

# **Tencent Cloud Lighthouse**

## **Operation Guide**

### **Product Documentation**



## Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

# Contents

## Operation Guide

### Logging In to Linux Instances

Logging in to Linux Instance via Tencent Cloud OrcaTerm

Logging in to Linux Instance via Remote Login Software

Logging in to Linux Instance via SSH Key

Logging in to Linux Instance via VNC

### Logging in Windows Instance

Logging in to Windows Instance via VNC

Logging in to Windows Instance via Remote Desktop Connection

## Managing Instances

### Resetting the instances passwords

Password Reset Operation Instruction

Troubleshoot the Issue That the Password Fails To Be Reset Online or Is Invalid

Troubleshoot the Issue That the Password Reset Fails To Be Reset Offline or Is Invalid for The Windows Instance

### Binding Key

### Viewing Instance Information

Shutting down Instance

Restarting Instance

Terminating Instance

Renewing Instance

Reinstalling System

Upgrading Instance Package

Managing Instance Tag

Changing Instance Public IP

### Batch Operations

## Working with Cloud Disks

Creating Cloud Disks

Attaching Cloud Disks

Initializing Cloud Disks

Renewing Cloud Disks

Detaching Cloud Disks

Terminating Cloud Disks

## Managing Keys

## Managing Firewall

Manage instance firewall

Managing Snapshot

Managing Image

- Working with Custom Images

- Replicating Custom Images Across Regions

- Share Custom Images

- Tencent Cloud Support for Lighthouse Images

Private Network Interconnection

OPS and Monitoring

- Instance Monitoring

Access Management

- CAM Overview

- Authorizable Resource Types

- Authorization Policy Syntax

Transferring File

- Uploading Local Files to Lighthouse

- Uploading File from Windows to Linux Lighthouse Instance via WinSCP

- Uploading File from Windows to Lighthouse Instance via FTP

- Uploading File from Windows to Windows Lighthouse Instance via Remote Desktop Connection

- Uploading File from Linux or macOS to Linux Lighthouse Instance via SCP

- Uploading File from Linux or macOS to Lighthouse Instance via FTP

- Uploading File from Linux to Windows Lighthouse Instance via rdesktop

- Uploading File from macOS to Windows Lighthouse Instance via MRD



# Operation Guide

## Logging In to Linux Instances

### Logging in to Linux Instance via Tencent Cloud OrcaTerm

Last updated : 2023-08-03 17:46:01

## Overview

OrcaTerm is a login method recommended by Tencent Cloud. You can use it to directly log in to a Linux instance quickly. It has the following strengths:

Supports copy and paste.

Supports scrolling with mouse wheel.

**Note:**

When you create a Linux Lighthouse instance, it will be bound to a key by default. The username of the key is `lighthouse` , which has the root privileges.

When you use OrcaTerm to log in to a Linux instance, the system will use the key of the `lighthouse` username for login by default.

## Supported Systems

Windows, Linux, or macOS.

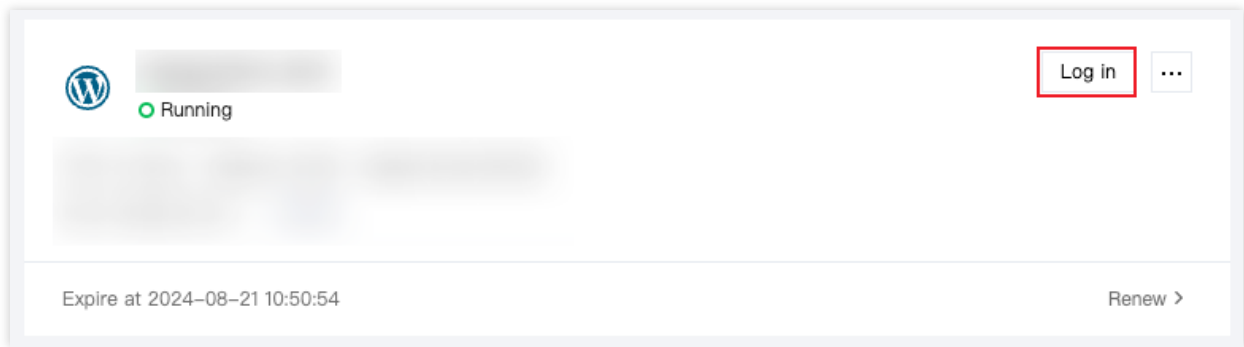
## Prerequisites

Before login, confirm that the firewall of the instance has passed port 22 (which has been enabled by default when the instance was created).

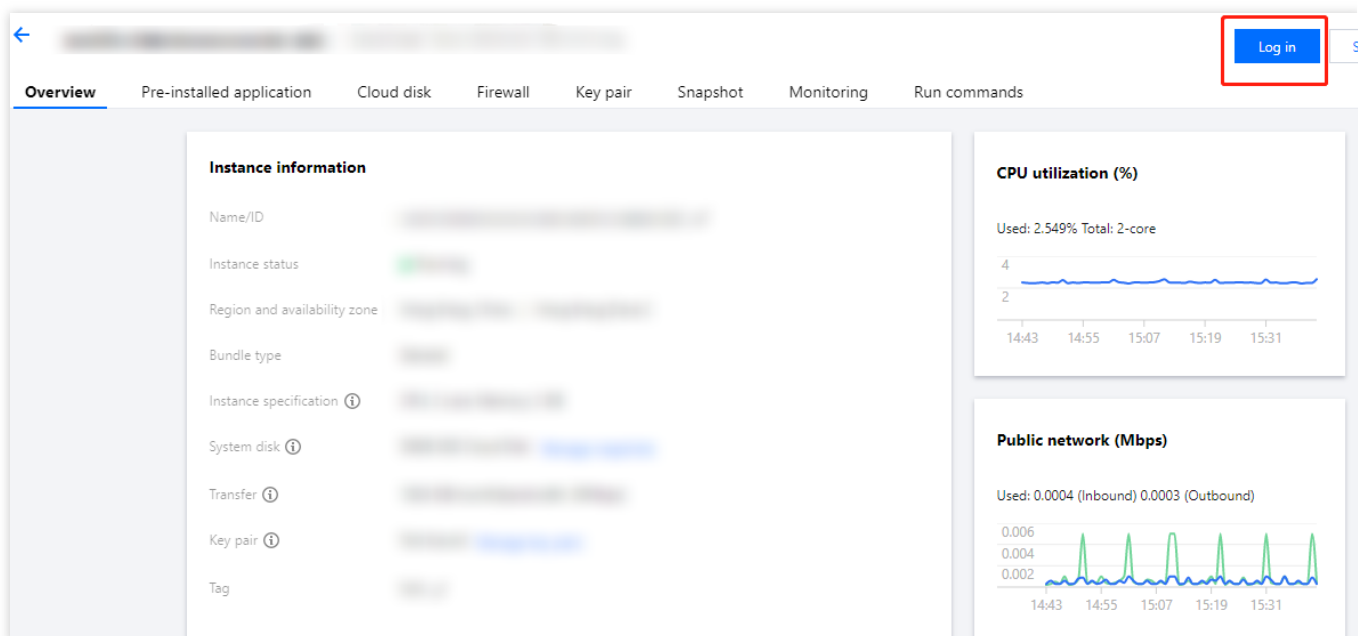
## Directions

1. Log in to the [Lighthouse console](#).
2. Find the target instance in the server list and select a login method as desired.

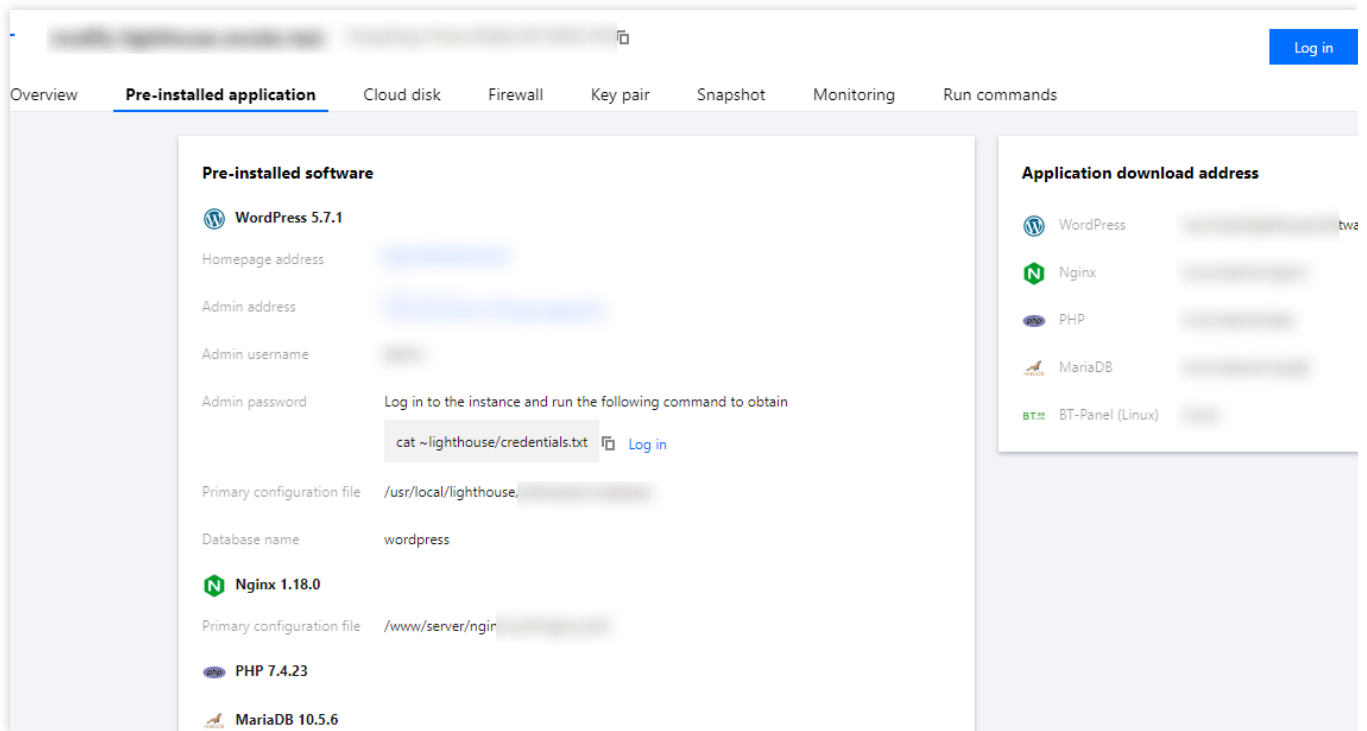
Click **Log in** in the instance card in the server list.



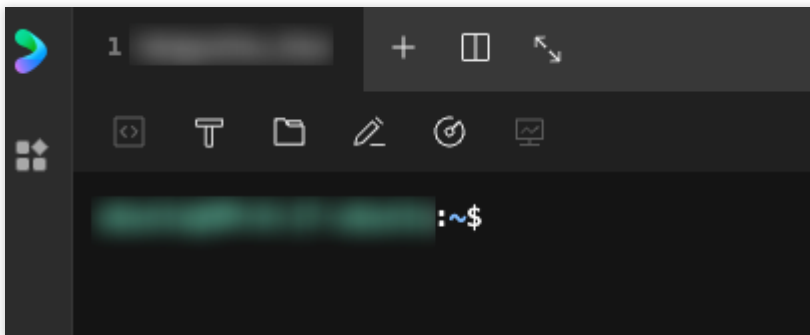
Click the instance card to enter the instance details page and click **Log In** in **Remote Login** or in the top-right corner of the page.



For an instance created by using an [application image](#), select **Pre-installed application** on the instance details page and click **Log in** in the top-right corner of the page.



The page for successful login is as shown below:



After successful login, you can set up low-load lightweight applications with a moderate number of access requests, such as small and middle-sized websites, web applications, blogs, forums, mini games, ecommerce, cloud storage, image hosting, and cloud-based development, testing, and learning environments as instructed in [Best Practices](#).

The OrcaTerm has a variety of features. You can use the virtual keyboard on the mobile client to change the OrcaTerm appearance, upload/download files, start self-service instance detection, enable multi-session, split the screen, and get the prompts as instructed in [More OrcaTerm features](#).

## Related Operations

### Enabling/Disabling OrcaTerm-based quick login

**Note:**

After a Lighthouse instance is created successfully, the OrcaTerm-based quick login feature will be enabled by default. You can disable or enable it again in the following steps:

1. Log in to the [Lighthouse console](#).
2. Find the target instance in the server list and enter the instance details page.
3. In **Quick login** in **Remote login**, you can **enable** or **disable** OrcaTerm-based quick login as needed:

**Close:** If you don't need to use quick login, you can disable it.

**Note:**

After quick login is disabled, you can still use the local SSH client to remotely log in to the instance. You can also enable quick login again.

After quick login is disabled, the public key (stored under the `lighthouse` user of the operating system by default) of the default system key won't be deleted at the same time. You can delete the public key by yourself. However, if it is deleted, quick login will not take effect after being enabled again.

**Enable:** After quick login is enabled, you can use the default system key to quickly log in to the instance through OrcaTerm in a browser.

**Note:**

Confirm that the public key (stored under the `lighthouse` user of the operating system by default) of the default system private key is not deleted; otherwise, the quick login feature won't work after being enabled.

## More OrcaTerm features

OrcaTerm offers a variety of features to ensure a satisfactory user experience.

OrcaTerm features are described as follows:

Multiple keyboard shortcuts

OrcaTerm supports

multiple keyboard shortcuts, which can be viewed on the UI as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. On the OrcaTerm UI, open the **Keyboard shortcuts** window to view the supported shortcuts.

If your local computer uses macOS: Press `⌘ + /`.

If your local computer uses Windows: Press `Ctrl + /`.

Viewing instance monitoring data

You can view the instance monitoring

data in real time on the OrcaTerm UI as instructed below. Currently, the data is refreshed once every 10 seconds.

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. At the bottom of the OrcaTerm UI, view the instance monitoring data.

Changing the username

You can specify the user to log

in via OrcaTerm as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. In the **Log in** pop-up window, the default username is `lighthouse` , which can be changed as needed.
3. Then click **Log in**

Quickly installing TencentCloud Automation Tools

You need to use TencentCloud Automation

Tools to implement quick passwordless login via OrcaTerm. If the tool is not installed for your instance, you can install it upon login as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. In the **Log in** pop-up window, select the installation method as needed if you are prompted that TencentCloud Automation Tools is not installed for your instance.

**Quick installation (reboot required):** Read the notes, select **Installation requires your agreement to a forced shutdown**, and click **Quickly install TencentCloud Automation Tools**.

**Manual installation (no reboot required):** Perform the installation as instructed in [Installing TAT Agent](#).

3. After the installation is completed, the instance can be quickly logged in to via OrcaTerm.

Using the command block mode

You can use the command block

mode on the OrcaTerm UI. After the mode is enabled, every executed command will be displayed as a module for easy use of OrcaTerm. You can also disable the mode as needed as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. On the OrcaTerm UI, enable or disable the command line mode.

**Enable the command line mode:** Select



on the toolbar of the OrcaTerm UI to enable the command block mode. After it is enabled, a command will be executed as follows:

```
[lighthouse@VM-12-16-centos /]$  
ls  
bin boot data dev etc home lib lib64 lost+found media mnt opt proc root run sbin srv sys tmp  
[lighthouse@VM-12-16-centos /]$  
pwd  
/  
[lighthouse@VM-12-16-centos /]$
```

**Disable the command line mode:** Select



on the toolbar of the OrcaTerm UI to disable the command block mode. After it is disabled, a command will be executed as follows:

```
[lighthouse@VM-12-16-centos ~]$ ls
bin  boot  data  dev  etc  home  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys
[lighthouse@VM-12-16-centos ~]$ pwd
/
[lighthouse@VM-12-16-centos ~]$
```

### Note:

If the command block mode is disabled and enabled again, you need to reconnect to OrcaTerm.

Viewing the release note

You can view the latest release

note of OrcaTerm, including the new features, bugfixes, and features coming soon, as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. Select



in the bottom-right corner of the OrcaTerm UI.

3. View the latest release note in the pop-up window.

Selecting an instance to log in

You can select any instance

to log in on the OrcaTerm UI as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. Select



on the toolbar of the OrcaTerm UI.

3. For the first time, the **Select the instance to be displayed** window will pop up. Select the target instance and click **OK**.
4. Select



> **Add instance** to add instances as needed.

### Note:

Currently, up to ten instances can be added.

5. After the instances are added successfully, you can select any instance to log in.

## Uploading/Downloading files

You can upload local files to

the instance or download files from the instance to your local file system as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. Select



on the toolbar of the OrcaTerm UI.

