Data Encryption Workshop

Getting Started

Issue 04

Date 2025-08-08

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

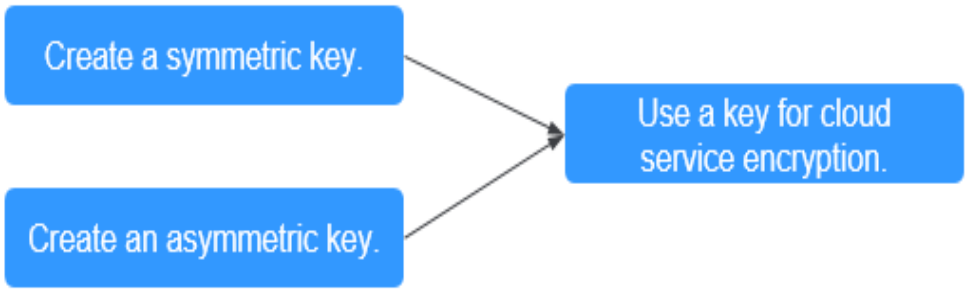
A key can be symmetric or asymmetric.

- 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**.
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

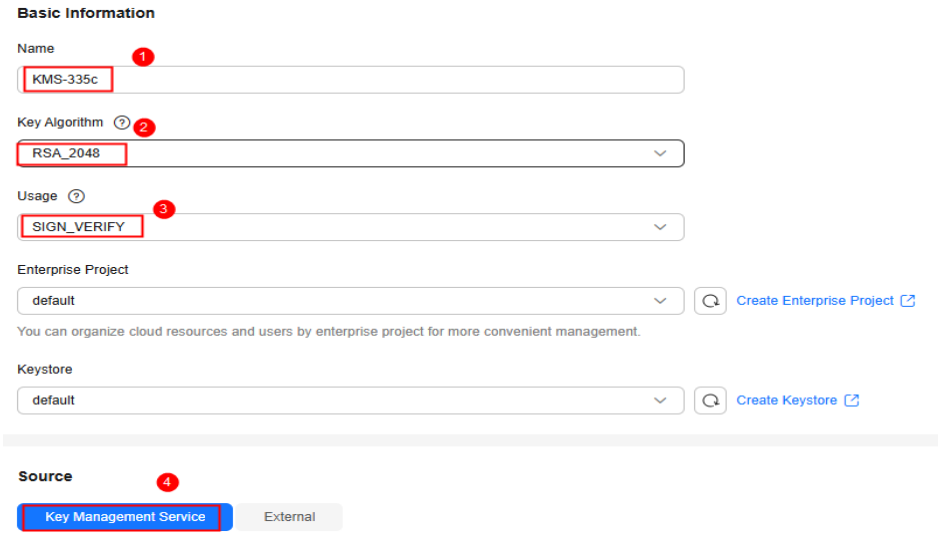


Table 1-2 Mandatory parameters

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**.
Usage	ENCRYPT_DECRYPT	The value cannot be changed after the key is created. For AES_256 symmetric keys, the default value is **ENCRYPT_DECRYPT**.

