

# Data Encryption Workshop

## Getting Started

**Issue** 01  
**Date** 2024-11-29



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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.....	5
3 Binding a Key Pair and Logging In to an ECS Using a Private Key.....	8
4 Using a Key to Encrypt Data in OBS.....	15
5 Logging In to a Linux ECS Using a Private Key.....	16
6 Getting Started with Common Practices.....	21

# 1 Creating a Key for Cloud Service Encryption

---

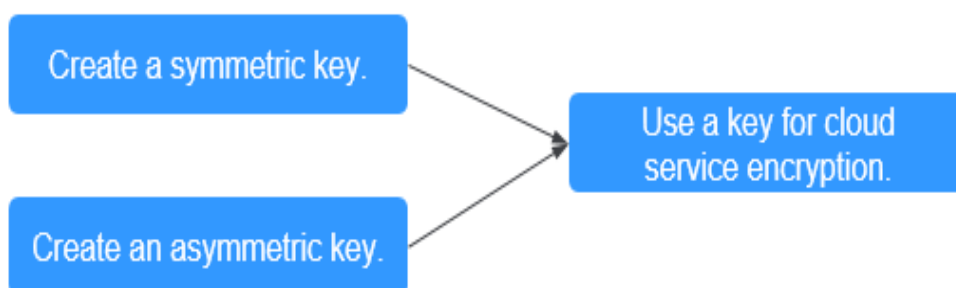
A key can be symmetric or asymmetric.

- 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
<b>Preparations</b>	Register a Huawei ID, enable Huawei Cloud services, top up the account, and grant KMS permissions to the account.
<ul style="list-style-type: none"> <li>• <b>Creating a Symmetric Key</b></li> <li>• <b>Creating an Asymmetric Key</b></li> </ul>	Create a key and select the key algorithm type.
<b>Cloud Service Encryption</b>	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](#) and [Real-Name Authentication](#).  
If you have enabled Huawei Cloud services and completed real-name authentication, 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


## Creating a Key

The following describes how to create a key.


## Creating a Symmetric Key

1. **Log in to the management console.** Click  on the left and choose **Security & Compliance > Data Encryption Workshop**.
2. On the displayed **Key Management Service** page, click **Create Key** in the upper right corner.
3. Configure the parameters as follows:
  - **Key Algorithm:** Choose **AES\_256**.  
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. For details about regions of replica keys, see [Function Overview](#).
  - Set other parameters as needed.
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

1. **Log in to the management console.** Click  on the left and choose **Security & Compliance > Data Encryption Workshop**.
2. On the displayed **Key Management Service** page, click **Create Key** in the upper right corner.
3. Configure the parameters as follows:
  - **Key Algorithm:** Choose **RSA\_2048**.  
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. For details about regions of replica keys, see [Function Overview](#).
  - Set other parameters as needed.
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 a Digest Key

1. **Log in to the management console.** Click  on the left and choose **Security & Compliance > Data Encryption Workshop**.
2. On the displayed **Key Management Service** page, click **Create Key** in the upper right corner.
3. Configure the parameters as follows:
  - **Key Algorithm:** Choose **HMAC\_256**.  
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. For details about regions of replica keys, see [Function Overview](#).
  - Set other parameters as needed.

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.

## 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](#)

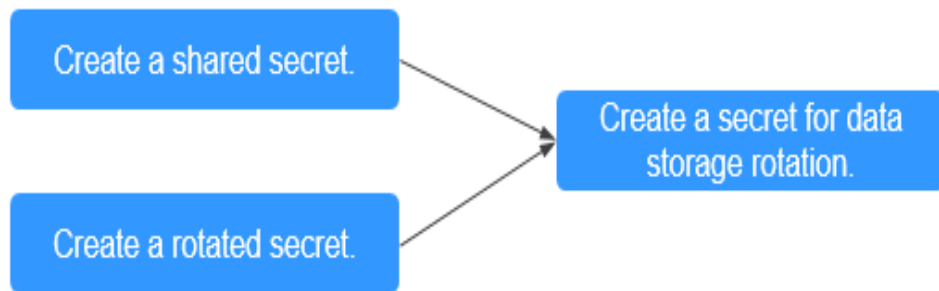
# 2 Creating a Secret for Data Storage Rotation

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 key for cloud service encryption



Procedure	Description
<b>Preparations</b>	Register a Huawei ID, enable Huawei Cloud services, top up the account, and grant CSMS permissions to the account.
<ul style="list-style-type: none"><li>• <b>Creating a Shared Secret</b></li><li>• <b>Creating a Rotated Secret</b></li></ul>	Create a secret and choose the secret type.