3. In the pop-up menu, select **Upload** or **Download**.

The detailed steps are as follows:

### Upload a file:

- 3.1.1 In the **Select the file and directory for upload** pop-up window, select **Local upload** or **Upload via URL** as needed.
- 3.1.2 If you select **Local upload**, click **Click to upload** and then select a local file. If you select **Upload via URL**, enter the file URL in **URL**.
- 3.1.3 Select the target upload directory and click **OK**.

### Note:

Currently, files can be uploaded only to the `home > lighthouse` directory.

- 3.1.4 Click



in the bottom-right corner of the page and view the operation result in the pop-up window. If the file is uploaded successfully, the result will be displayed.

### Download a file:

- 3.2.1 In the **Download file** pop-up window, open the directories and select the target file.
- 3.2.2 Click **OK** and select the local directory in the pop-up window.
- 3.2.3 Click



in the bottom-right corner of the page and view the operation result in the pop-up window. If the file is downloaded successfully, the result will be displayed.

## Using self-service instance detection

If you encounter any

problem when logging in to or using the instance, you can perform self-service instance detection as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. Select



on the toolbar of the OrcaTerm UI.

3. In the **Self-service instance detection** pop-up window, click **OK**.

Enabling the multi-tag window

You can open multiple instance

connection pages in the form of tags on the OrcaTerm UI as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. Select



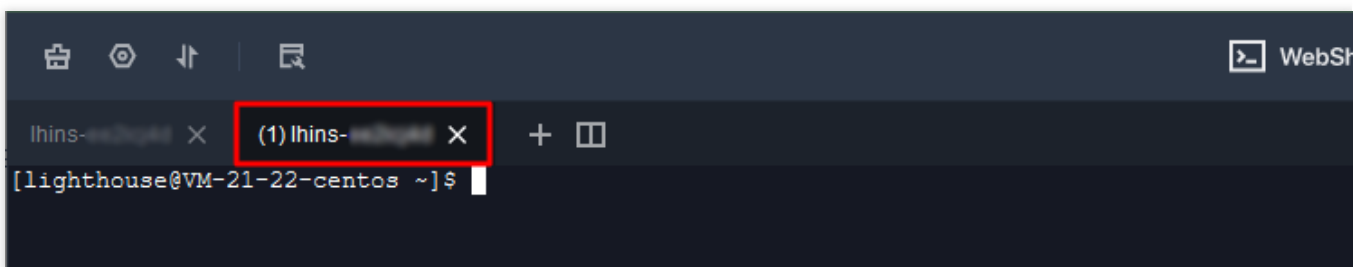
at the top of the OrcaTerm UI.

3. You can see that the `(1) instance ID` tag has been created.

**Note:**

Up to five tags can be opened at the same time.

A tag will be named in the format of `(Incrementing number) instance ID`.



Enabling screen splitting<sup>[[id:splitScreen)</sup>

You can split the screen on the OrcaTerm UI to view and execute multiple operation tasks at the same time as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. Select



at the top of the OrcaTerm UI.

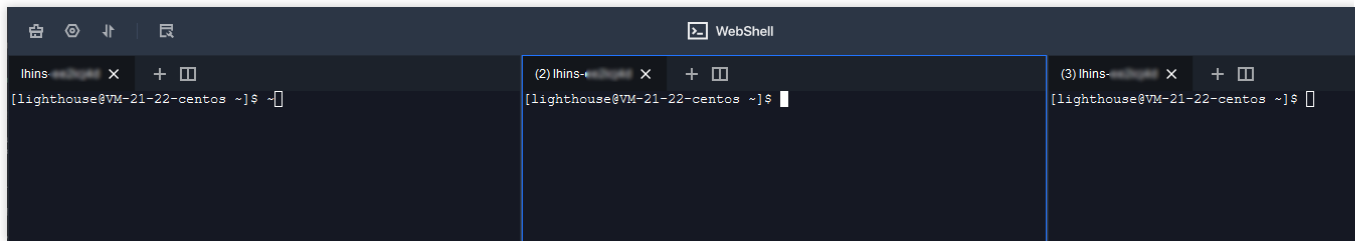
3. You can see that the screen has been split into three sections named in the format of `(Incrementing number) instance ID`:

**Note:**

The screen can be split into up to four sections.

A section will be named in the format of `(Incrementing number) instance ID`.





## Changing the skin

You can change the text size

, font, and color on the WebShell UI as instructed below:

1. Log in to the instance as instructed in [Logging in to Linux Instance via OrcaTerm](#).
2. Select



on the toolbar of the OrcaTerm UI.

3. In the pop-up window, change the text size, font, or color of the OrcaTerm as you like.

# Logging in to Linux Instance via Remote Login Software

Last updated : 2022-06-10 10:15:46

## Overview

This document takes PuTTY as an example to describe how to log in to a Linux instance from a Windows local computer by using the remote login software.

## Supported Operating Systems

Windows

### Note:

If your local computer uses Linux or macOS, [use SSH to log in to the Linux instance](#).

## Authentication Method

**Password or Key**

## Prerequisites

You have obtained the username and password (or SSH key) to log in to the instance.

### Note:

If it is your first time to log in to a Linux instance through a local remote login application, you need to reset the password of your username (e.g., `root` and `ubuntu` ) or bind your key. For detailed directions, see [Resetting Password](#) and [Managing Key](#).

Make sure the network connection between the local computer and the instance is working, and the port 22 is open in the firewall policies of the instance (Port 22 is open by default upon the creation of the instance).

## Limits

For instances created with Ubuntu images, password login is disabled by default for the `root` account. To enable it, see [Uploading Local Files](#).

## Directions

Password login

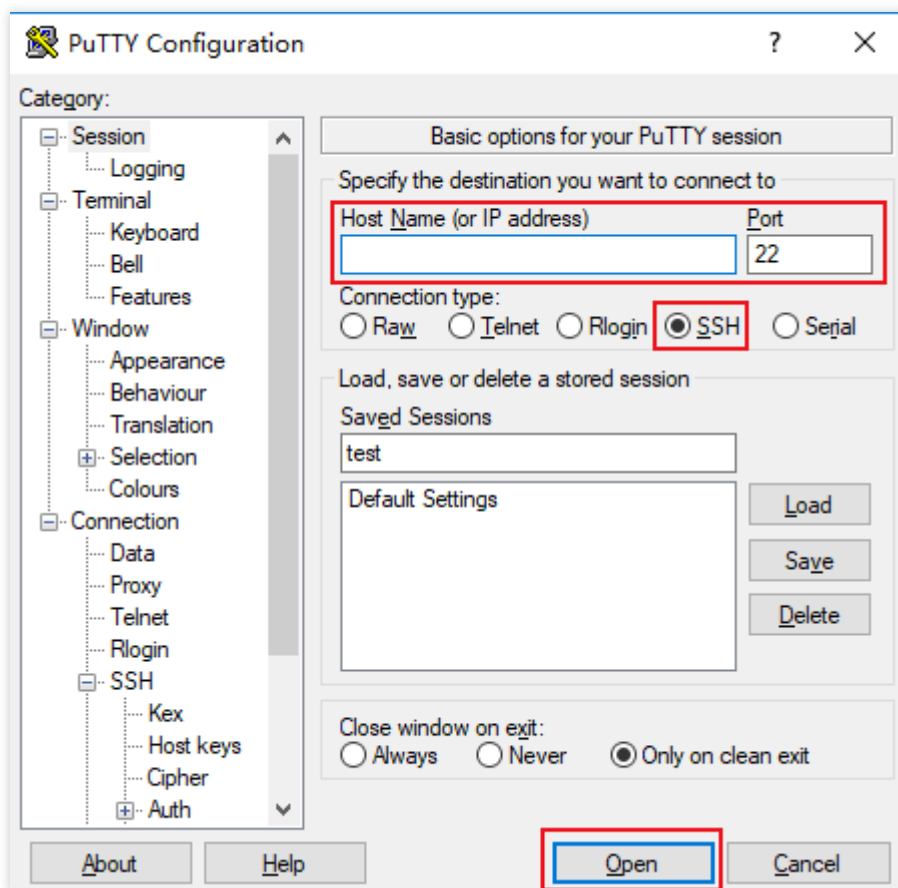
SSH key login

1. Download the Windows remote login software: PuTTY.

[Download PuTTY](#)

2. Double-click **putty.exe** to open the PuTTY Client.

3. In the **PuTTY Configuration** window, enter the following content, as shown below:



Configure parameters as follows:

**Host Name (or IP address):** The public IP of the Lighthouse instance. You can check this public IP in the [Lighthouse console](#).

**Port:** The port open for remote login on the Lighthouse side. For a Linux instance, it defaults to 22.

**Connection type:** Select **SSH**.

**Saved Sessions:** Enter the session name, such as `test` .

After configuring **Host Name**, configure and save **Saved Sessions**. You can double-click the session name saved under **Saved Sessions** to log in to the instance.

4. Click **Open** to enter the **PuTTY** page. The **login as:** command prompt appears.

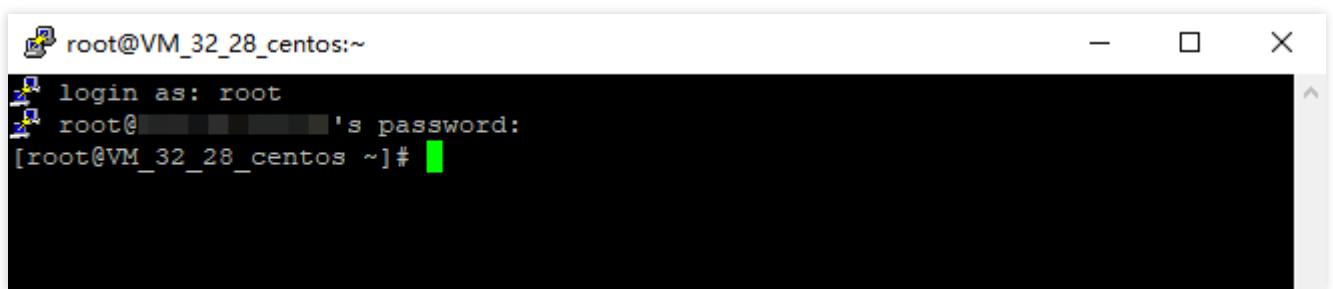
5. Enter your username after **login as:** (e.g., `root` ) and press **Enter**.

**Note:**

For all Linux images, except Ubuntu images, you can log in with the `root` account. For Ubuntu system, the default username is `ubuntu` . To log in with the `root` account, see [How do I log in to an instance with root on Ubuntu?](#)

6. Enter your password after **Password** and press **Enter**.

The entered password is invisible by default.



Once logged in, you can see the information about the current Lighthouse instance on the left side of the command prompt.

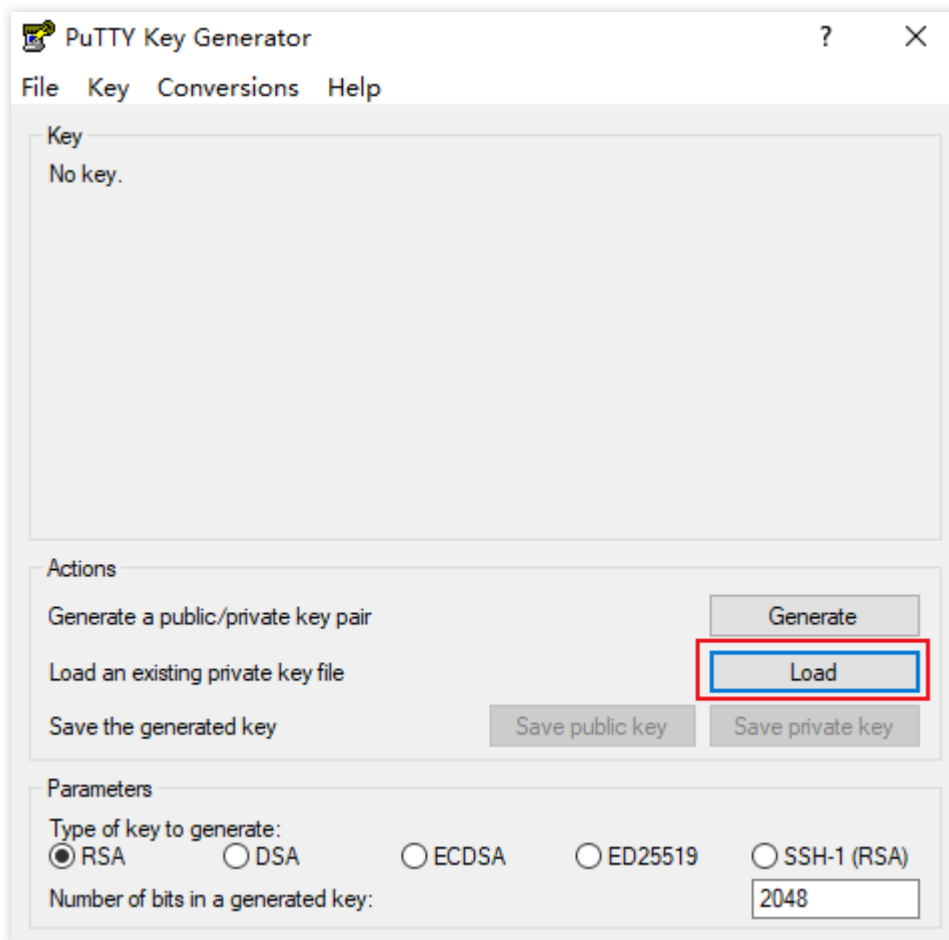
1. Download the Windows remote login software, PuTTY.

Download both putty.exe and puttygen.exe. To download PuTTY, [click here](#).

2. Double-click **puttygen.exe** to open the PuTTY Key Client.

3. Click **Load**, select and open the path where the downloaded private key is saved, as shown below:

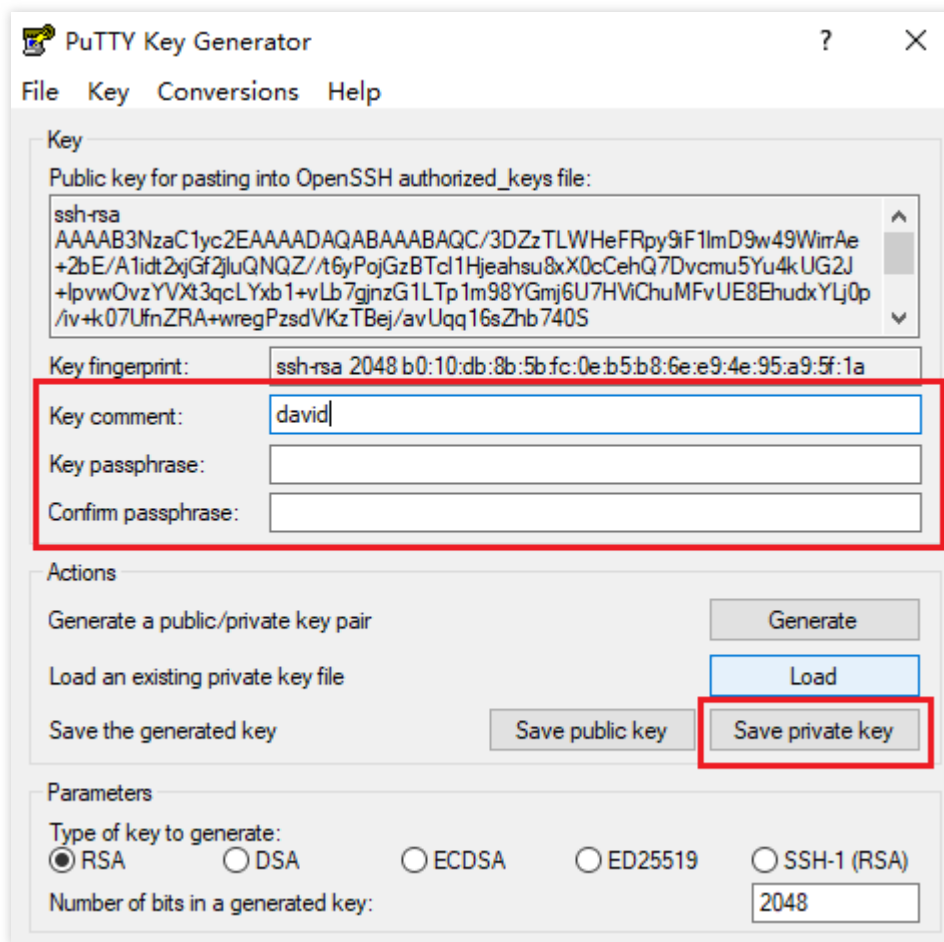
For example, select and open the private key file `david` .