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

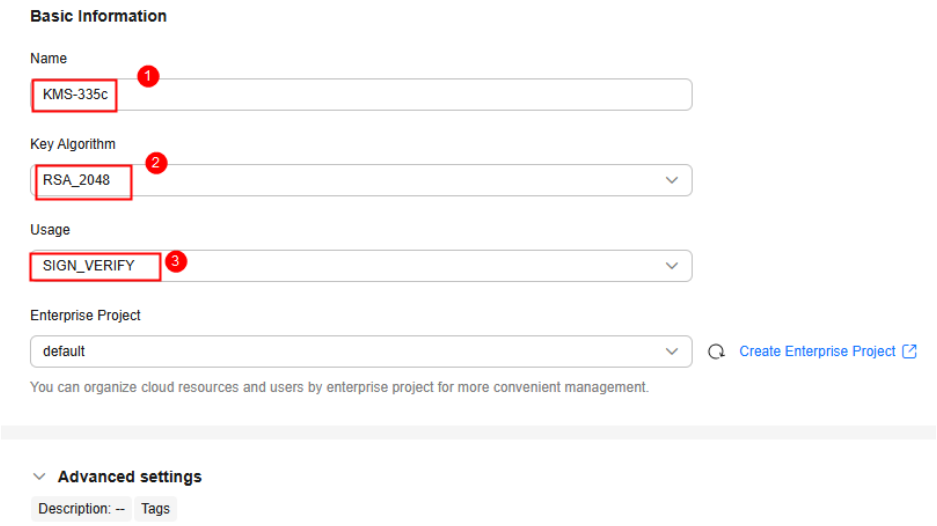


Table 1-3 Mandatory parameters

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**.

Parameter	Example Value	Description
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**.

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

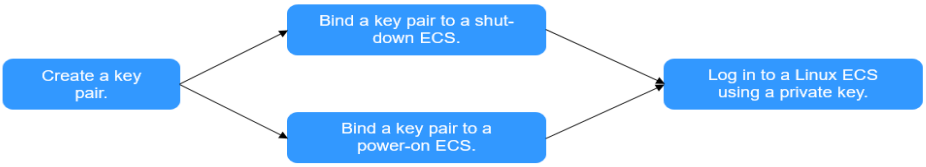
A key pair, including one public key and one private key, are generated based on a cryptographic algorithm. The public key is automatically saved in Key Pair Service (KPS), while the private key can be saved to the user's local host. If you have configured the public key in a Linux ECS, you can use the 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 2-1 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 • **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**.
2. An ECS has been created. For details, see **Purchasing a Spot ECS**.

   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 .
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 2-1 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 2-2**. For details about the parameters, see **Table 2-2**.

Figure 2-2 Creating a private key pair

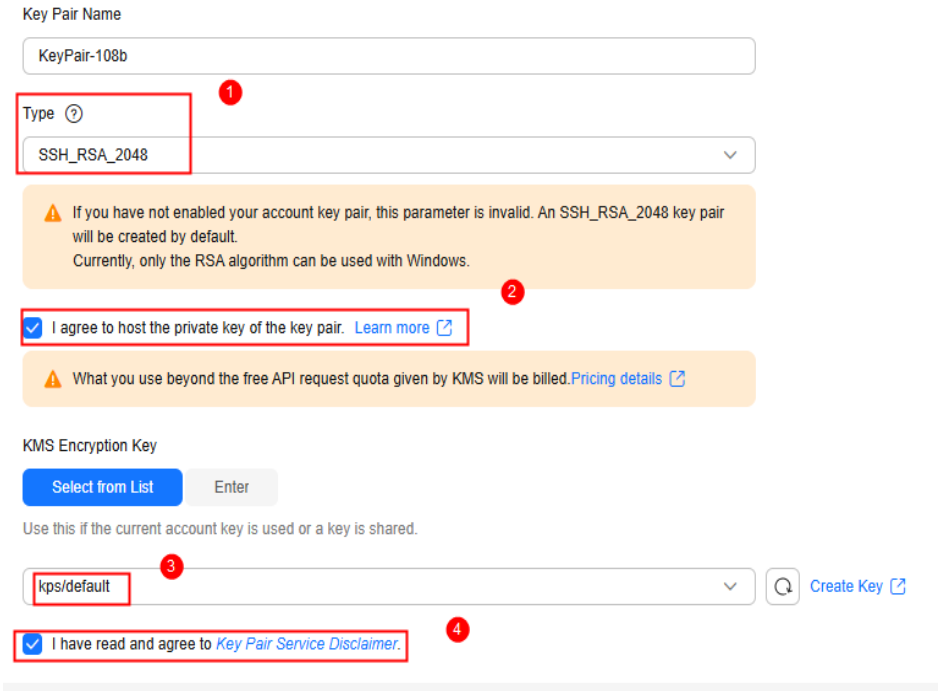


Table 2-2 Parameters for creating a private key pair

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: • **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