Procedure	Description
<a href="#">Data Rotation</a>	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](#) and [Real-Name Authentication](#).  
If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Before purchasing an instance, ensure that your account balance is sufficient. For details, see [Top-Up and Repayment](#).
3. You have created an encryption key on KMS.
  - The default key is **csms/default**.
  - Select the custom keys created on KMS. For details, see [Creating a Key](#).
4. Before using a rotated secret, you need to create a database instance and database account.
  - For details about how to create an RDS instance, see [Buying an RDS for MySQL DB Instance](#).
  - For details about how to create a GaussDB instance, see [Buying a GaussDB Instance](#).

## Creating a Shared Secret

1. [Log in to the management console](#). Click  on the left and choose **Security & Compliance > Data Encryption Workshop**.
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. Configure the parameters as follows:
  - **Type**: Select **Shared secret**.  
The created secret can be used only in the current region. To use it in other regions, switch to the target region and create a secret. For details about regions of secret management, see [Function Overview](#).
  - **KMS Encryption Key**: Choose the default key or a created key from the list.
  - Set other parameters as needed.
4. Click **OK**. In the secret list, you can view the created secrets, which are in the **Enabled** state by default.

## Creating a Rotated Secret

1. **Log in to the management console.** Click  on the left and choose **Security & Compliance > Data Encryption Workshop**.
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. Configure the parameters as follows:
  - **Type:** Select **Rotated secret** and choose an **RDS secret** or **GaussDB(for MySQL) secret**.  
The created secret can be used only in the current region. To use it in other regions, switch to the target region and create a secret. For details about regions of secret management, see [Function Overview](#).
  - **KMS Encryption Key:** Choose the default key or a created key from the list.
  - **Secret Value:** Choose the created database account and enter the password.
  - Set other parameters as needed.
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.

## Data Rotation

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

- [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

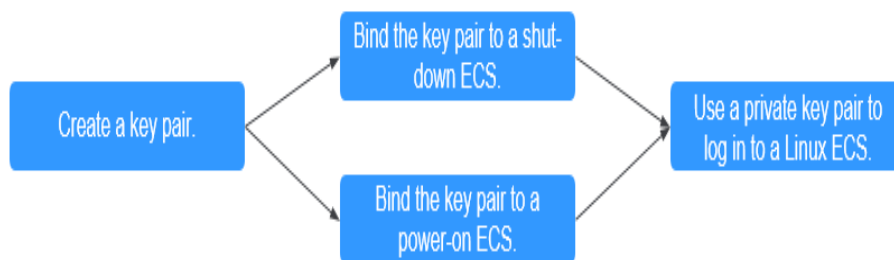
A key pair, including one public key and one private key, are generated based on a cryptographic algorithm. The public key is automatically saved in Key Pair Service (KPS), while the private key can be saved to the user's local host. If you have configured the public key in a Linux ECS, you can use the 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
<a href="#">Preparations</a>	Register a Huawei ID, enable Huawei Cloud services, top up the account, and grant KPS permissions to the account.
<a href="#">Step 1: Creating a Key Pair</a>	Create a key pair and select the key pair type.
<ul style="list-style-type: none"><li>• <a href="#">Step 2: Binding a Key Pair to a Shut-down ECS</a></li><li>• <a href="#">Step 2: Binding a Key Pair to a Running ECS</a></li></ul>	Bind a key pair to the ECS.
<a href="#">Step 3: Logging in to an ECS Using a Private Key</a>	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](#) and [Real-Name Authentication](#).  
If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. An ECS has been created. For details, see [Purchasing a Custom 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 [Enhancing Security for SSH Logins to Linux ECSs](#).
3. You have created an encryption key on KMS.
  - The default key is **kps/default**.
  - Select the custom keys created on KMS. For details, see [Creating a Key](#).


## Step 1: Creating a Key Pair

1. [Log in to the management console](#). Click  on the left and choose **Security & Compliance > Data Encryption Workshop**.
2. In the navigation pane on the left, choose **Key Pair Service**. Click the **Private Key Pairs** tab and click **Create Key Pair** in the upper left corner.
3. Configure the parameters as follows:
  - **Type**: Choose **SSH\_RSA\_2048**.
  - Select **I agree to manage the private key of the key pair**.
  - **KMS Encryption Key**: Choose the default key or a created key from the list.
  - Select **I have read and agree to the Key Pair Service Disclaimer**.
4. Click **OK**. The private key file is downloaded automatically. When a message is displayed, indicating that the download is complete, save the private key file.

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

1. **Log in to the management console.** Click  on the left and choose **Security & Compliance > Data Encryption Workshop**.
2. In the navigation pane on the left, choose **Key Pair Service**. In the **ECS List** tab, locate the target ECS in the **Shut down** state, and click **Bind** in the **Operation** column.
3. Configure the parameters as follows:
  - **New Key Pair:** Choose the target key pair from the drop-down list.
  - Select **Disable the password login mode**.
  - Select **I have read and agree to the Key Pair Service Disclaimer**.
4. Click **OK**.