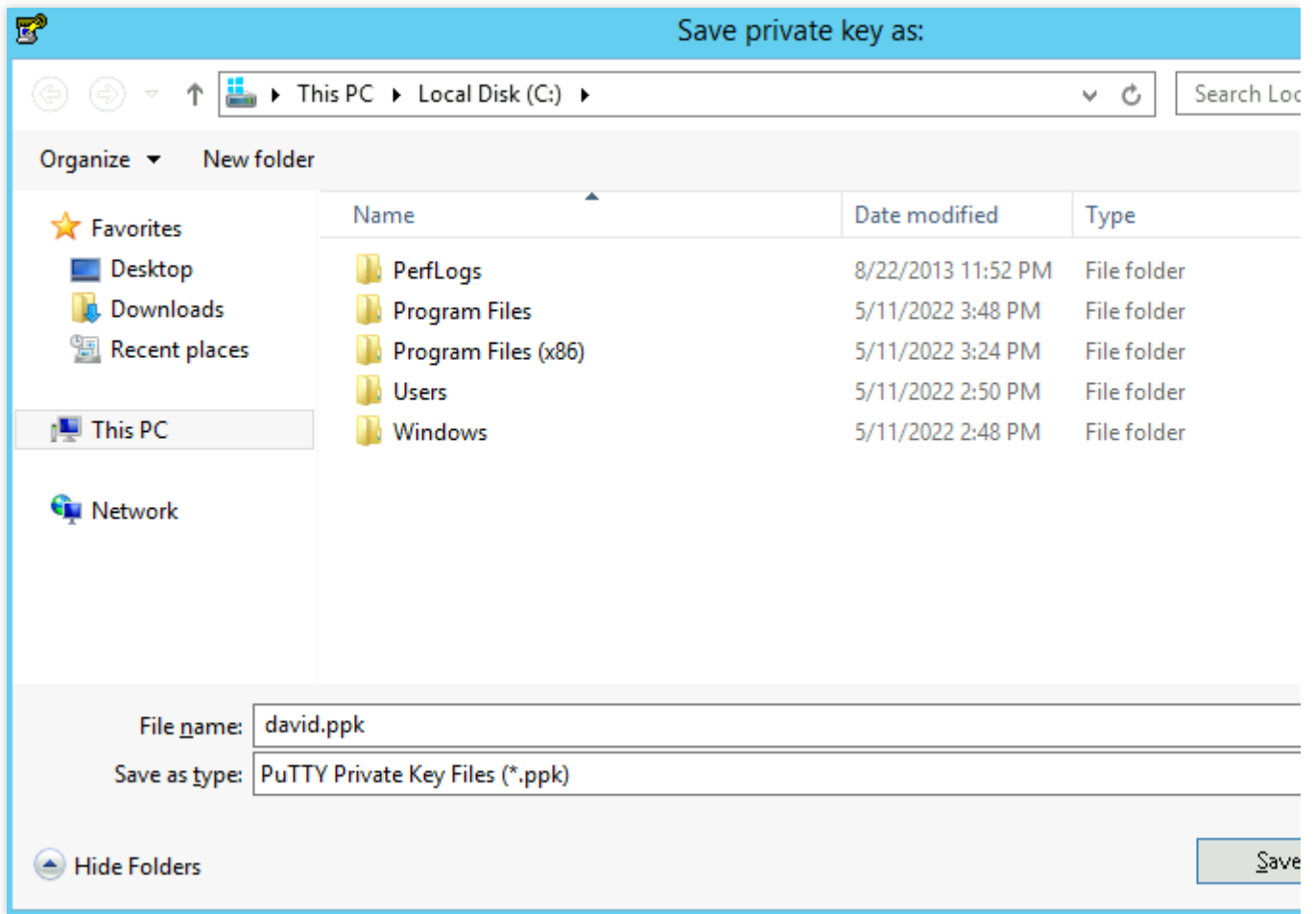
4.

In the **PuTTY Key Generator** window,

you can enter the key name and create a password for the key (optional). When finished, click **Save private key**, as shown below:



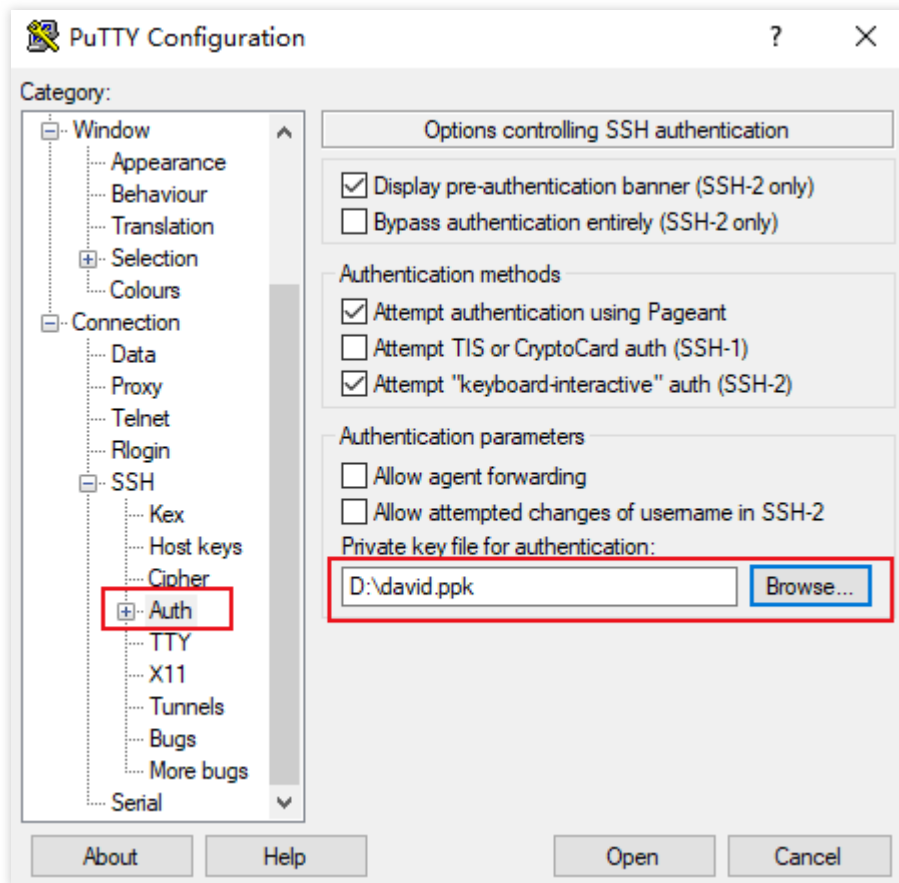
5. In the pop-up window, select the path to store the key. In the **File name** field, enter “[Key Name].ppk” and click **Save**. For example, save the private key file `david` as `david.ppk`.



6. Double-click **putty.exe** to open the PuTTY Client.

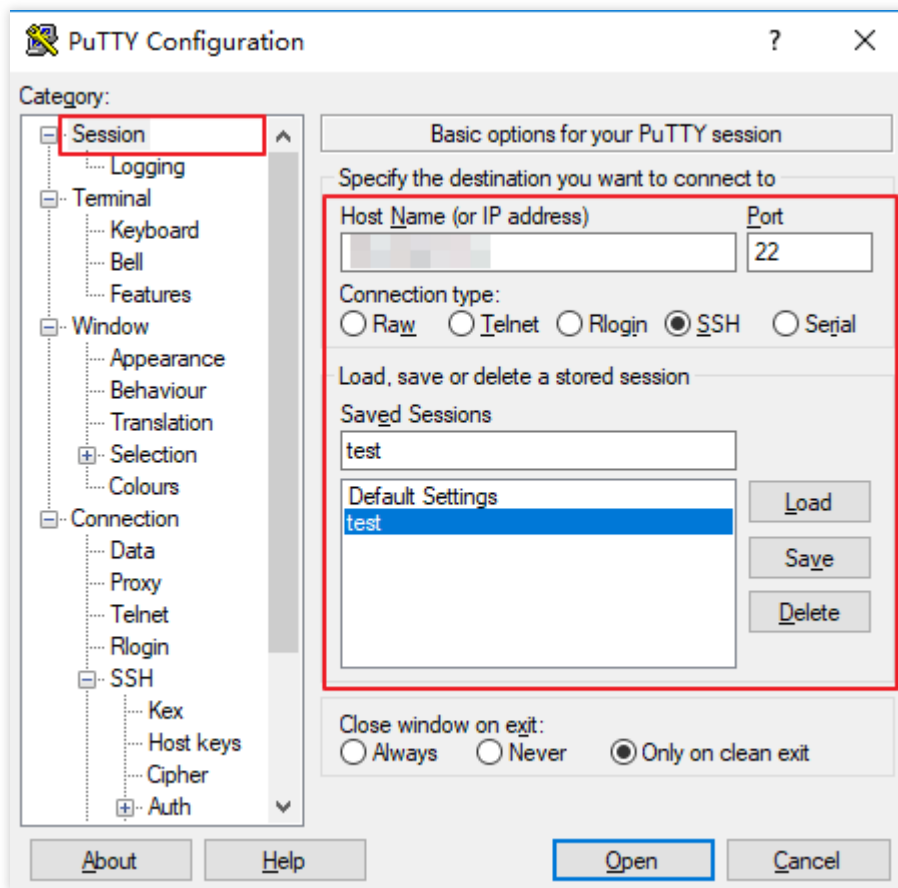
In the left sidebar, select **Connection > SSH > Auth** to enter the Auth configuration page.

7. Click **Browse** to select and open the path where the key is saved.



8. Switch to the **Session** configuration page. Configure the server IP, port, and connection type.





**Host Name (IP address):** The public IP of the Lighthouse instance. You can check this public IP in the [Lighthouse console](#).

**Port:** The port open for remote login on the Lighthouse side. For a Linux instance, it defaults to 22.

**Connection type:** Select **SSH**.

**Saved Sessions:** Enter the session name, such as `test`.

After configuring **Host Name**, configure and save **Saved Sessions**. You can double-click the session name saved under **Saved Sessions** to log in to the instance.

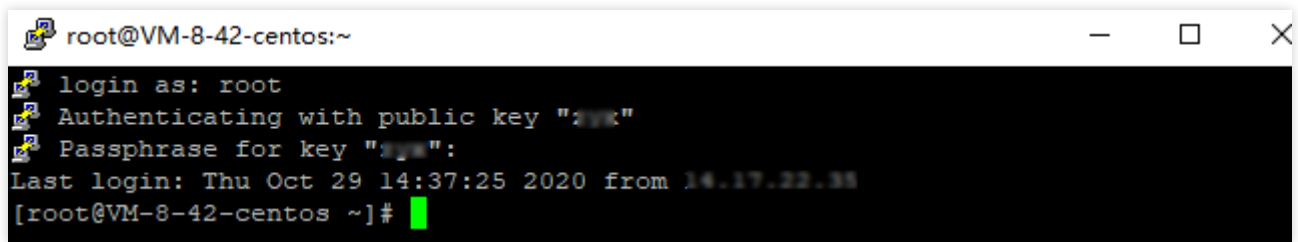
9. Click **Open** to enter the **PuTTY** running interface. The **login as:** command prompt appears.

10. Enter your username after **login as:** and press **Enter**.

**Note:**

For all Linux images, except Ubuntu images, you can log in with the `root` account. For Ubuntu system, the default username is `ubuntu`. To log in with the `root` account, see [How do I log in to an instance with root on Ubuntu?](#).

If a password is set for the encrypted private key in [Step 4](#), enter the password here and press **Enter**. The password is invisible by default.

A terminal window titled 'root@VM-8-42-centos:~' with standard window controls. The terminal output shows an SSH login sequence: 'login as: root', 'Authenticating with public key "ssh-rsa"', 'Passphrase for key "ssh-rsa":', and 'Last login: Thu Oct 29 14:37:25 2020 from 14.17.22.34'. The prompt '[root@VM-8-42-centos ~]#' is followed by a green cursor.

```
root@VM-8-42-centos:~  
login as: root  
Authenticating with public key "ssh-rsa"  
Passphrase for key "ssh-rsa":  
Last login: Thu Oct 29 14:37:25 2020 from 14.17.22.34  
[root@VM-8-42-centos ~]#
```

Once logged in, you can see the information about the current Lighthouse instance on the left side of the command prompt.

# Logging in to Linux Instance via SSH Key

Last updated : 2022-05-12 12:24:11

## Overview

This document describes how to use an SSH key to log in to a Linux Lighthouse instance from a Linux, macOS, or Windows computer.

## Supported Operating Systems

Linux, macOS, and Windows (Windows 10 and Windows Server 2019).

## Authentication Method

**Password** or **Key**

## Prerequisites

You have obtained the username (custom username or default username *root*) and password (or key) to log in to the instance.

### Note:

If it is your first time to log in to a Linux instance through the local SSH client, you need to reset the password of the default username (*root*) or bind your key. For detailed directions, see [Resetting Password](#) and [Managing Keys](#).

Make sure the network connection between the local computer and the instance is working, and the port 22 is open in the firewall policies of the instance (Port 22 is open by default upon the creation of the instance).

## Directions

Password login

SSH key login

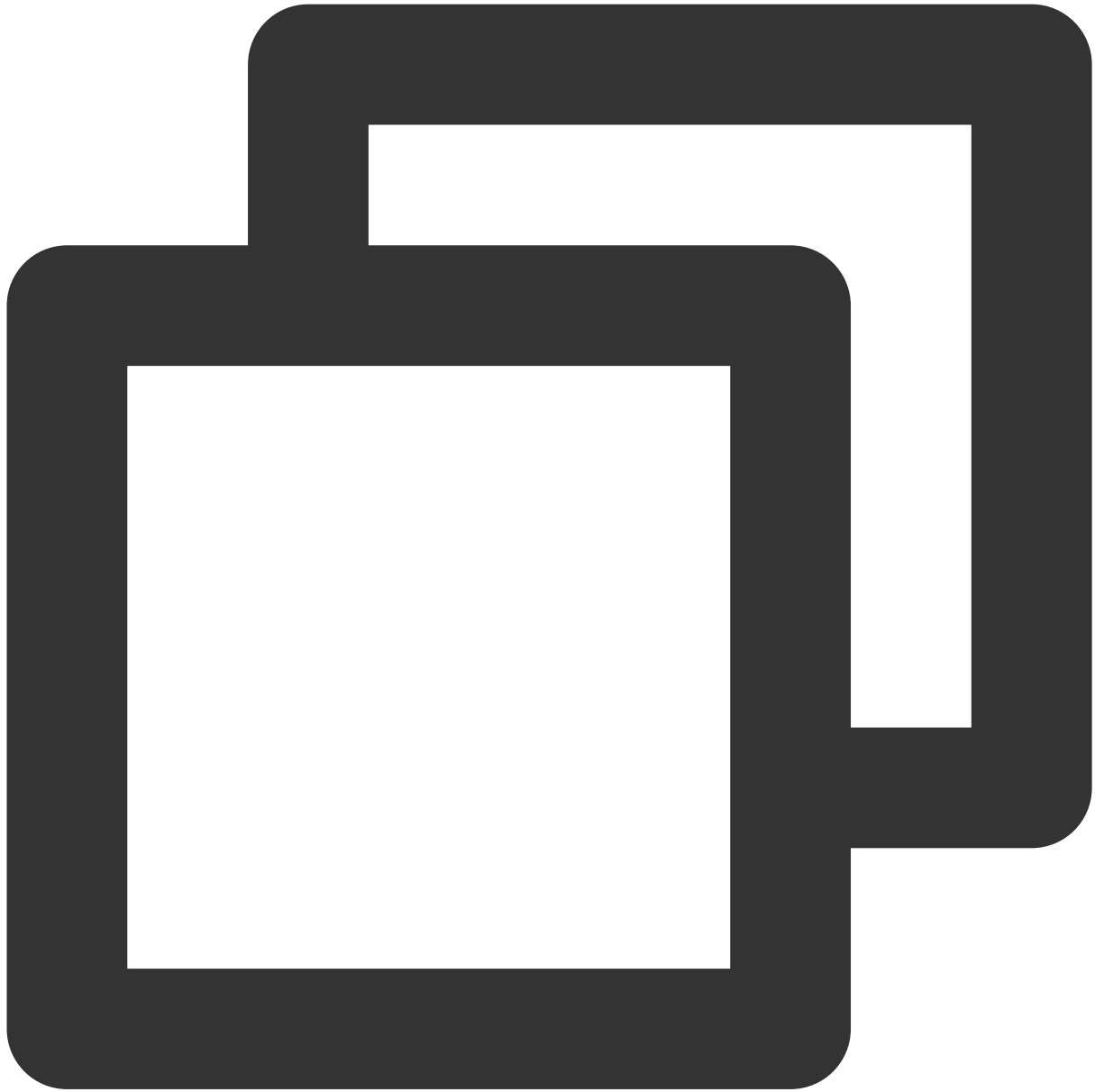
1. Run the following command to connect to your Linux instance.

