Algorithm	AES-256	Supported key algorithm types and description. For details, see Key algorithms supported by KMS .
Usage	ENCRYPT_DECRYPT	The value cannot be changed after the key is created. For AES_256 symmetric keys, the default value is ENCRYPT_DECRYPT .

Parameter	Example Value	Description
Source	Key Management Service	The following key material sources are supported: <ul style="list-style-type: none">• Key Management Service: KMS generates key materials.• External: Import local key materials to KMS.

4. Click **OK**. A message is displayed in the upper right corner of the page, indicating that the key is created. In the key list, you can view the created keys, which are in the **Enabled** state by default.

Step 3: Uploading Files to an OBS Bucket

Upload files to the OBS bucket and use the KMS key encrypt the files.


1. Click  on the left and choose **Storage > Object Storage Service**.
2. Click the bucket created in [Step 1: Creating a Bucket](#) to access its details page.
3. On the displayed page, click **Upload Object**. Then, configure the parameters as shown in [Figure 4-2](#). For details about the parameters, see [Table 4-3](#).

Figure 4-2 Uploading objects

×

1

Upload actions will generate [requests](#). After the upload, you will be billed for [data storage](#).

The total size of files to be uploaded at a time cannot exceed 5 GB. For more flexible upload options, use [OBS Browser+](#), [obsutil](#), [APIs](#), or [SDKs](#).

Storage Class

1

Inherit from bucket

Standard

Infrequent Access

Archive

If you do not change this setting, your uploaded objects will be stored using the default storage class you selected during bucket creation. [Learn more](#)

Upload Object

2

⚠

The file or folder you newly upload will overwrite any existing file or folder with the same name. To keep different versions of the same file or folder, enable versioning for the current bucket.

⊕

Drag and drop files or folders, or [add files](#)

(A maximum of 100 files can be uploaded at a time. The total size cannot exceed 5 GB.)

Server-Side Encryption

3

☒

Enabled

If server-side encryption is enabled, new objects uploaded to this bucket will be automatically encrypted. After a bucket is created, you can also change this encryption configuration on the bucket's overview page. [Learn more](#)

Encryption is recommended to keep data secure. Any requests filled over the quota limit will **be billed**. [Pricing details](#)

Encryption Method

4

SSE-KMS

SSE-OBS

If server-side encryption is enabled, new objects uploaded to this bucket will be automatically encrypted. After a bucket is created, you can also change this encryption configuration on the bucket's overview page. [Learn more](#)

Encryption Algorithm

5

AES256

Choose the algorithm you want to encrypt your data.

Encryption Key Type

6

Default

Custom

You can use a custom key below to encrypt your objects.

Custom

7

AES256 / KMS-335c

🔍

View KMS Keys

⌵

(Optional) Configure Advanced Settings


Issue 05 (2025-07-22)

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

26

Table 4-3 Mandatory parameters

Parameter	Example Value	Description
Storage Class	Inherit from bucket	<p>Storage class of the object. If this parameter is not specified, the objects you upload inherit the default storage class of the bucket.</p> <ul style="list-style-type: none">• Standard: It is for storing a large number of hot files or small files that are frequently accessed (multiple times per month on average) and require fast access.• Infrequent Access: It is for storing data that is less frequently accessed (less than 12 times per year on average), but when needed, the access has to be fast.• Archive: It is for archiving data that is rarely accessed (once a year on average) and does not require fast access.• Deep Archive: It is for storing data that is very rarely accessed and does not require fast access.
Upload Object	-	<p>Drag and drop the files or folders you want to upload to the Upload Object area.</p> <p>You can also click add files and choose the local files.</p>

Parameter	Example Value	Description
Server-Side Encryption		If server-side encryption is enabled, new objects uploaded to this bucket will be automatically encrypted.
Encryption Method	SSE-KMS	KMS generates and keeps keys, and OBS uses the keys to encrypt objects.
Encryption Key Type	Custom AES256/KMS-335c	Select the encryption key type. In this case, select the type of the key created in Step 2: Creating a Key .

4. Click **OK**.

5 Getting Started with Common Practices

After completing basic operations such as creating keys, key pairs, and secrets, you can get started with common Data Encryption Workshop (DEW) practices as needed.