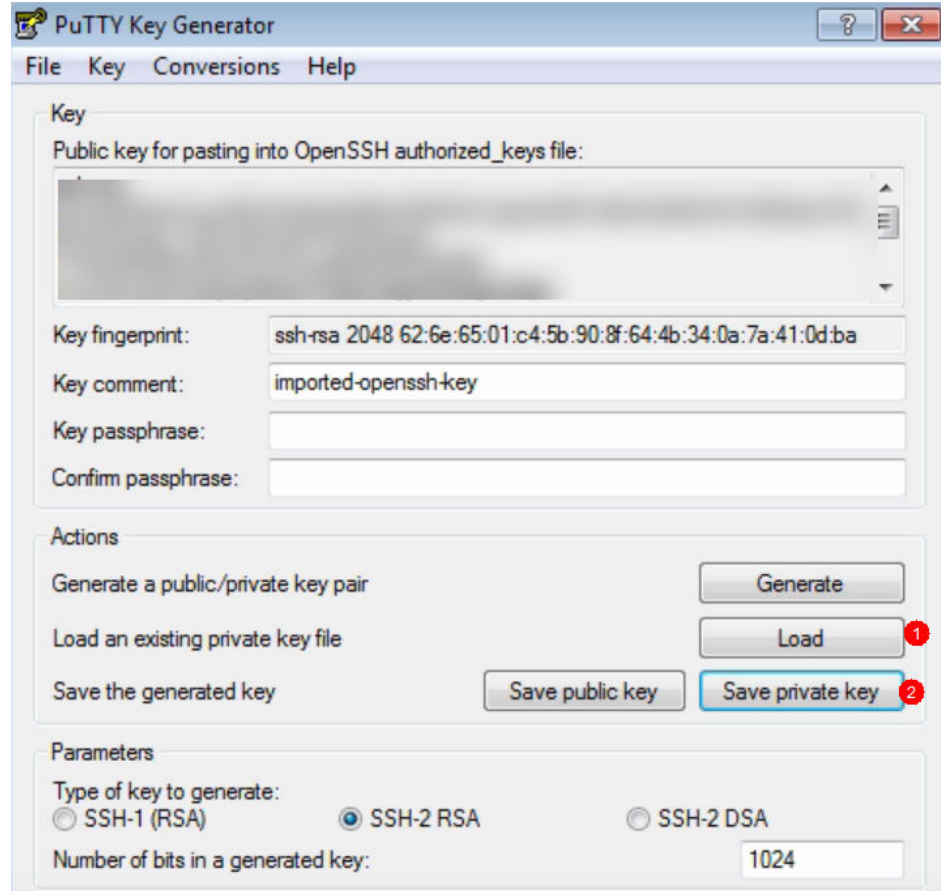
## Step 2: Binding a Key Pair to a Running ECS

1. **Log in to the management console.** Click  on the left and choose **Security & Compliance > Data Encryption Workshop**.
2. In the navigation pane on the left, choose **Key Pair Service**. In the **ECS List** tab, locate the target ECS in the **Running** state, and click **Bind** in the **Operation** column.
3. Configure the parameters as follows:
  - **New Key Pair:** Choose the target key pair from the drop-down list.
  - Enter the password of user **root**.
  - The default port is **22**.
  - Select **Disable the password login mode**.
  - Select **I have read and agree to the Key Pair Service Disclaimer**.
4. Click **OK**.

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

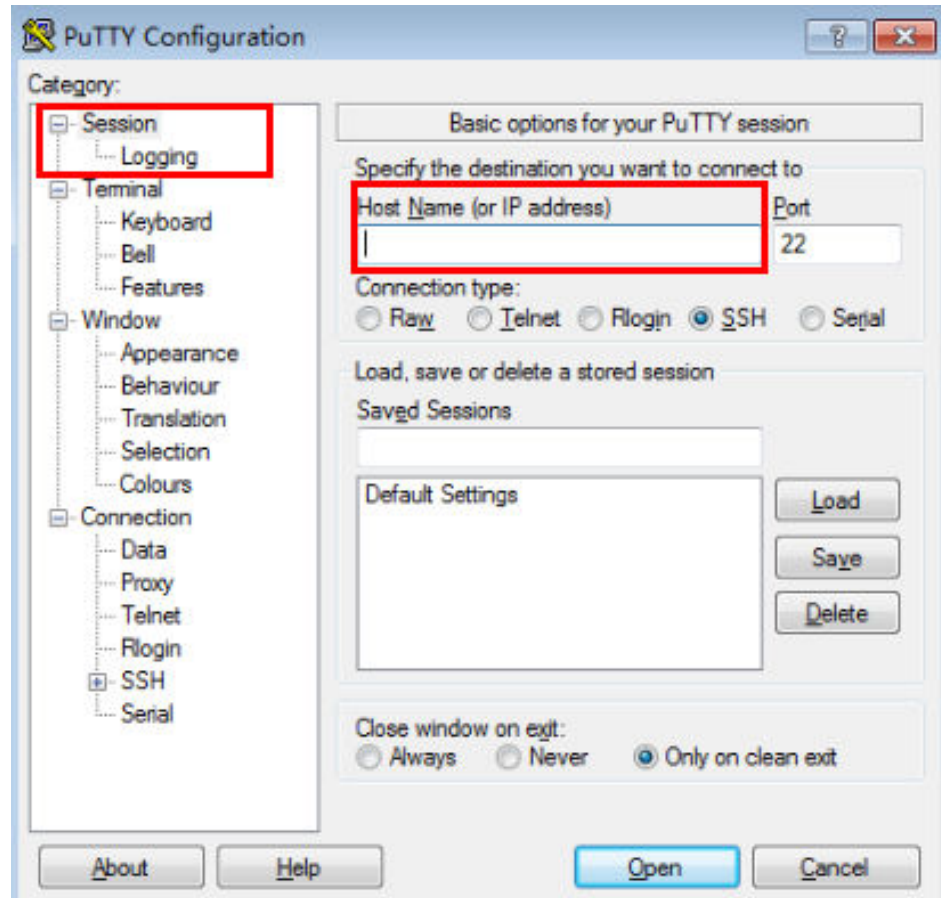
1. Check whether the private key file has been converted to .ppk format.
  - If yes, log in to the ECS server.
  - If no, perform the following operations to convert the format of the private key file and then log in to ECS.  
Open the third-party PuTTY, import the .pem private key file, and export the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