### Note:

Linux distribution without GUI: Run the following command on the system interface directly.

Linux distribution with GUI or macOS: Open the command line interface that comes with the system (e.g., Terminal on macOS) before running the following command.

Windows 10 or Windows Server 2019: Open the command prompt (CMD) before running the following command.



```
ssh <username>@<IP address or domain name>
```

`username` is the obtained username in [Prerequisites](#), such as `root` and `ubuntu` .

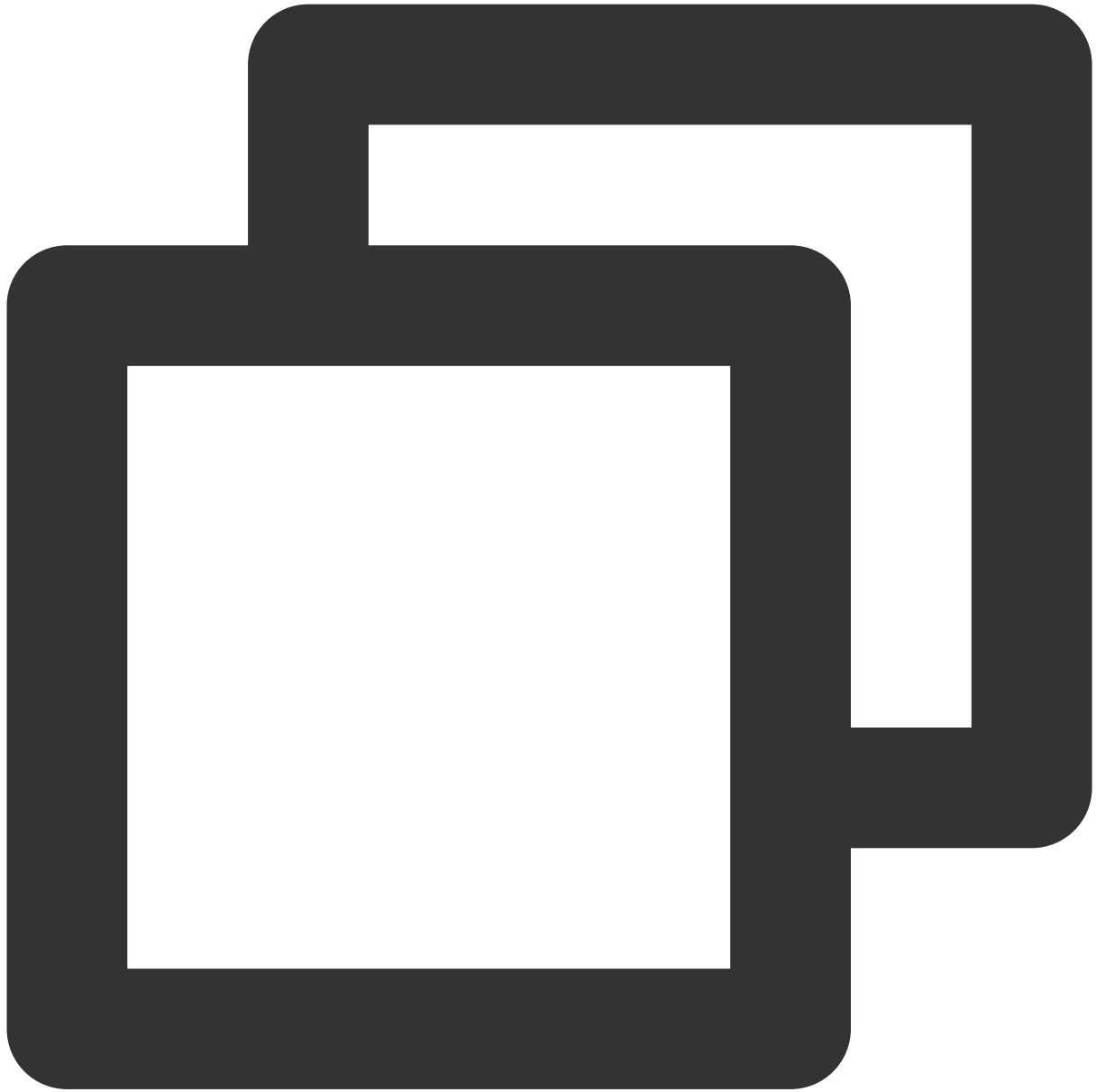
`IP address or domain name` is the public IP address or custom domain of your Linux instance. You can view the instance's public IP address in the [Lighthouse console](#).

2. Enter the password you have obtained, and press Enter to log in.

1. Execute the following command to set the private key file readable only to you.

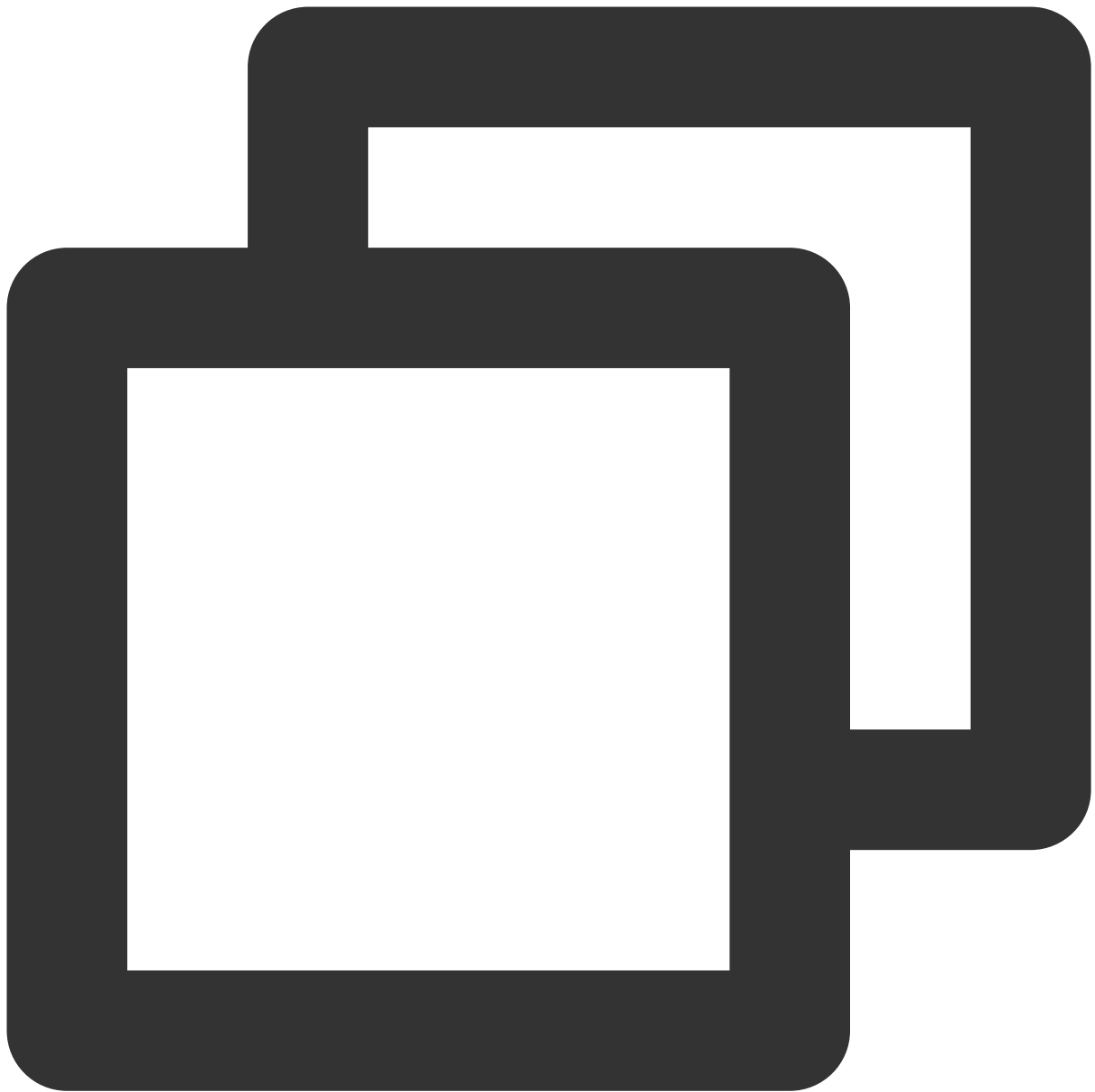
macOS: Open the terminal that comes with the system before executing the following command.

Linux: Directly execute the following command.

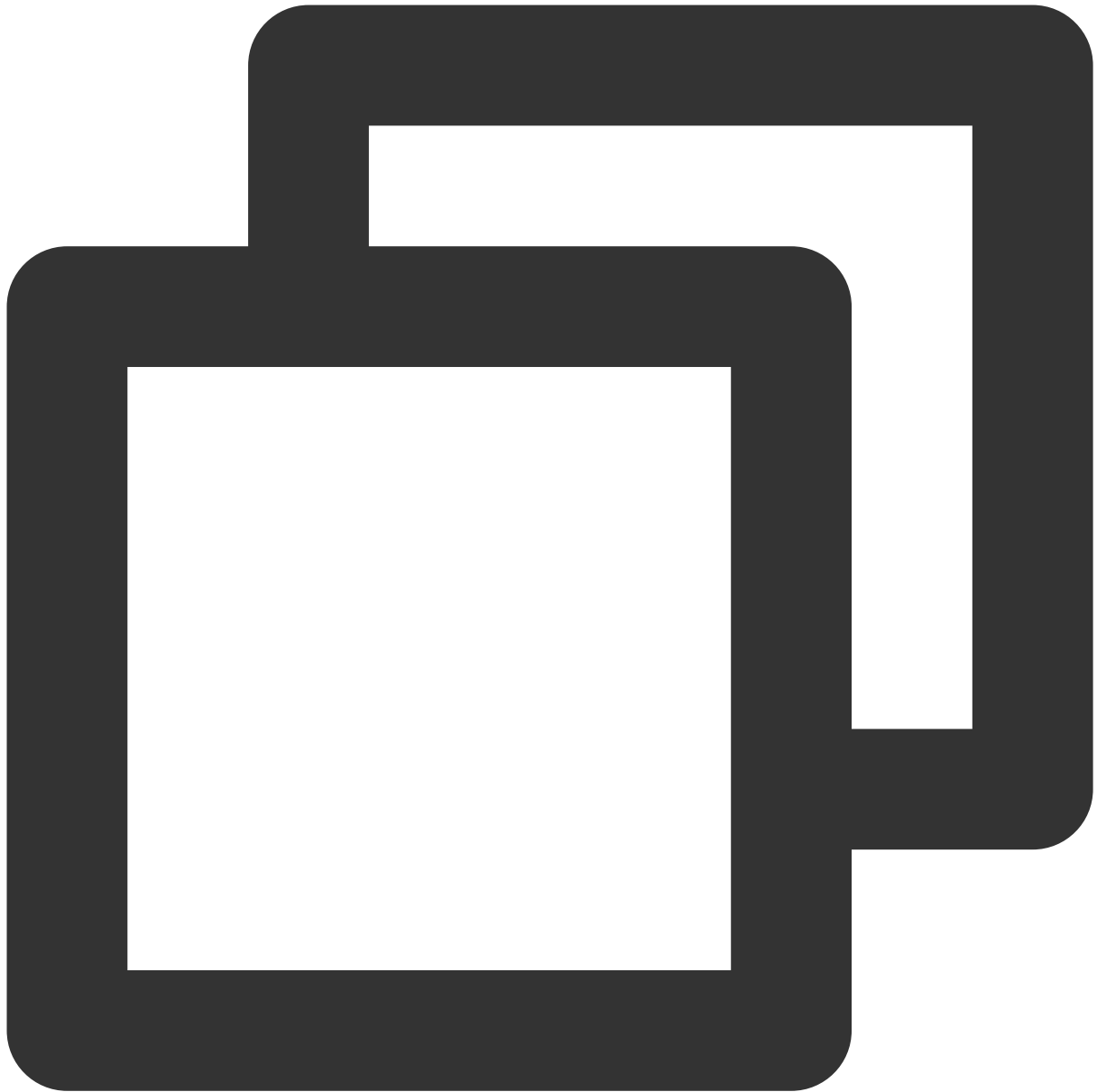


```
chmod 400 <absolute path of the downloaded private key associated with the instance
```

Windows 10 or Windows Server 2019: Open the command prompt (CMD) first and run the following commands in sequence.

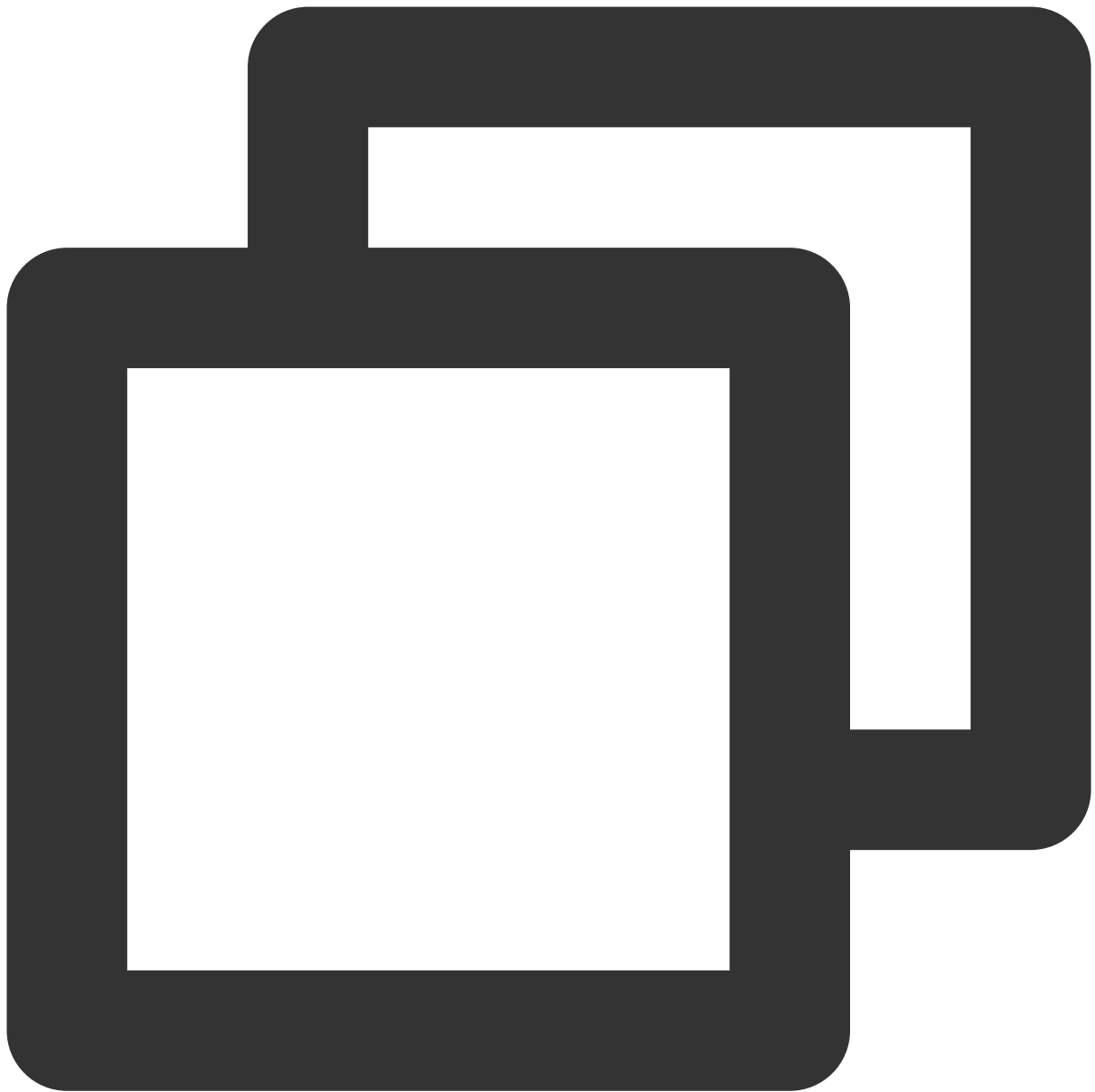


```
icaccls <path of the downloaded private key file associated with the instance> /gran
```



```
icaccls <path of the downloaded private key file associated with the instance> /inhe
```

2. Execute the following command for remote login.



```
ssh -i <path of the downloaded private key file associated with the instance> <user
```

`username` is the obtained username in [Prerequisites](#), such as `root` and `ubuntu` .