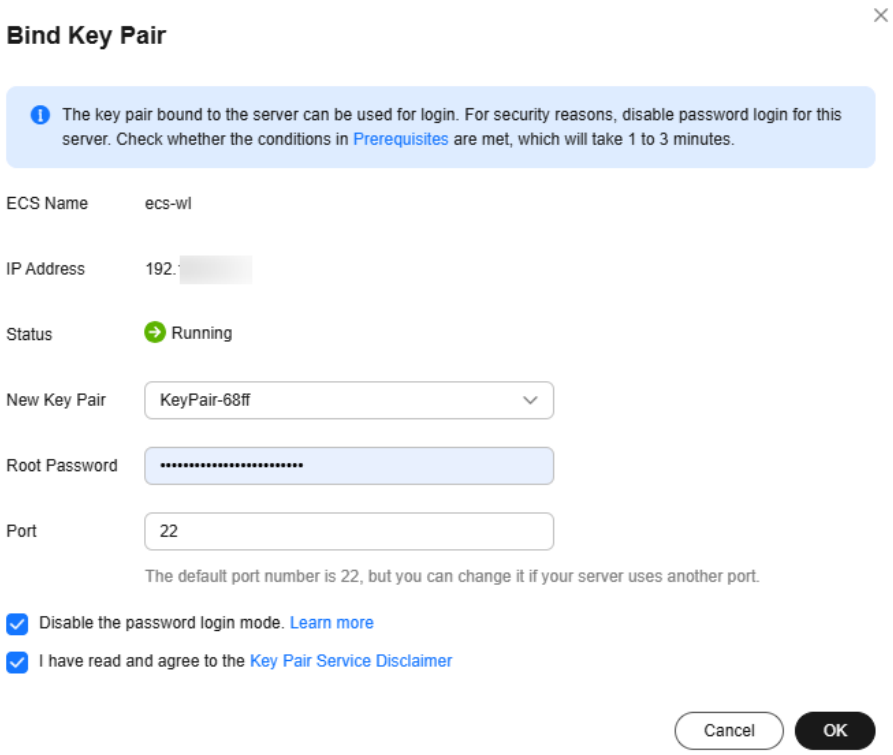
1. In the navigation pane on the left, choose **Key Pair Service**. On the displayed page, click the **ECS List** tab.
2. Locate the target shut-down ECS and click **Bind** in the **Operation** column.
3. On the displayed page, select a key pair. Then, select **Disable the password login mode** and **I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

- 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 2-3 Binding a key pair



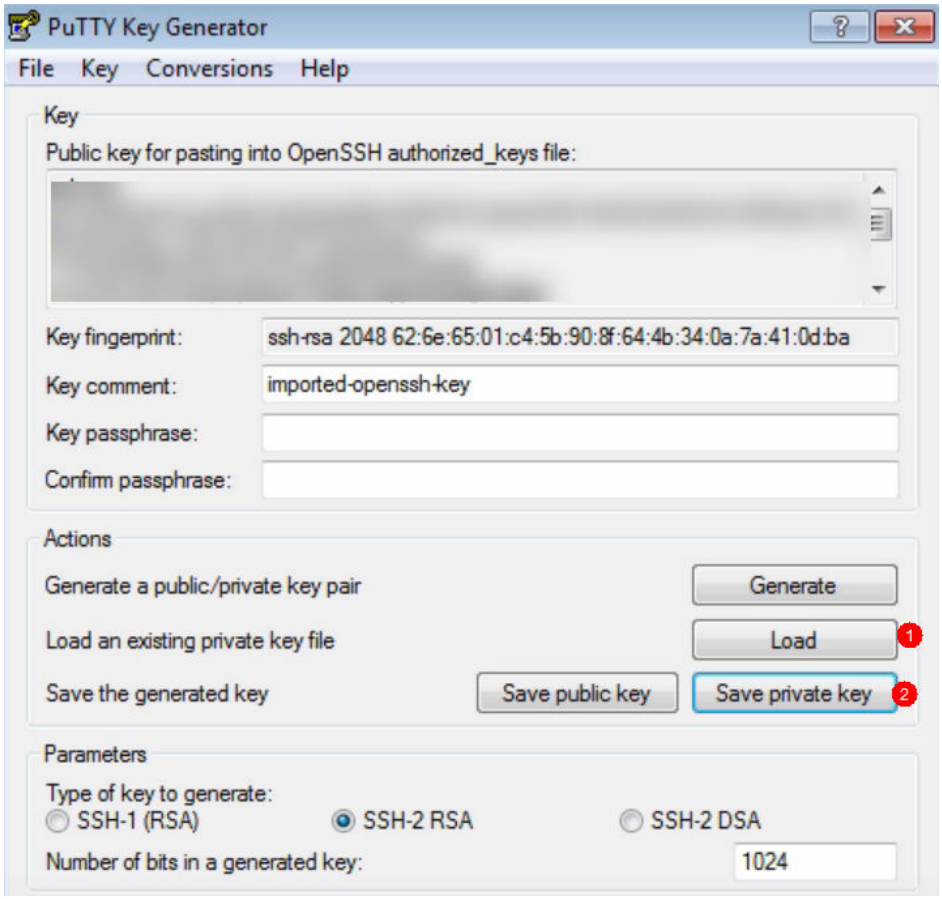
4. Click **OK**.