**Figure 3-2** Converting the format of the private key file



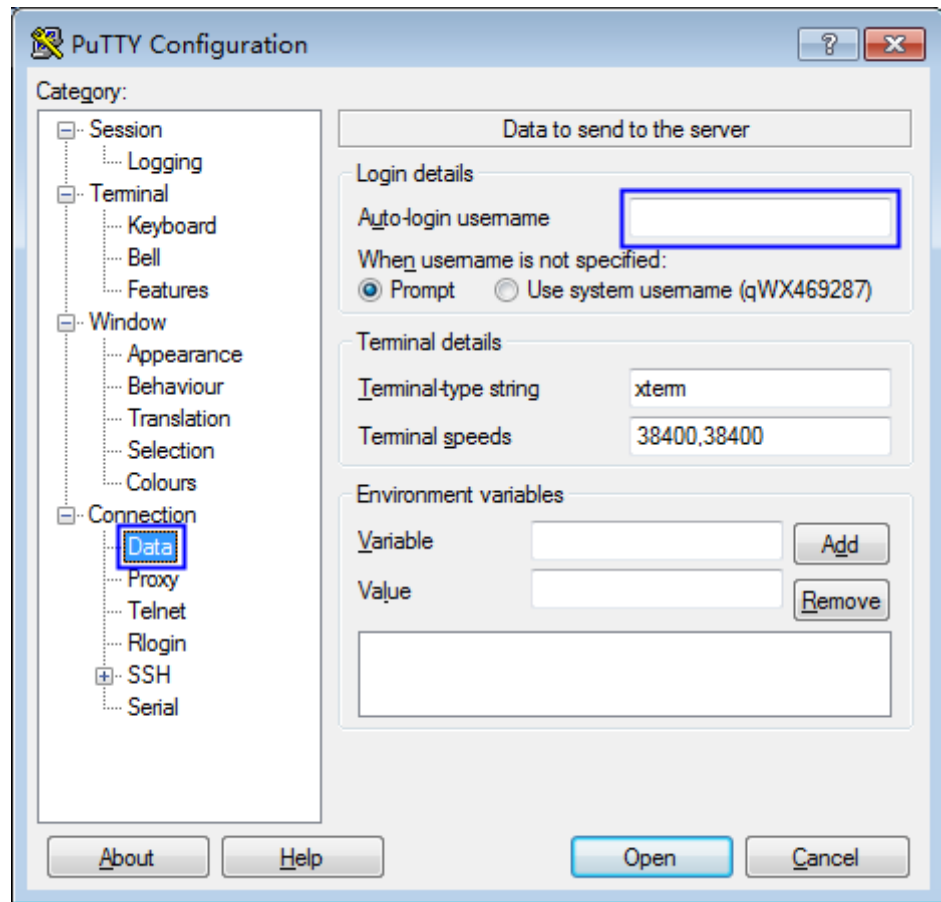
2. Use PuTTY to log in to ECS.
  - Enter the IP address of the ECS. Port 22 is used by default.

Figure 3-3 IP address of ECS



- Enter the username of the ECS image.