`IP address or domain name` is the public IP address or custom domain of your Linux instance. You can view the instance's public IP address in the [Lighthouse console](#).

For example, run the `ssh -i /Users/macuser/Downloads/test_private_key root@35.222.45.145` command on macOS to remotely log in to the Linux instance.



# Logging in to Linux Instance via VNC

Last updated : 2022-05-12 12:24:11

## Overview

VNC login allows for remote login of Lighthouse instances by using a web browser. If the remote login client is not available and all the other login methods failed, you can log in to an instance via VNC to check the instance status and perform basic management operations.

## Usage Limits

VNC does not support copy and paste, and file upload or download.

Use a mainstream browser, such as Chrome, Firefox, and IE 10 or later.

Only one user can log in to an instance by using VNC at a time.

## Prerequisites

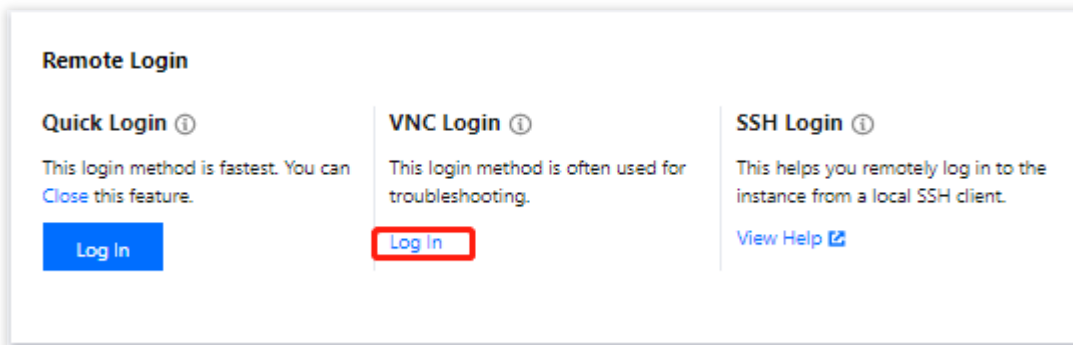
You must have the admin account and password for logging in to a Linux instance remotely.

### Note:

Make sure you've set the login password. For more information, see [Resetting Password](#).

## Directions

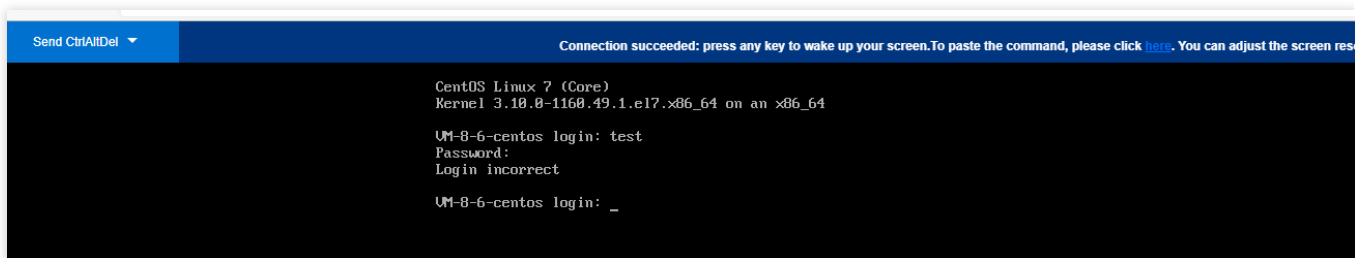
1. Log in to the [Lighthouse console](#).
2. Find the target instance and enter its details page.
3. Select **Remote login** and click **Log in** under **VNC Login**.



4. In the pop-up window, enter the username after *login* and press Enter.

5. Enter the password after **Password** and press Enter.

The entered password is invisible by default.



Once logged in, you can see the information of the instance on the left of the command prompt.

**Note:**

Click **Send remote command** in the top-left corner and select the command you want.

# Logging in Windows Instance

## Logging in to Windows Instance via VNC

Last updated : 2022-05-12 12:24:11

### Overview

VNC login provided by Tencent Cloud allows you to remotely log in to a Lighthouse instance via a web browser. If Remote Desktop Connection is not installed or cannot be used, you can log in to an instance via VNC to check the instance status and perform basic management operations.

### Use Limits

VNC currently does not support copy and paste, Chinese input methods, and file upload or download.

When you use VNC to log in to an instance, you must use a mainstream browser, such as Chrome, Firefox, and IE 10 or later.

VNC login is a dedicated terminal, meaning only one user can use VNC login at a time.

### Prerequisites

You must have the admin account (Administrator) and password for logging in to a Windows instance remotely.

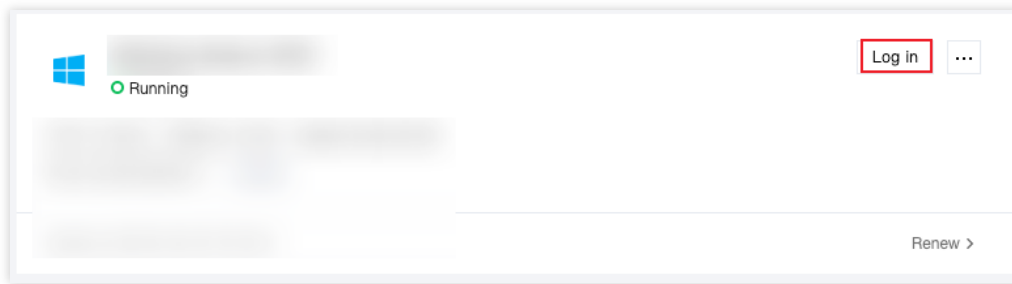
If you set a login password when creating an instance, use it for login. If you forgot it, you can [reset it](#).

If you choose to generate a random password when creating an instance, you can get it from [Message Center](#).

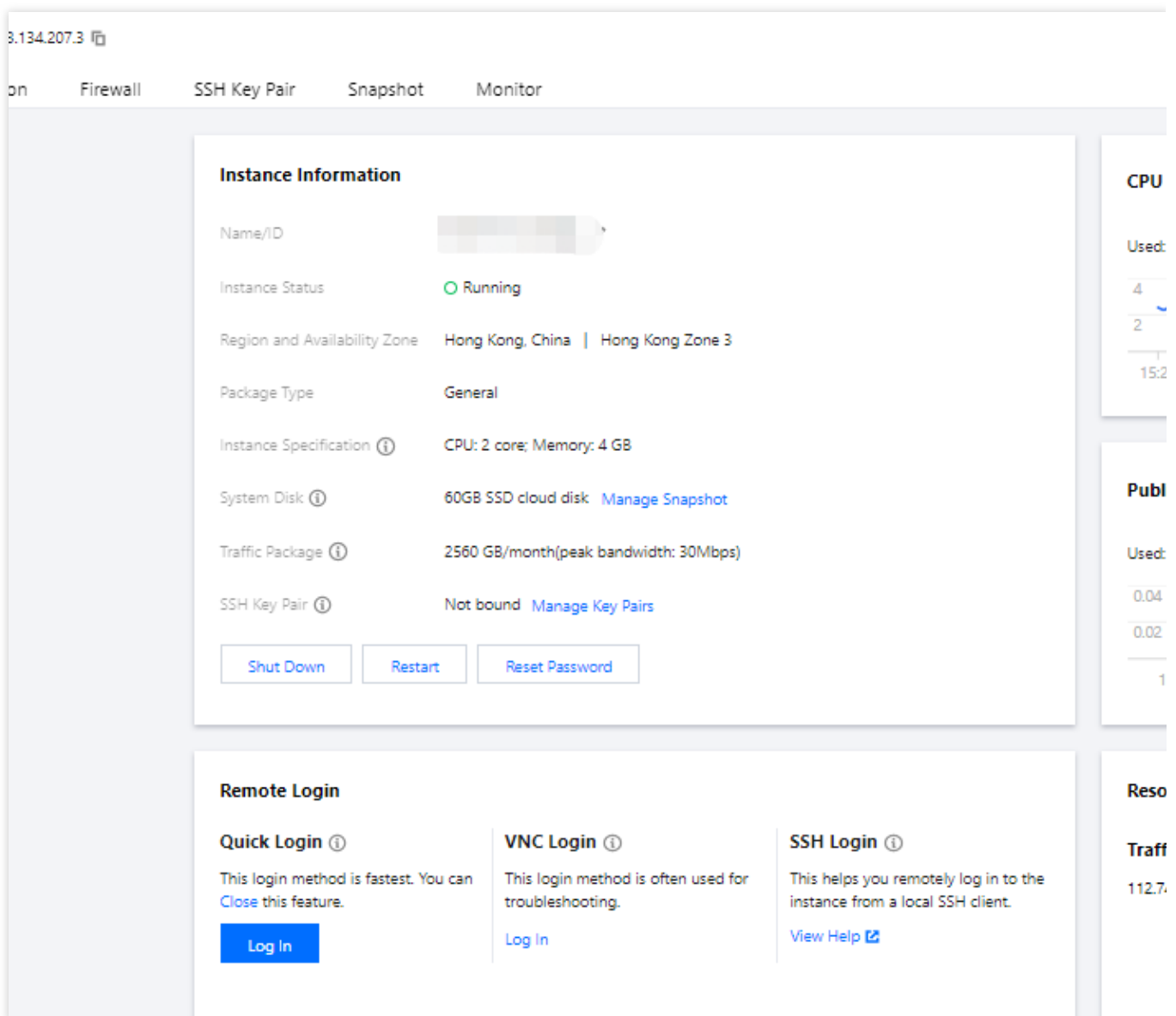
### Directions

1. Log in to the [Lighthouse console](#).
2. Find the target instance in the server list and select a login method as desired.

Click **Log in** in the instance card of the server list.



On the server details page, select the **Overview** tab, and click **Log In** under **Remote Login > VNC Login**.



After successful login, you can set up low-load lightweight applications with a moderate number of access requests, such as small and middle-sized websites, web applications, blogs, forums, mini programs, mini games, ecommerce, cloud storage, image hosting, and cloud-based environments for developing, testing, and learning.

# Logging in to Windows Instance via Remote Desktop Connection

Last updated : 2022-05-12 12:24:11

## Overview

This document describes how to log in to a Windows instance through remote desktop software on local Windows, Linux, and macOS computers.

## Supported Operating Systems

Windows, Linux, and macOS.

## Prerequisites

You must have the admin account (Administrator) and password for logging in to a Windows instance remotely.

If you set a login password when creating an instance, use it for login. If you forgot it, you can [reset it](#).

If you choose to generate a random password when creating an instance, you can get it from [Message Center](#).

Make sure the network connection between the local computer and the instance is working, and the port 3389 is open in the firewall policies of the instance (Port 3389 is open by default upon the creation of instance).

## Directions

Select one of the following remote desktop applications to log in to your Windows instance based on your local operating system.

Windows

Linux

macOS

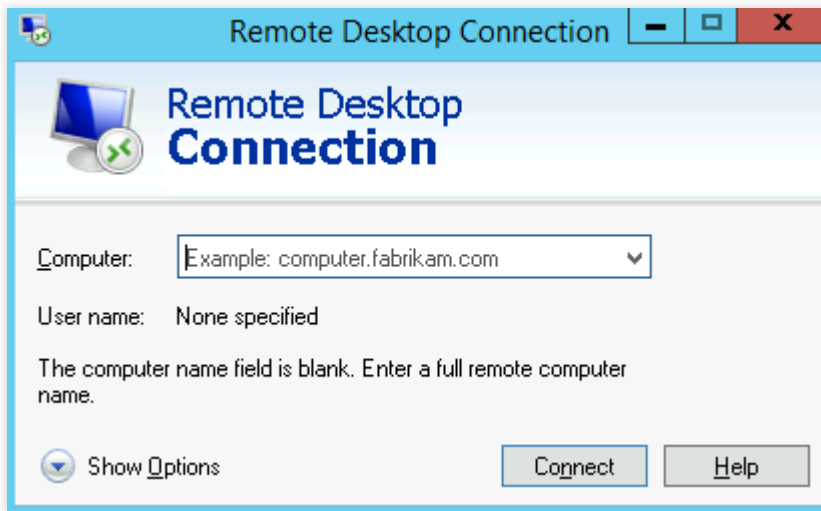
### Note:

The following takes Windows 7 as an example.

1. On the local Window server, click



, enter **mstsc** in **Search programs and files**, and press **Enter** to open the **Remote Desktop Connection** window.



2. Enter the Windows instance's public IP after **Computer** and click **Connect**.

You can get the Window instance's public IP in the [Lighthouse console](#).

3. Enter the instance's admin account/password in the **Windows Security** pop-up window.

**Note:**

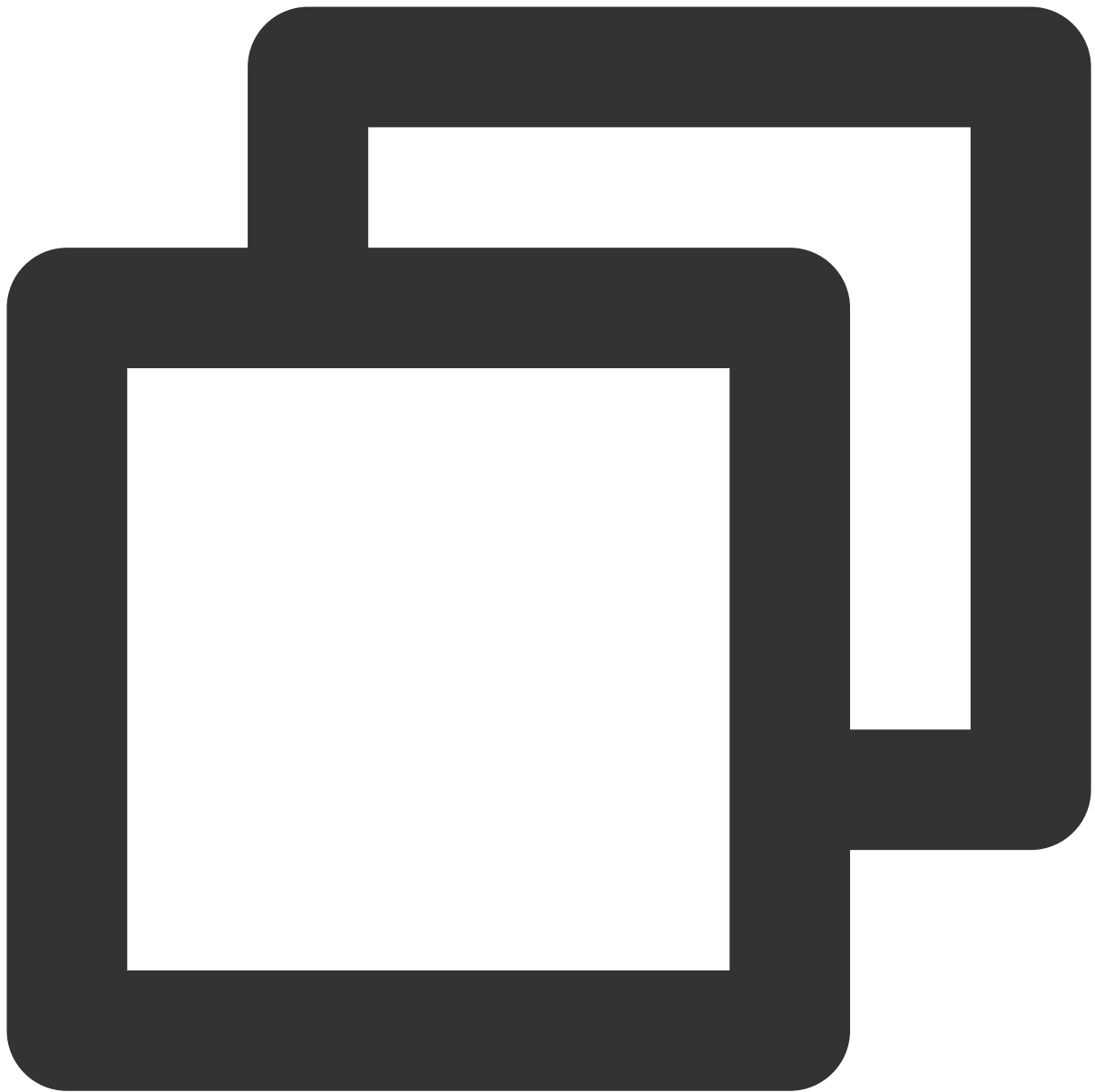
If the **Do you trust this remote connection?** window pops up, you can select **Don't ask me again for connections to this computer** and click **Connect**.

4. Click **OK**.

**Note:**

We recommend you use rdesktop as the remote desktop client. For more information, see the [official introduction to rdesktop](#).