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.

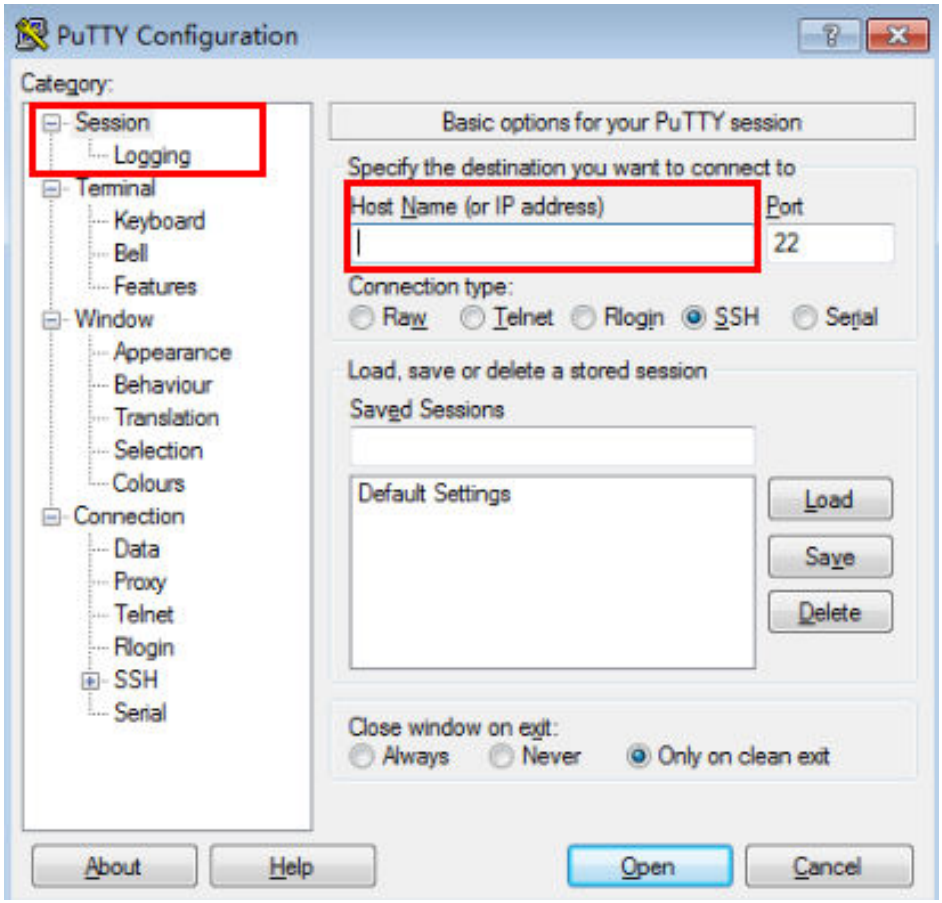
     Open the third-party PuTTY, import the .pem private key file, and export the converted .ppk private key file.