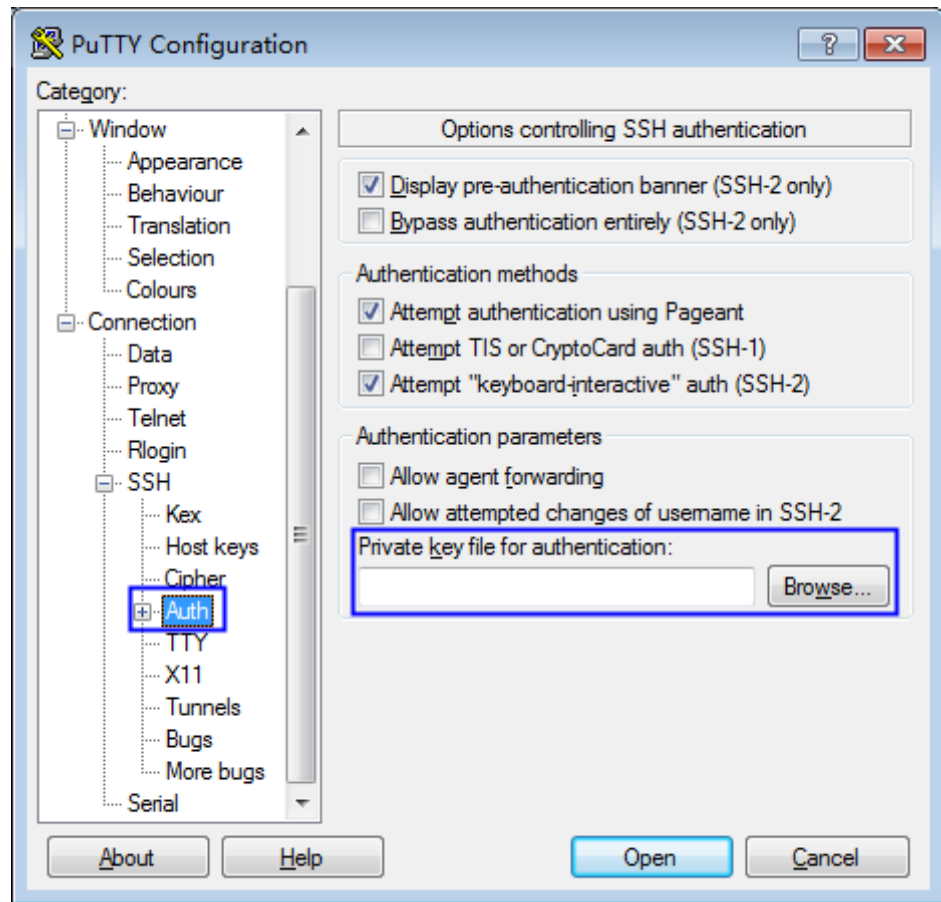
Figure 3-4 Username



- Upload the private key file in .ppk format.



**Figure 3-5** Uploading the private key file



- Click **Open**.

# 4 Using a Key to Encrypt Data in OBS

---

- DEW is a cloud data encryption service. The 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.

## Step 1 Preparing the Environment

1. Log in to the [management console](#). In the navigation pane on the left, choose **Storage > Object Storage Service**.
2. On the displayed page, click **Create Bucket** to store uploaded files.

## Step 2 Creating a Key

1. Log in to the management console. In the navigation pane on the left, choose **Security > Data Encryption Workshop**.
2. On the displayed **Key Management Service** page, click **Create Key** in the upper right corner.
3. On the **Create Key** page, enter the key alias and description, and click **OK**.

### NOTE

You can also import your local keys to the KMS console and have them managed by KMS. For details about how to import keys, see [Importing Key Materials](#).

## Step 3 Uploading Files to an OBS Bucket

1. Log in to the management console. In the navigation pane on the left, choose **Storage > Object Storage Service**. On the displayed page, click a bucket name to go to its details page.
2. In the **Objects** tab, click **Upload Object**.
3. Select the files to be uploaded, set **Encryption Method** to **SSE-KMS**, configure **Encryption Key Type**, and click **Upload**.

# 5 Logging In to a Linux ECS Using a Private Key

---

- DEW is a cloud data encryption service. The Key Pair Service (KPS) provided by DEW is a secure, reliable, and easy-to-use key pair management service. As an alternative to the traditional username+password authentication method, key pairs allow you to remotely log in to Linux ECSs.
- 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 Huawei Cloud, while the private key can be saved to your local host. You can also save your private keys in Huawei Cloud and have them managed by KPS.
- The following shows how to use a created key pair to log in to a Linux ECS, helping you understand KPS better.

## Step 1 Preparing the Environment

1. Log in to the [management console](#).
2. In the navigation pane on the left, choose **Compute > Elastic Cloud Server**. On the displayed page, create an ECS to bind a key pair.

## Step 2 Creating a Key Pair

1. Log in to the [management console](#) and choose **Security > Data Encryption Workshop** from the left.
2. In the navigation pane on the left, choose **Key Pair Service**. On the displayed page, click **Create Key Pair**.

### NOTE

- You can choose whether to host your private keys on Huawei Cloud as needed.
- To ensure ECS security, private keys that are not managed by Huawei Cloud can be downloaded only once. Keep your downloaded private keys properly. Private keys that are managed by Huawei Cloud can be exported anytime you need.