1. Run the following command to check whether rdesktop has been installed.



```
rdesktop
```

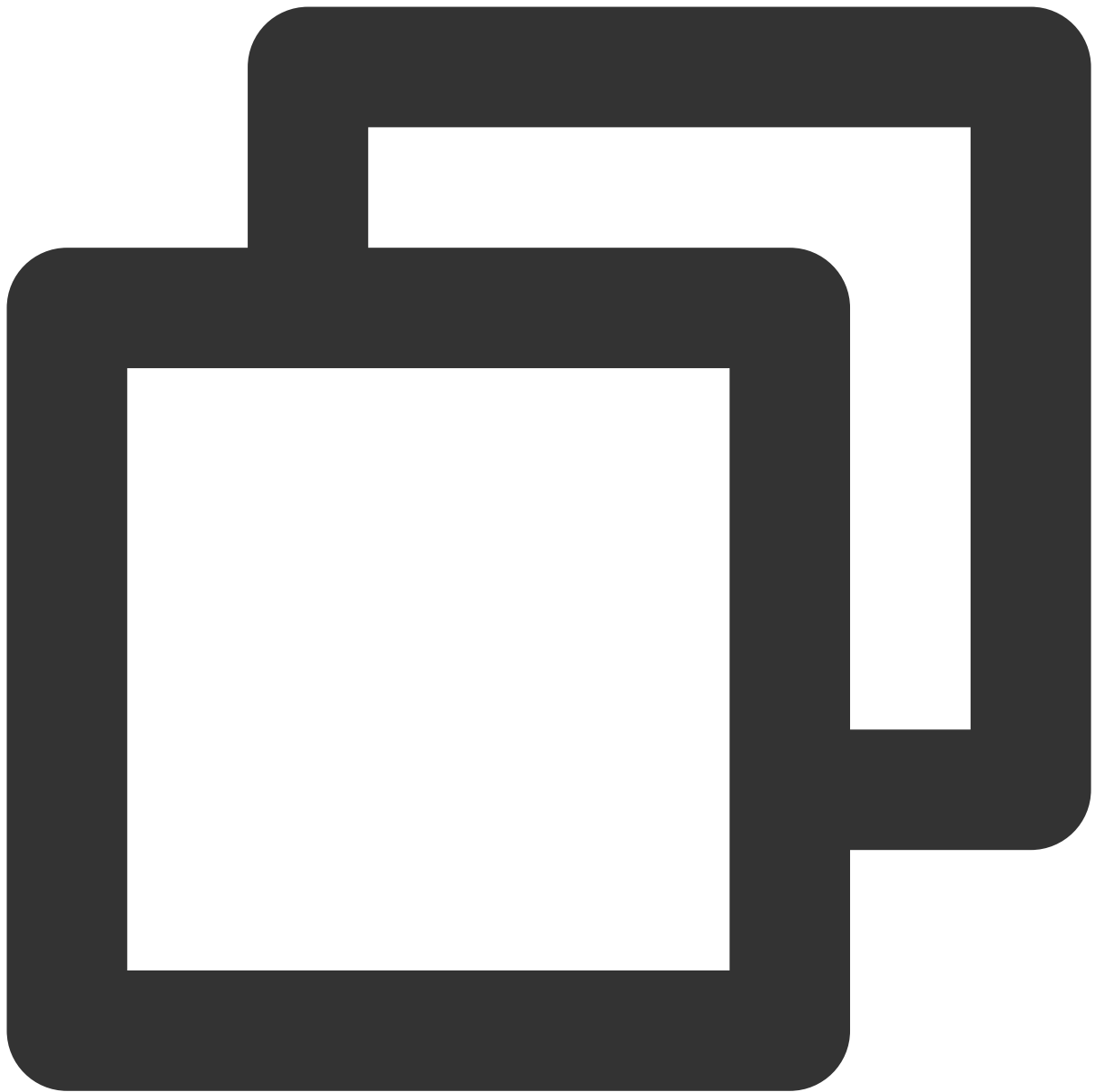
If yes, perform [step 4](#).

If no, you will be prompted with "command not found". In this case, perform [step 2](#).

2.

Open a terminal window and

run the following command to download rdesktop. This step uses rdesktop v1.8.3 as an example.

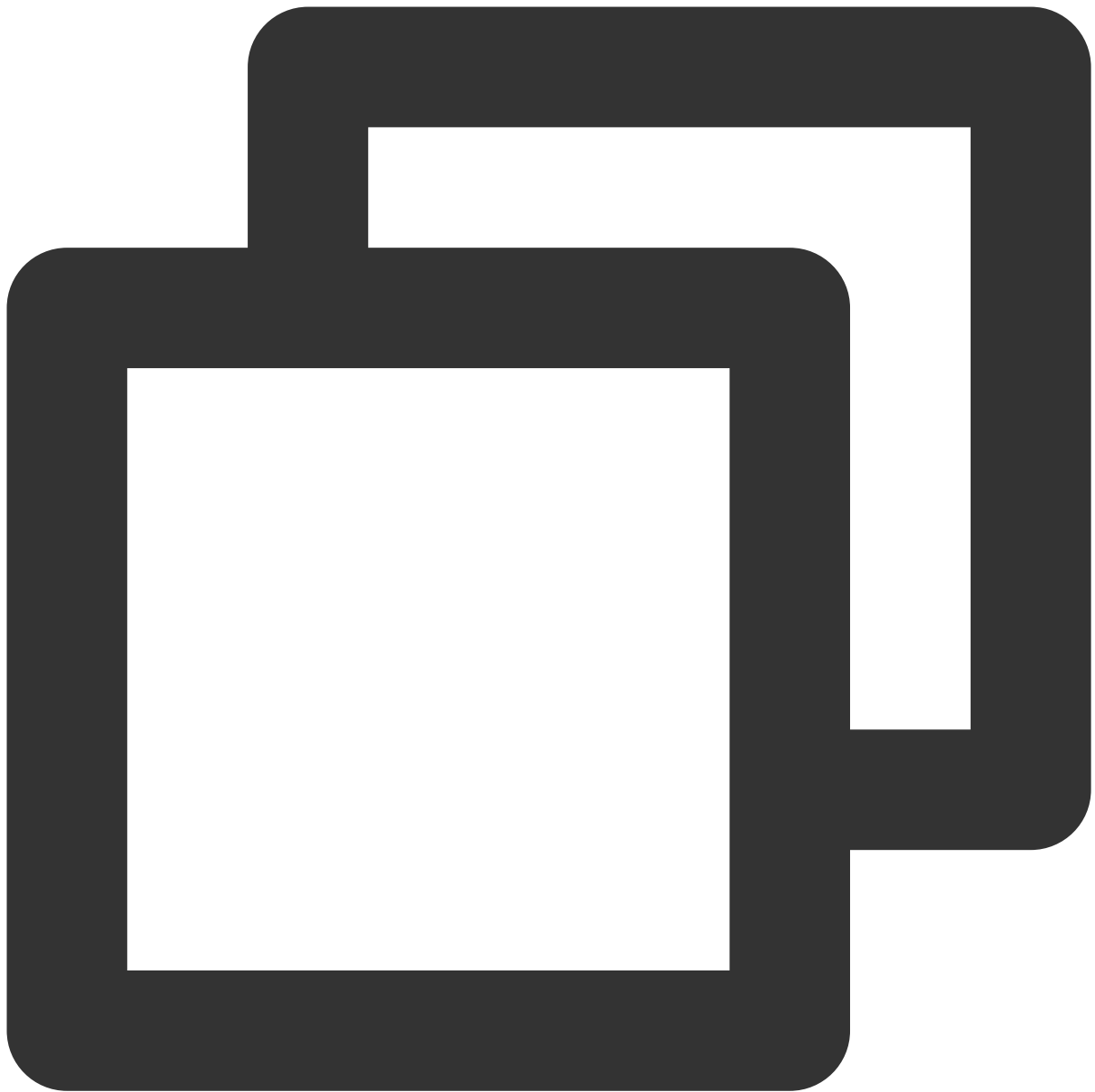


```
wget https://github.com/rdesktop/rdesktop/releases/download/v1.8.3/rdesktop-1.8.3.t
```

If you want to install the latest version, visit [the rdesktop page on GitHub](#) to find it. Then replace the path in the command with that of the latest version.

3. In the directory where rdesktop will be installed, run the following commands to decompress and install rdesktop.





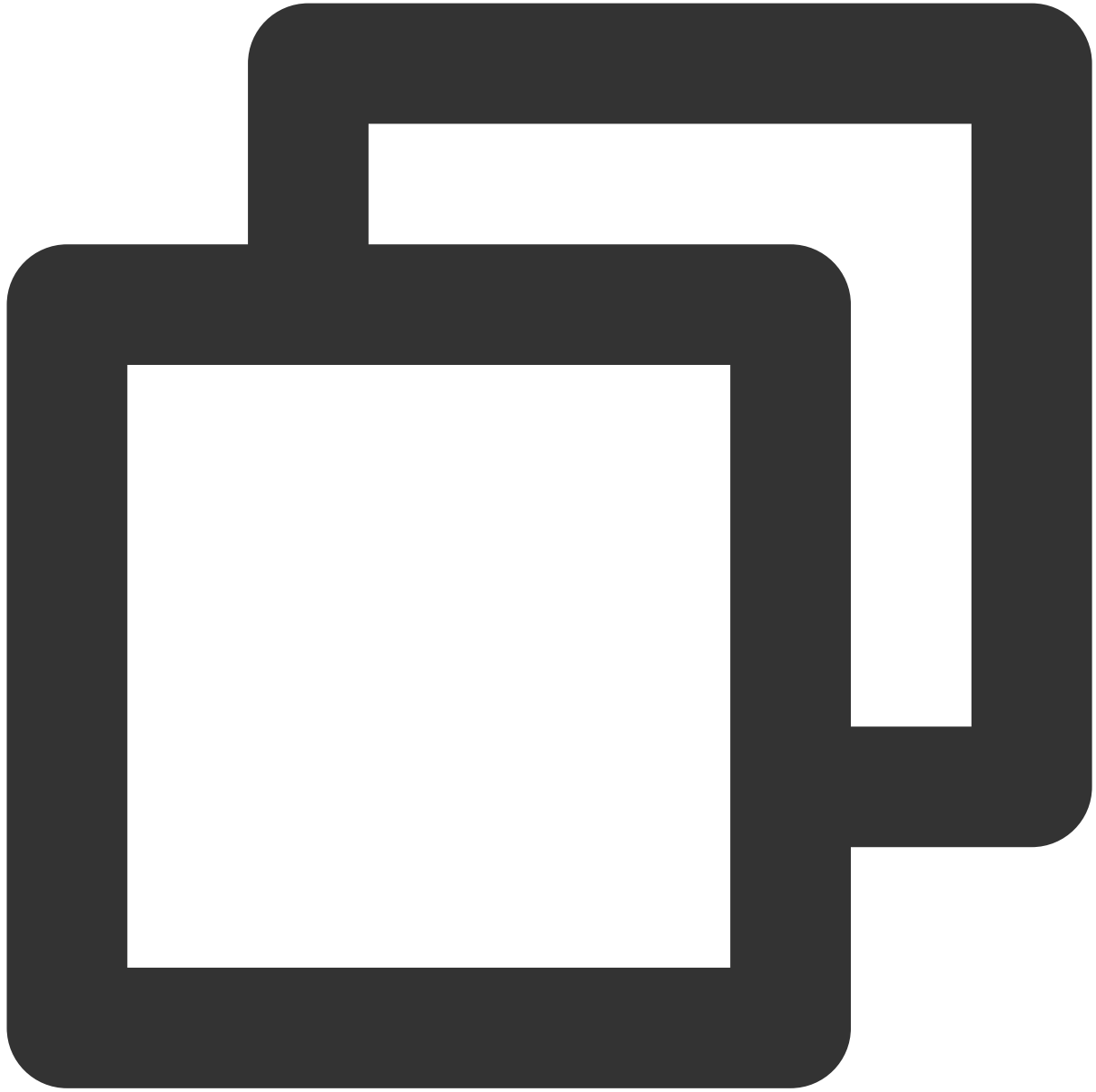
```
tar xvzf rdesktop-<x.x.x>.tar.gz ## Replace x.x.x with the version number of the do
cd rdesktop-1.8.3
./configure
make
make install
```

4.

Run the following command to connect to the remote Windows instance.

**Note:**

Replace the parameters in the example with your own parameters.



```
rdesktop -u Administrator -p <your-password> <hostname or IP address>
```

`Administrator` refers to the admin account mentioned in the prerequisites section.

`<your-password>` refers to the login password that you set.

If you forgot your password, you can [reset it](#).

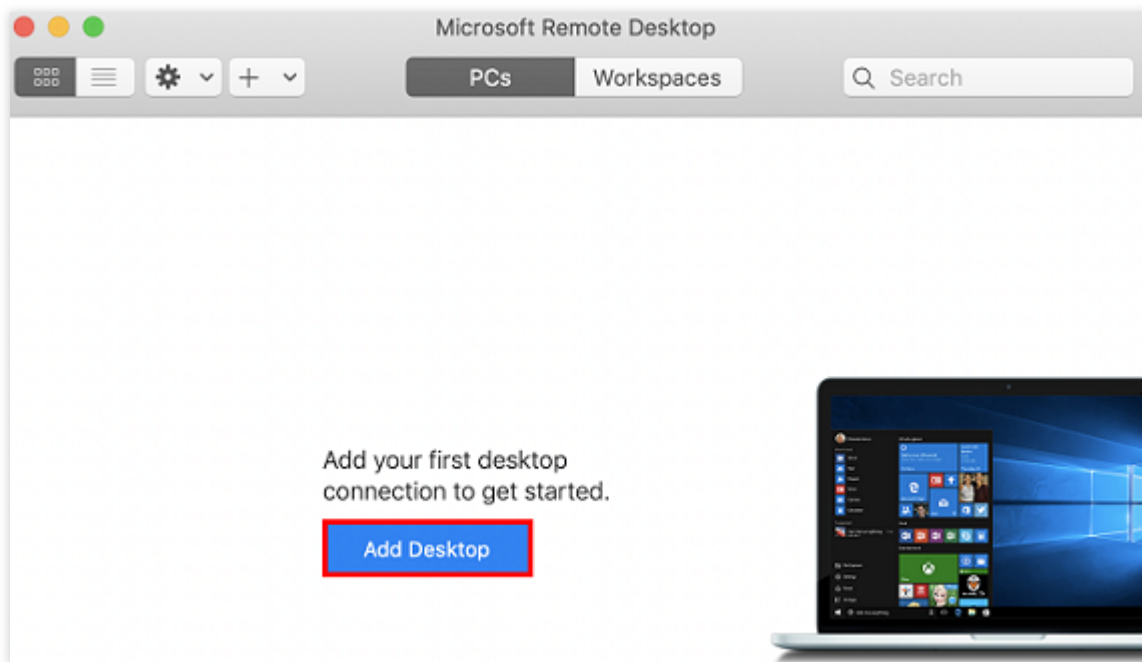
`<hostname or IP address>` refers to the public IP address or custom domain name of your Windows instance.

**Note:**

The following operations use Microsoft Remote Desktop for Mac as an example. Microsoft stopped providing a link to download the Remote Desktop client in 2017. Currently, its subsidiary HockeyApp is responsible for releasing the beta client. Go to [Microsoft Remote Desktop Beta](#) to download a Beta version.

The following operations use a Lighthouse instance on Windows Server 2012 R2 as an example:

1. Download and install Microsoft Remote Desktop for Mac on your local computer.
2. Start MRD and click **Add Desktop**.



3. In the **Add PC** pop-up window, follow the steps illustrated in the following image to establish a connection to your Windows instance.

**Add PC**

PC name: 118.