Table 5-1 Common practices

Practice		Description
Data protection	Encrypting and Decrypting Small Amounts of Data	You can use online tools on the Key Management Service (KMS) console or call the necessary KMS APIs to directly encrypt or decrypt small-size data with a Customer Master Key (CMK), such as passwords, certificates, or phone numbers.
	Encrypting and Decrypting Large Amounts of Data	If you want to encrypt or decrypt large volumes of data, such as pictures, videos, and database files, you can use envelope encryption, which allows you to encrypt and decrypt files without having to transfer a large amount of data over the network.
	Using the Encryption SDK to Encrypt and Decrypt Local Files	Encryption Software Development Kit (SDK) can encrypt and decrypt data and file streams. You can easily encrypt and decrypt massive amounts of data simply by calling APIs. If large files and images are sent to KMS through HTTPS for encryption, a large number of network resources will be consumed and the encryption will be slow. You can use the encryption SDK to encrypt and decrypt local files.
	Encrypting and Decrypting Data Through Cross-region DR	If a fault occurs during encryption or decryption in a region, you can use KMS to implement cross-region DR encryption and decryption, ensuring service continuity.

Practice		Description
	Using KMS to Protect File Integrity	When a large amount of files (such as images, electronic insurance policies, and important files) need to be transmitted or stored securely, you can use KMS to sign the file digest. When the files are used again, you can recalculate the digest for signature verification. Ensure that files are not tampered with during transmission or storage.
Cloud services use KMS for encryption	Encryption in ECS	KMS supports one-click encryption for Elastic Cloud Server (ECS). The images and data disks of ECS can be encrypted. <ul style="list-style-type: none">When creating an ECS, if you select an encrypted image, the system disk of the created ECS automatically has encryption enabled, with its encryption mode same as the image encryption mode.When creating an ECS, you can encrypt added data disks.
	Encryption in OBS	When you enable server-side encryption in Object Storage Service (OBS): <ul style="list-style-type: none">An object uploaded to OBS is encrypted on the server before being stored.When the object is downloaded, data is decrypted on the server first. Server-side encryption with KMS-managed keys (SSE-KMS) can be implemented for the objects to be uploaded.
	Encryption in EVS	In case your services require encryption for the data stored on disks, KMS is integrated with Elastic Volume Service (EVS). You can use the key provided by KMS to encrypt the disk.
	Encryption in IMS	When creating a private image, you can select KMS encryption and use the key provided by KMS to encrypt the image, ensuring image data security.
	Encrypting an RDS Database	After encryption is enabled, disk data will be encrypted and stored on the server when you create a Relational Database Service (RDS) database instance or expand disk capacity. When you download encrypted objects, the encrypted data will be decrypted on the server and displayed in plaintext.

Practice		Description
	Encrypting a DDS Database	After encryption is enabled, disk data will be encrypted and stored on the server when you create a Document Database Service (DDS) database instance or expand disk capacity. When you download encrypted objects, the encrypted data will be decrypted on the server first.
Secret encryption	Using CSMS to Change Hard-coded Database Account Passwords	Generally, the secrets used for access are embedded in applications. To update a secret, you need to create a secret and spend time updating your applications. CSMS is required to manage credentials more conveniently, efficiently, and securely.
	Using CSMS to Prevent AK and SK Leakage	You can use Identity and Access Management (IAM) to obtain temporary access keys for ECS to protect AKs and SKs.
	Using CSMS to Automatically Rotate Security Passwords	Use FunctionGraph and CSMS to generate, host, and rotate strong secure passwords periodically.
	Rotating a Secret for a User	You can update the information of a user in a secret. This is the most commonly used secret rotation policy.
	Rotating a Secret for Two Users	You can update the information of two users in a secret. To prevent access failures when changing the user password and updating the secret content, use the multi-user secret rotation policy to ensure high availability of applications.
	Rotating IAM Secrets Using FunctionGraph	Use the function workflow template and CSMS to rotate IAM secrets.
API calling	Retrying Failed DEW Requests by Using Exponential Backoff	If you receive an error message when calling an API, you can use exponential backoff to retry the request.