## Step 3 Binding a Key Pair

1. On the **Key Pair Service** page, click the **ECS List** tab.

2. Locate the target ECS in the list and click **Bind** in the **Operation** column. In the displayed **Bind Key Pair** dialog box, configure the parameters, and click **OK**.

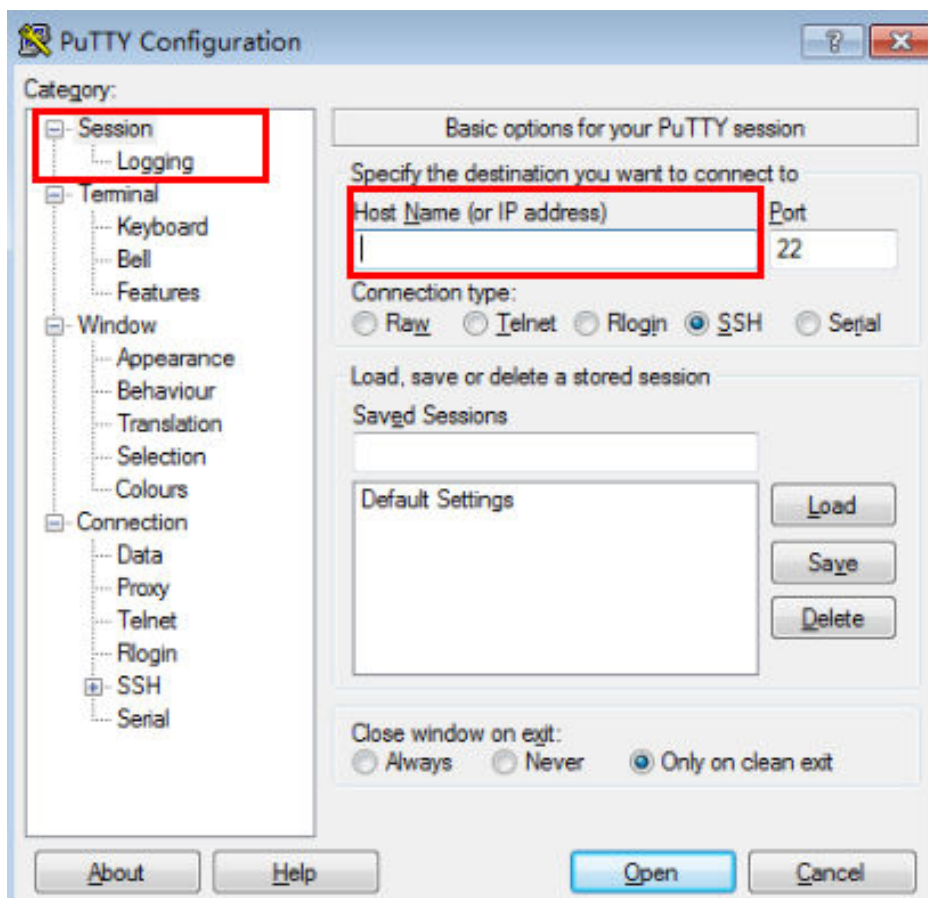
 **NOTE**

- If you have the root password of the ECS, directly enter the password to bind the key pair to the ECS.
- If you do not have the root password of the ECS, shut down ECS, wait until it is stopped, and then bind the key pair to the ECS.

## Step 4 Logging In to an ECS Using a Private Key

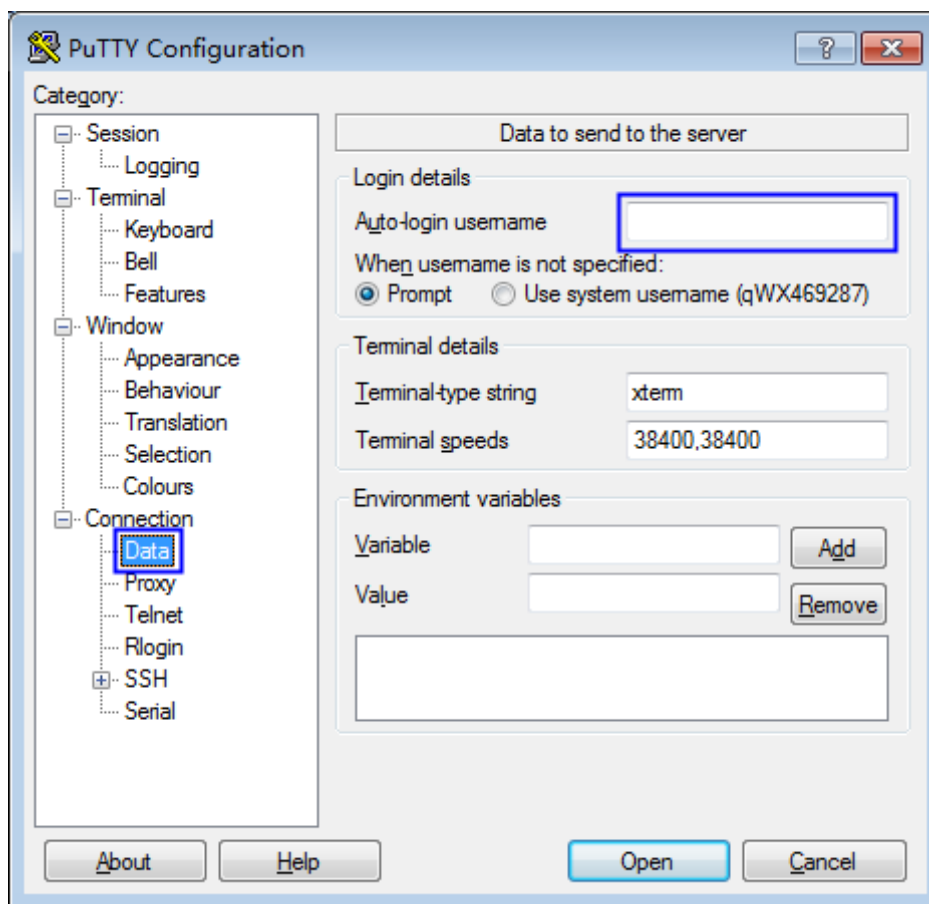
1. Open PuTTY.