User account: Ask when required

**General** Display Devices & Audio Folders

Friendly name: Optional

Group: Saved PCs

Gateway: No gateway

☒ Bypass for local addresses

☒ Reconnect if the connection is dropped

☐ Connect to an admin session

☐ Swap mouse buttons

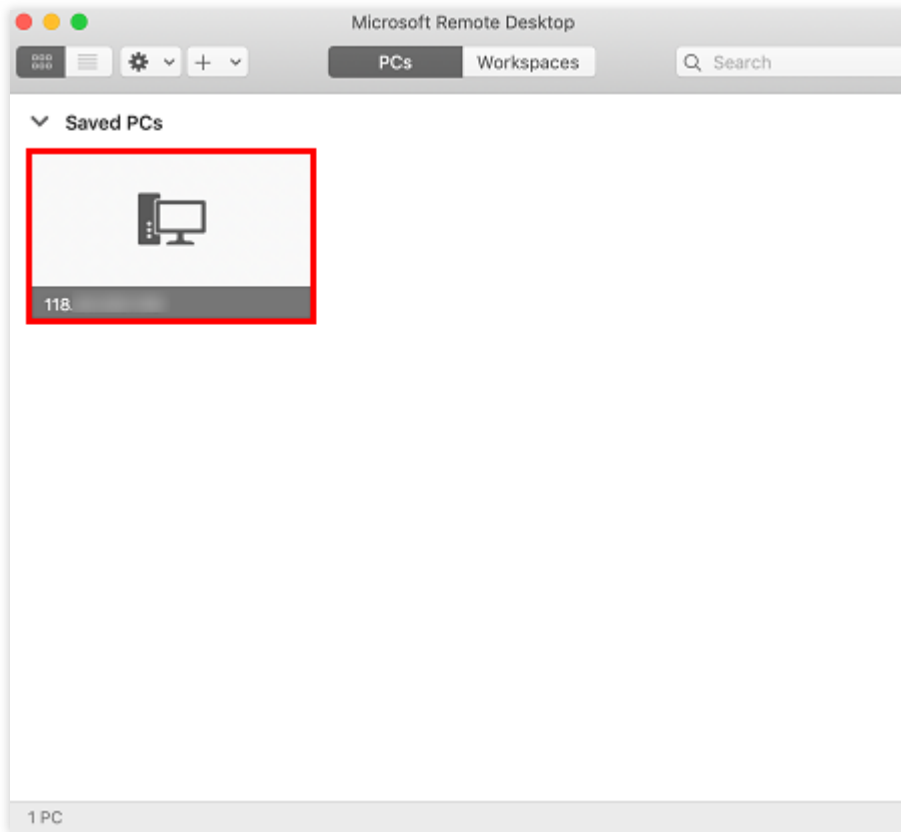
Cancel Add

3.1 In the **PC name** field, enter the instance's public IP.

3.2 Click **Add**.

3.3 Retain the default settings for the other options and establish the connection.

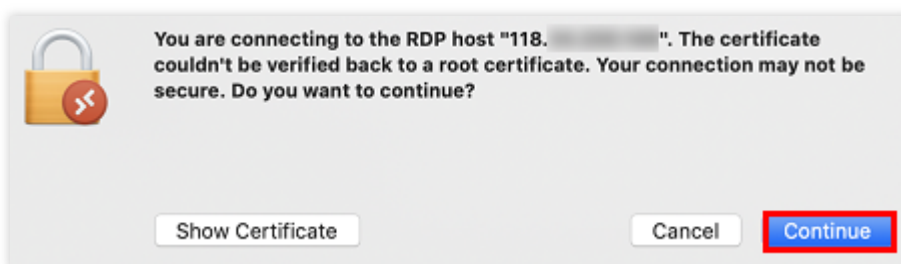
Your entry has now been saved



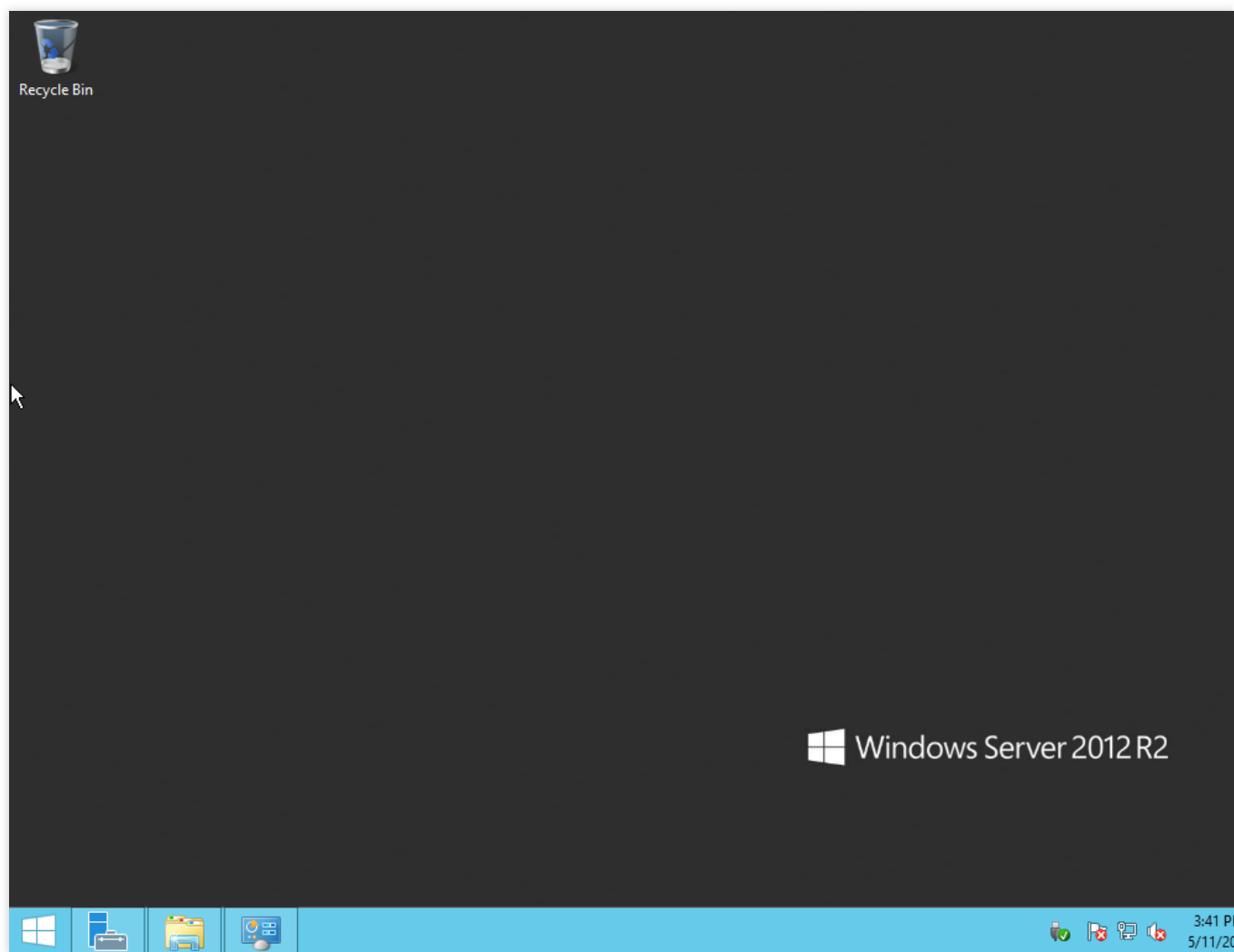
4. Double-click the new entry. In the pop-up window, enter your admin account and password obtained in "Prerequisites" as prompted and click **Continue**.

If you forgot your password, you can [reset it](#).

5. In the pop-up window, click **Continue** to establish the connection.



If the connection is successful, the following Windows instance page will appear:



# Managing Instances

## Resetting the instances passwords

### Password Reset Operation Instruction

Last updated : 2024-08-14 14:40:44

## Overview

Tencent Cloud Lighthouse offers the instance login password reset feature. This feature is mainly applicable to the following scenario:

A remote login to the instance is initiated from a local computer for the first time.

You need to reset the user (root) password before the first remote login or SSH key login of a Linux instance.

Before the initial login to the Windows instance, if you have set the **login method** to **automatically generating a password** during the instance creation, you are advised to perform this operation to reset the password of the administrator account (such as Administrator), to replace it with a custom login password.

Reset the password if you have forgotten your instance login password.

## Notes

The Tencent Cloud Lighthouse Console offers two approaches to reset passwords, including **Online Reset** and **Offline Reset**.

If you choose online reset, the server will shut down during the password reset of a running instance. To avoid any data losses, plan for the operation time in advance. It is recommended that you perform the operation during business off-peak periods, to minimize impact.

If you choose to reset the password online, please ensure that the **status** and **Tencent Cloud Automation Tools status** of your selected instance are both **running**.

Instances created using the Ubuntu image, by default, disallow the root user from logging in to the instance through password authentication. To enable this method, see [How do I log in to an instance as the root user on Ubuntu?](#)

For enhancing the security of your instance, it is recommended that you log in to the Linux instance using the SSH key pair method. For further information, see [Managing Keys](#).

## Directions

1. After you log in to the [Tencent Cloud Lighthouse Console](#), find the corresponding instance in the server list. You can open the window to reset the instance password as follows:

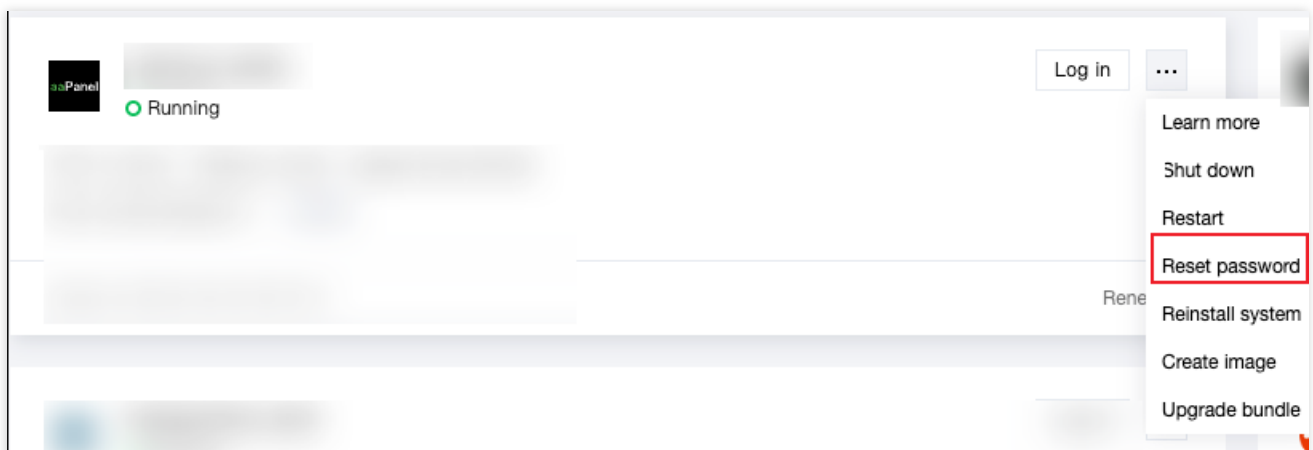
Instance Card

Instance List

Instance Details Page

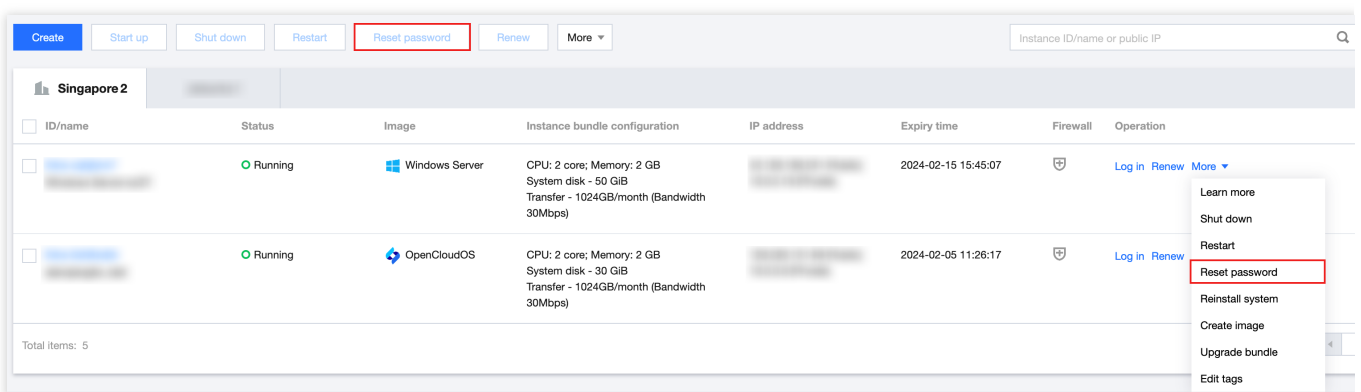
Resetting the **Single** instance password: In the instance card, choose

 **> Reset password.**



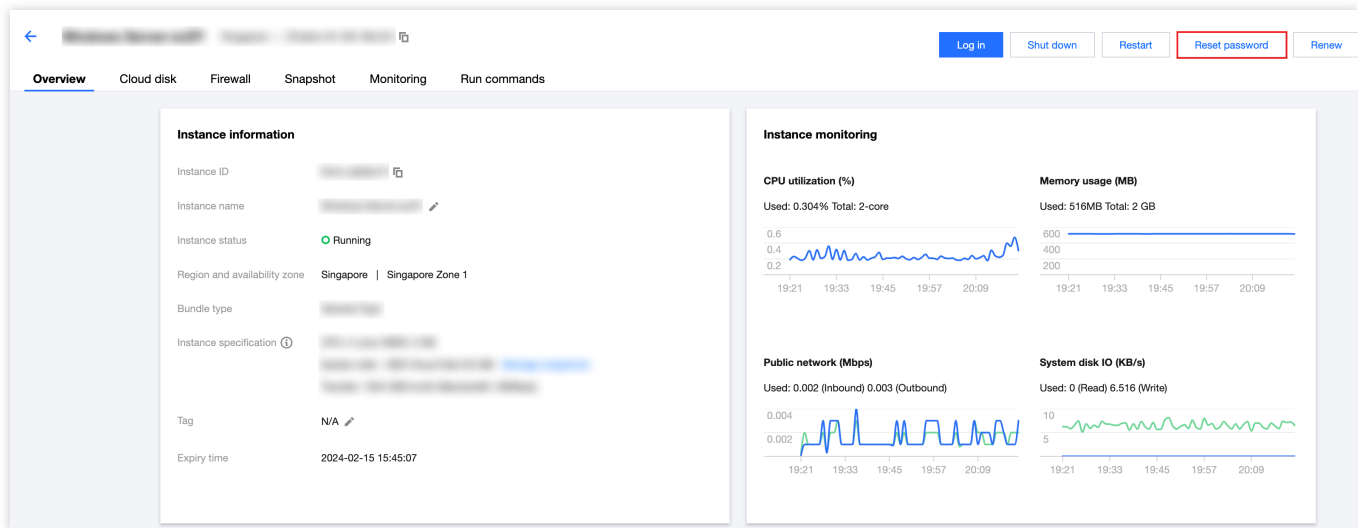
Resetting the **Single** instance password: Choose **More > Reset Password** on the right side of the instance for which the password needs to be reset.

Resetting **Multiple** instance passwords: In the instance list, select the instances for which you want to reset the password, and click **Reset Password** above.



Enter the details page of the instance, click **Reset Password** in the upper right corner of the page.





2. In the pop-up window, based on the **instance status** and **Tencent Cloud Automation Tools status**, you can choose to reset the password online or offline. More details as follows:

#### Note:

The online password reset process uses [Tencent Cloud Automation Tools](#) to execute the password reset command within the instance. The password reset does not require shutdown, without disrupting the business.

Online Password Reset

Offline Password Reset

#### Note:

Prerequisites: Ensure the **Instance Status** and the **Tencent Cloud Automation Tools Status** of your selected instance are both **Running**. Otherwise, the password cannot be reset online.

1. Confirm the **Username** for which the password need to be reset.

#### Note:

The default username for the Ubuntu system is ubuntu.

2. Enter a **New Password** and **Confirm Password** that meet the complexity requirements.

#### Note:

When both Linux and Windows machines are selected simultaneously, password complexity requirements must be compliant with the requirements of the Windows system.

3. Click **OK** to complete the reset.

### Reset password

You've selected 1 instance. [less](#) [Learn More](#)

Instance ID/name	Bundle configuration	Instance status	TencentCloud Automation Tools (TAT) ⓘ
	CPU: 2 core; Memory: 2 GB System disk: SSD Cloud Disk 50 GB Transfer - 1024 GB/month (Bandwidth: 30Mbps)	Running	Running

ⓘ For Linux instances bound with SSH keys, after the password is reset, you can log in remotely with both the new password and the original SSH key.

Username

New password

Confirm password

Reset mode

☒ **Reset online**  
Reset the password via the TAT agent without shutting down the instance. [Learn more](#)

☐ **Reset offline**  
You need to shut down the instance to reset the password.

4. After the password reset is complete, you may proceed to the details page of the target instance to check the password reset result, choose **Run\*\*\*\* Command** and click the **View execution details** on the right side of the command line.