Figure 2-4 Converting the format of the private key file



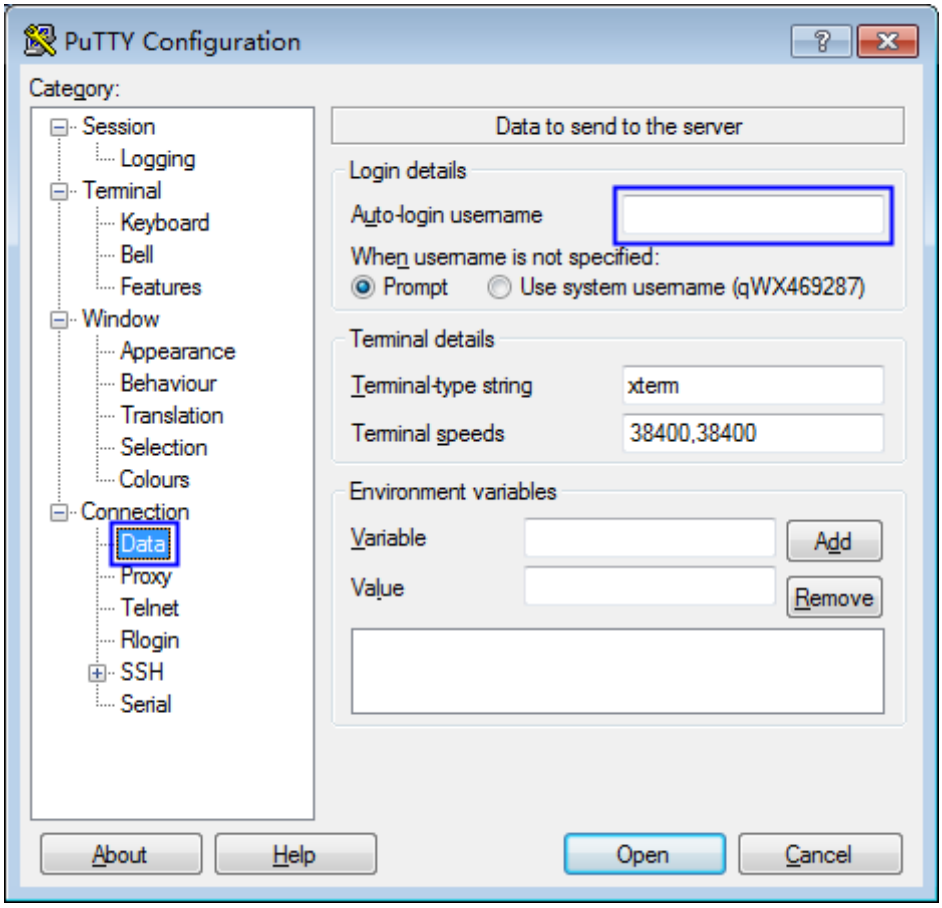
2. Use PuTTY to log in to ECS.
   - Enter the IP address of the ECS. Port **22** is used by default.