**Figure 5-1** IP address of the ECS



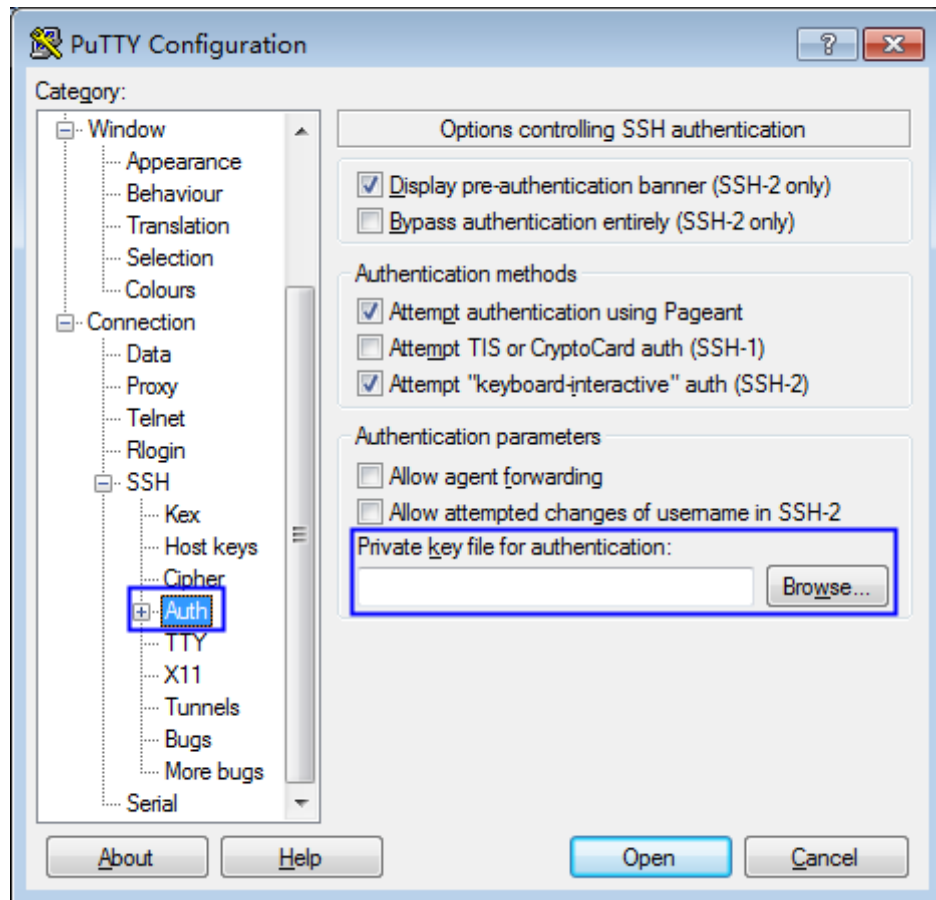
2. Enter the username of the ECS image.

Figure 5-2 Username



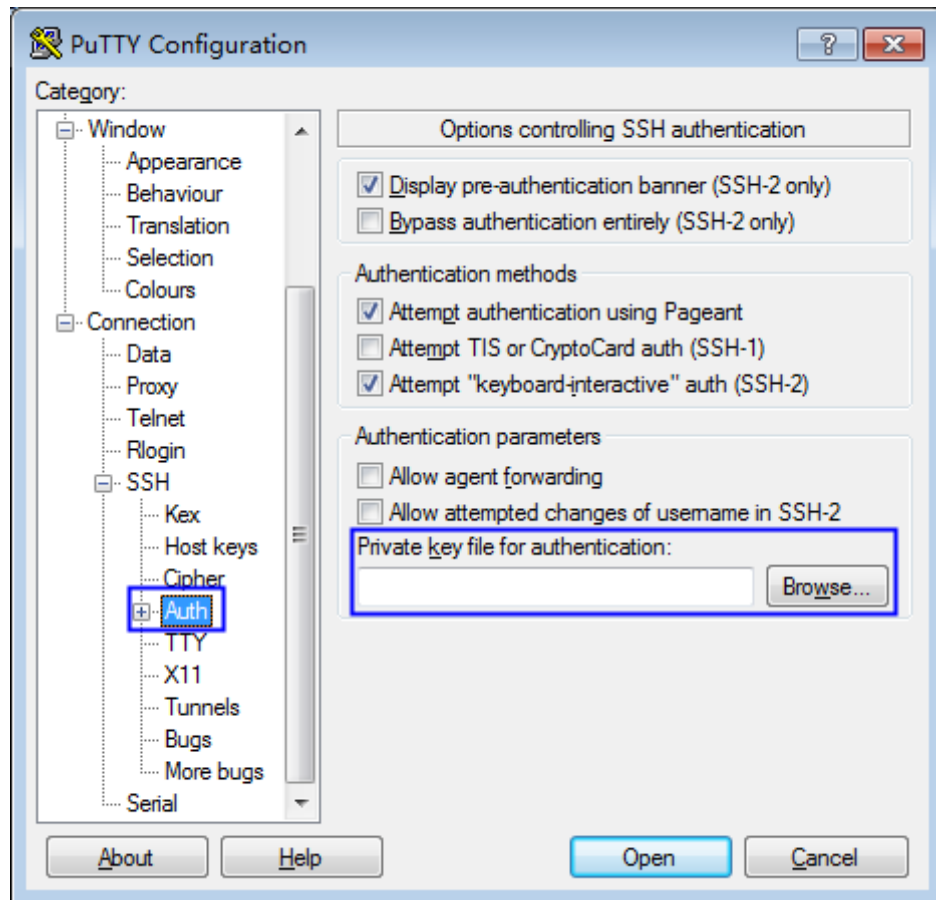
3. Upload the .ppk private key file.

Figure 5-3 Uploading the private key file



4. Enter the elastic IP address of the ECS.

Figure 5-4 Uploading the private key file



**NOTE**

- If the public image is a CoreOS image, the username is **core**. In other occasions, the username is **root**.
- The private key file to be uploaded must be a .ppk file.

# 6 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 6-1** Common practices

Practice		Description
Data protection	<b>Encrypting and Decrypting Small Amounts of Data</b>	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.
	<b>Encrypting and Decrypting Large Amounts of Data</b>	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.
	<b>Using the Encryption SDK to Encrypt and Decrypt Local Files</b>	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.
	<b>Encrypting and Decrypting Data Through Cross-region DR</b>	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
	<b>Using KMS to Protect File Integrity</b>	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	<b>Encryption in ECS</b>	<p>KMS supports one-click encryption for Elastic Cloud Server (ECS). The images and data disks of ECS can be encrypted.</p> <ul style="list-style-type: none"> <li>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.</li> <li>When creating an ECS, you can encrypt added data disks.</li> </ul>
	<b>Encryption in OBS</b>	<p>When you enable server-side encryption in Object Storage Service (OBS):</p> <ul style="list-style-type: none"> <li>An object uploaded to OBS is encrypted on the server before being stored.</li> <li>When the object is downloaded, data is decrypted on the server first.</li> </ul> <p>Server-side encryption with KMS-managed keys (SSE-KMS) can be implemented for the objects to be uploaded.</p>
	<b>Encryption in EVS</b>	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.
	<b>Encryption in IMS</b>	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.
	<b>Encrypting an RDS Database</b>	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
	<a href="#">Encrypting a DDS Database</a>	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	<a href="#">Using CSMS to Change Hard-coded Database Account Passwords</a>	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.
	<a href="#">Using CSMS to Prevent AK and SK Leakage</a>	You can use Identity and Access Management (IAM) to obtain temporary access keys for ECS to protect AKs and SKs.
	<a href="#">Using CSMS to Automatically Rotate Security Passwords</a>	Use FunctionGraph and CSMS to generate, host, and rotate strong secure passwords periodically.
	<a href="#">Rotating a Secret for a User</a>	You can update the information of a user in a secret. This is the most commonly used secret rotation policy.
	<a href="#">Rotating a Secret for Two Users</a>	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.
	<a href="#">Rotating IAM Secrets Using FunctionGraph</a>	Use the function workflow template and CSMS to rotate IAM secrets.
API calling	<a href="#">Retrying Failed DEW Requests by Using Exponential Backoff</a>	If you receive an error message when calling an API, you can use exponential backoff to retry the request.