Figure 2-5 IP address of ECS



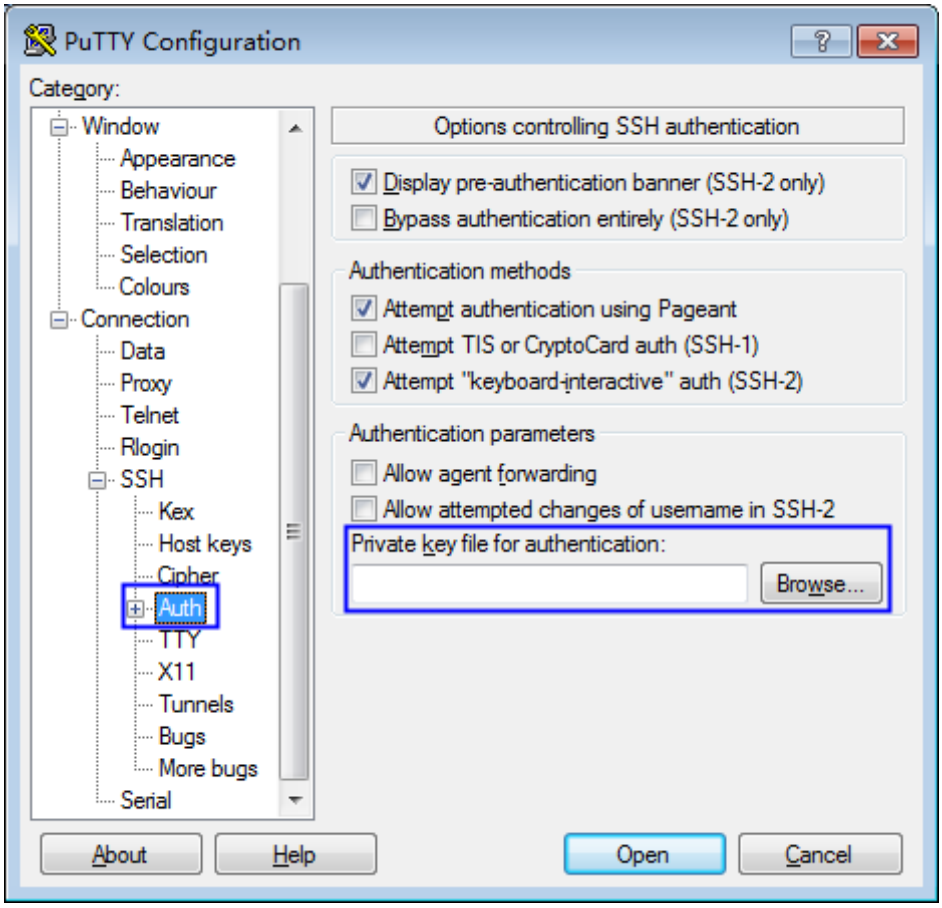
– Enter the username of the ECS image.

Figure 2-6 Username



– Upload the private key file in .ppk format.

Figure 2-7 Uploading the private key file



– Click **Open**.

3 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**.
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 3-1 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.

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 3-2**.

Figure 3-1 Creating a key

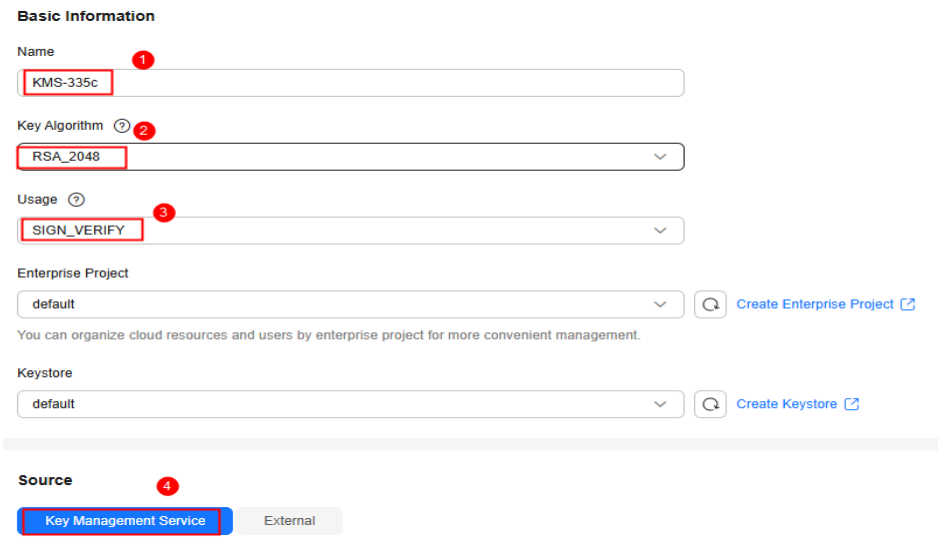


Table 3-2 Mandatory parameters

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**.

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 3-2**. For details about the parameters, see **Table 3-3**.

Figure 3-2 Uploading objects

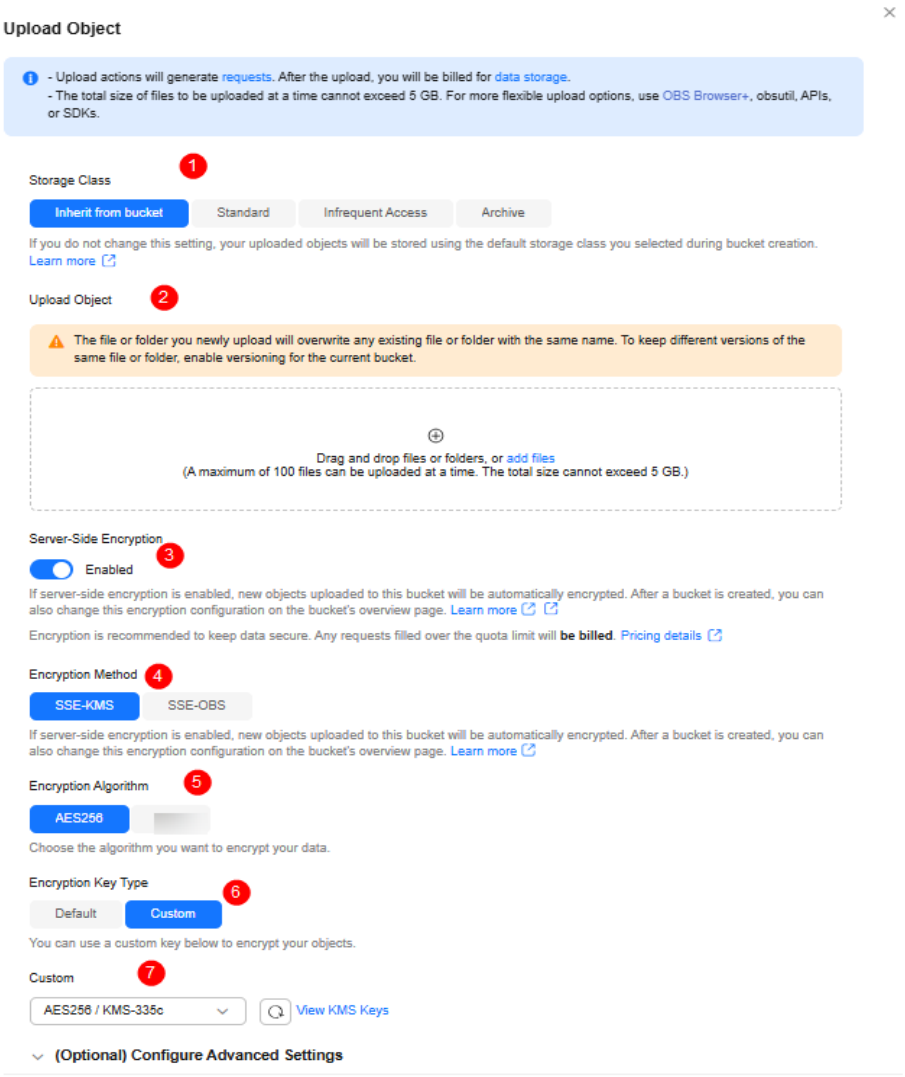


Table 3-3 Mandatory parameters

Parameter	Example Value	Description
Storage Class	Inherit from bucket	Storage class of the object. If this parameter is not specified, the objects you upload inherit the default storage class of the bucket. • **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	-	Drag and drop the files or folders you want to upload to the **Upload Object** area. You can also click **add files** and choose the local files.

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**.

4 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 4-1 Common practices

Practice		Description
Data protection	**Encrypting or Decrypting Small Volumes of Data**	You can use online tools on the Key Management Service (KMS) console or call the required KMS APIs to directly encrypt or decrypt small-volume data with a Customer Master Key (CMK), such as passwords, certificates, or phone numbers.
	Encrypting or Decrypting a Large Amount 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.
Cloud services use KMS for encryption	**Encrypting Data in ECS**	KMS supports one-click encryption for Elastic Cloud Server (ECS). The images and data disks of ECS can be encrypted. • 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.

Practice		Description
	Encrypting Data in OBS	When you enable server-side encryption in Object Storage Service (OBS): • 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.
	Encrypting Data 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.
	Encrypting Data 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 DB Instance	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.
	Encrypting a DDS DB Instance	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.
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.