Overview	Cloud disk	Firewall	Snapshot	Monitoring	Run commands
ⓘ Lighthouse now supports <a href="#">Tencent Cloud Automation Tools (TAT)</a> , which enables you to manage and operate instances, check the task progress and history via commands, without logging in to an instance.					
<input type="button" value="Execute command"/> <input type="text" value="Separate keywords with ' '; press Enter to separate filter tags"/>					
Execution ID	Execute task ID	Start time	Time elapsed	Execution result	Operation
inv-kq4vxmuzh9	invt-kgzdpkls	2024-01-17 20:09:47	2 second(s)	Command successful	<a href="#">View execution details</a>

#### Note:

For Linux instances, if in the `sshd_config` configuration file, the `PasswordAuthentication` parameter is set to `No` , during an online password reset, this parameter will be changed to `Yes` . In the mean time, the `sshd` process within the instance will be restarted, possibly disrupting connected SSH sessions.

For Windows instances, if the user you have chosen to reset the password for is locked or disabled, this user will also be automatically enabled during online password reset.

If your online password reset fails or does not take effect, see [Troubleshoot the Issue That the Password Fails To Be Reset Online or Is Invalid](#) to investigate the cause.

**Note:**

If you choose offline password reset, note that servers will be shut down during the reset process for running instances. It is recommended that you perform the operation during business off-peak periods, to minimize impact of service shutdown.

1. Confirm the **Username** for which the password need to be reset.

**Note:**

The default username for the Ubuntu system is ubuntu.

2. Enter a **New Password** and **Confirm Password** that meet the complexity requirements.

**Note:**

When both Linux and Windows machines are selected simultaneously, password complexity requirements must be compliant with the requirements of the Windows system.

3. Read and check the **Offline Reset Notice**, and click **OK** to complete the reset.

**Reset password** ×

You've selected 1 instance. [less](#) [Learn More](#)

Instance ID/name	Bundle configuration	Instance status	TencentCloud Automation Tools (TAT) ⓘ
lhins-n2nyd3w9 Windows Server-XKfL	CPU: 2 core; Memory: 2 GB System disk: SSD Cloud Disk 50 GB Transfer - 1024 GB/month (Bandwidth: 30Mbps)	Running	Running

ⓘ For Linux instances bound with SSH keys, after the password is reset, you can log in remotely with both the new password and the original SSH key.

Username

System default

Administrator

New password

Please enter the instance

Confirm password

Please enter the instance

Reset mode

☐ Reset online

Reset the password via the TAT agent without shutting down the instance. [Learn more](#)

☒ Reset offline

You need to shut down the instance to reset the password.

- Note that Running instances will be **shut down forcibly**.
- Forced shutdown may result in **data loss or file system corruption**. We recommend manually shutting down the instance before the operation.
- It may take a long time to forcibly shut down the instance.
- After the password is reset, running instances resume the Running status.

☐ I acknowledge the above statement

OK

Cancel

**Note:**

If your offline password reset fails or does not take effect, see [Troubleshoot the Issue That the Password Reset Fails To Be Reset Offline or Is Invalid for The Windows Instance](#).

# Troubleshoot the Issue That the Password Fails To Be Reset Online or Is Invalid

Last updated : 2024-02-21 15:06:42

This document describes the symptoms and solutions when the online password reset operation for Tencent Cloud Lighthouse instances fails or does not take effect.

## Symptom

After the online instance password reset, a message is displayed indicating **Password Reset Failure**.  
After the online instance password reset, the new password does not take effect, and the login password is still the original one.

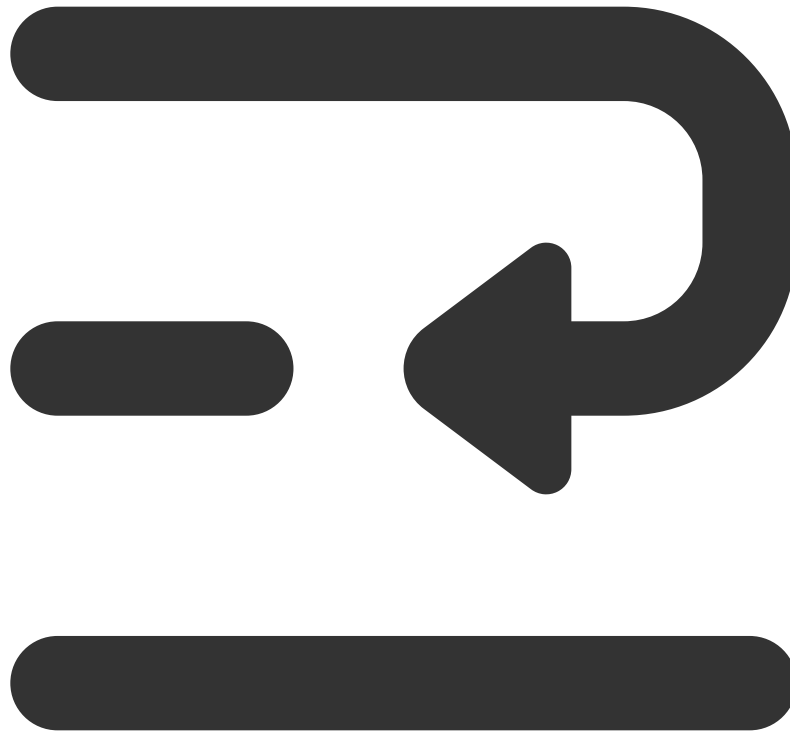
## Possible Causes and Solutions

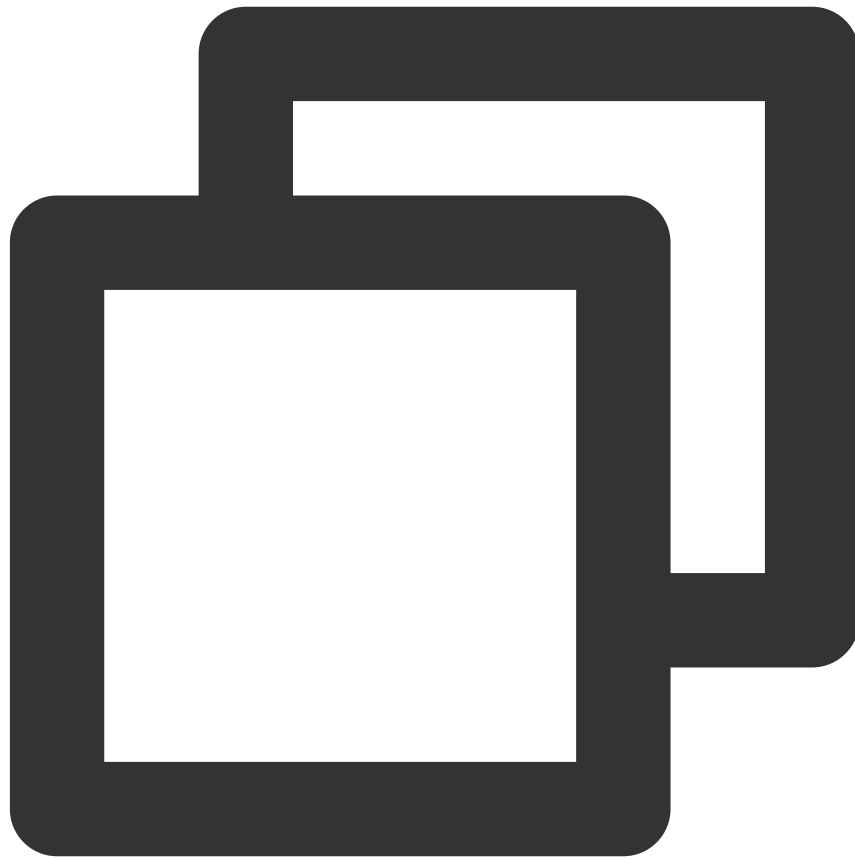
### Linux Instances

**Note:**

Error messages may differ among different systems.

Cause	Error Prompt	Solution
The username does not exist.		The enter does not confirm w entered u correct.

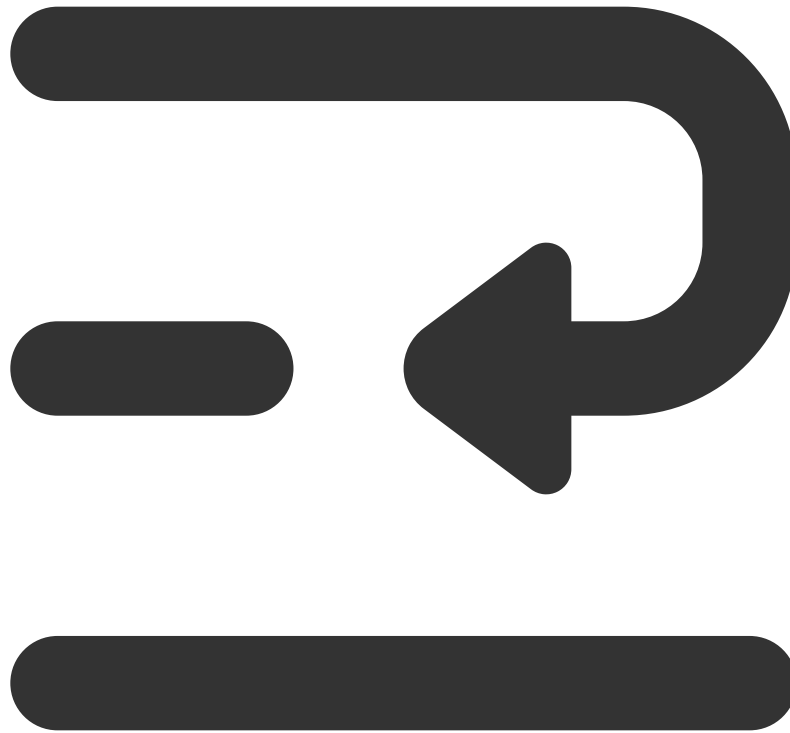




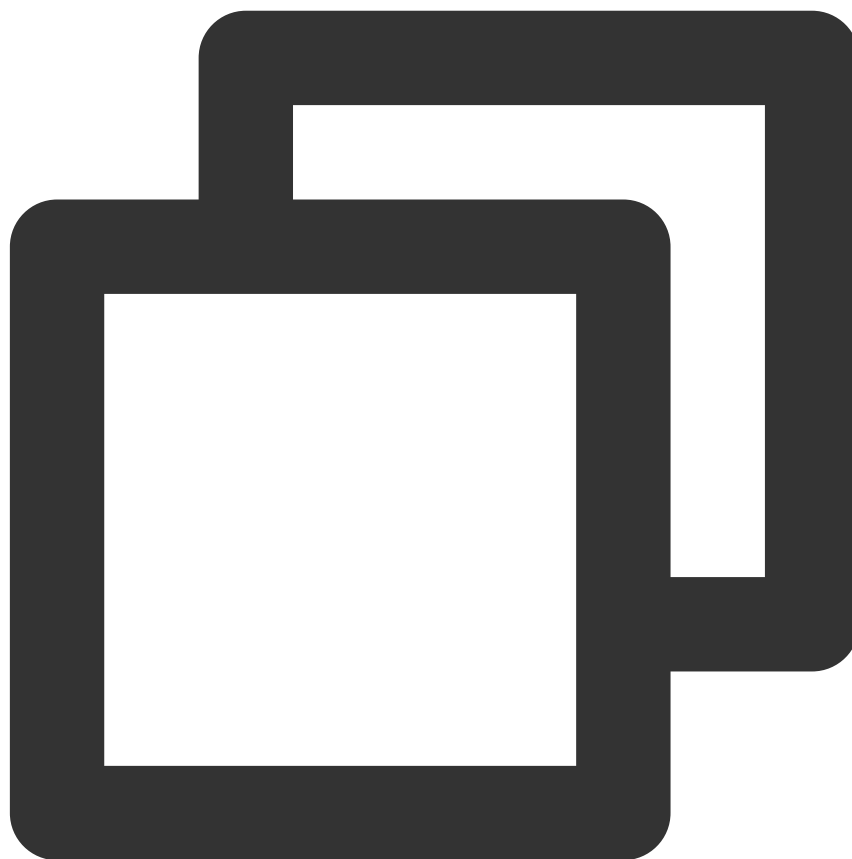
```
chpasswd: line 1: user 'ubuntu' does not existchpasswd:
error detected,
changes ignored
```

The  
chpasswd  
command is  
not found.

If the inst:  
be loggec  
normally,  
instance :  
command  
type f  
"chpass  
check wh  
chpasswd  
If the inst:  
be loggec  
normally,  
enter the  
to check i  
in the chp  
system fil





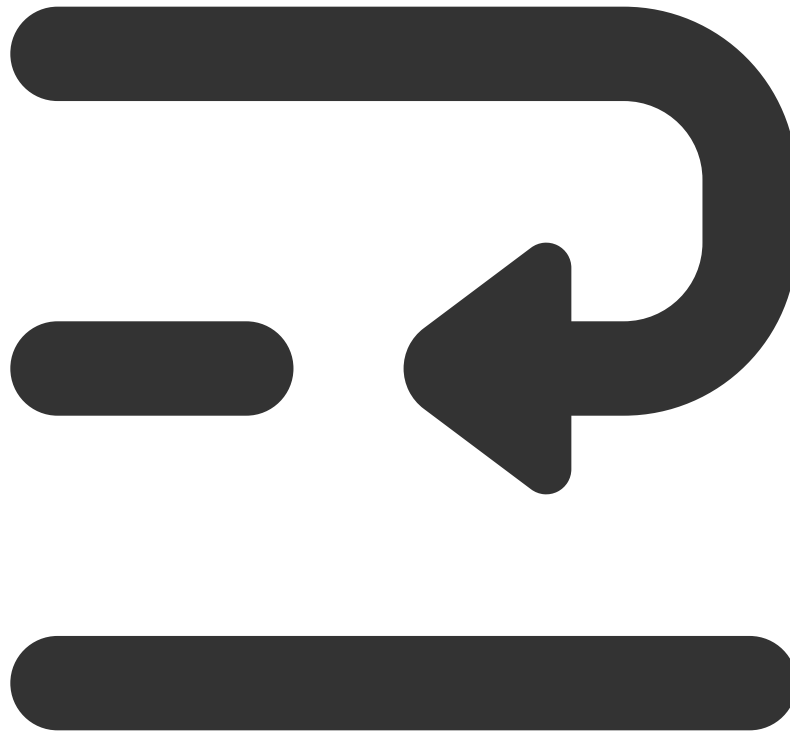


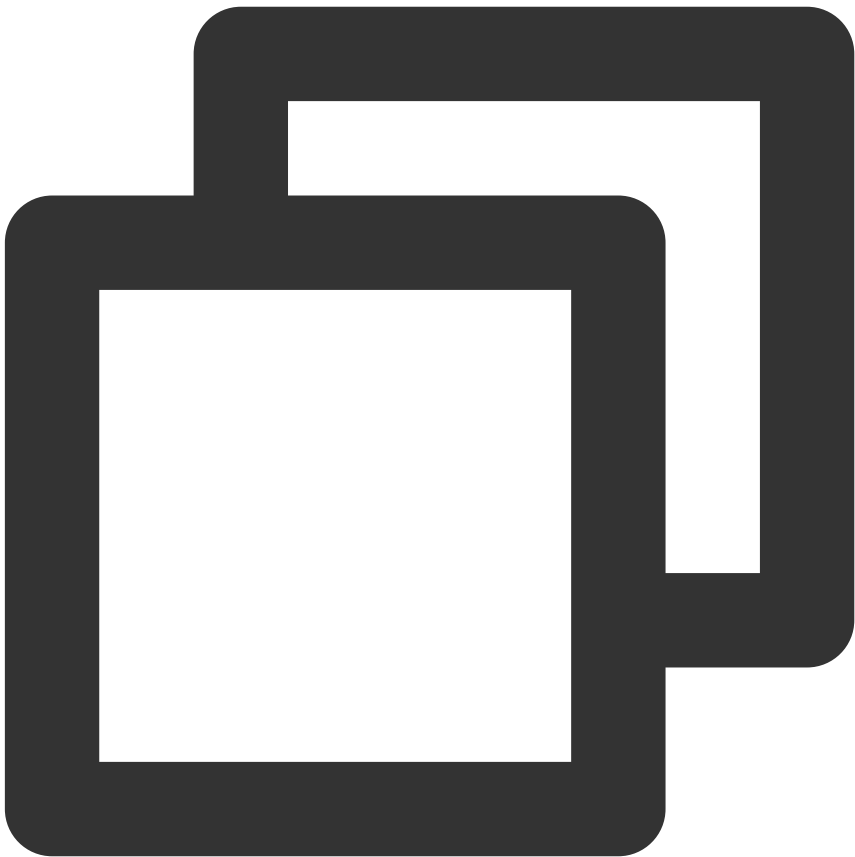
```
-bash: chpasswd: command not found
```

cannot lock  
/etc/passwd

Log in to  
and execute  
following  
recovery.  
instance  
logged in  
is recomr  
you resta  
instance.

```
rm  
/etc/pa  
rm  
/etc/sh
```

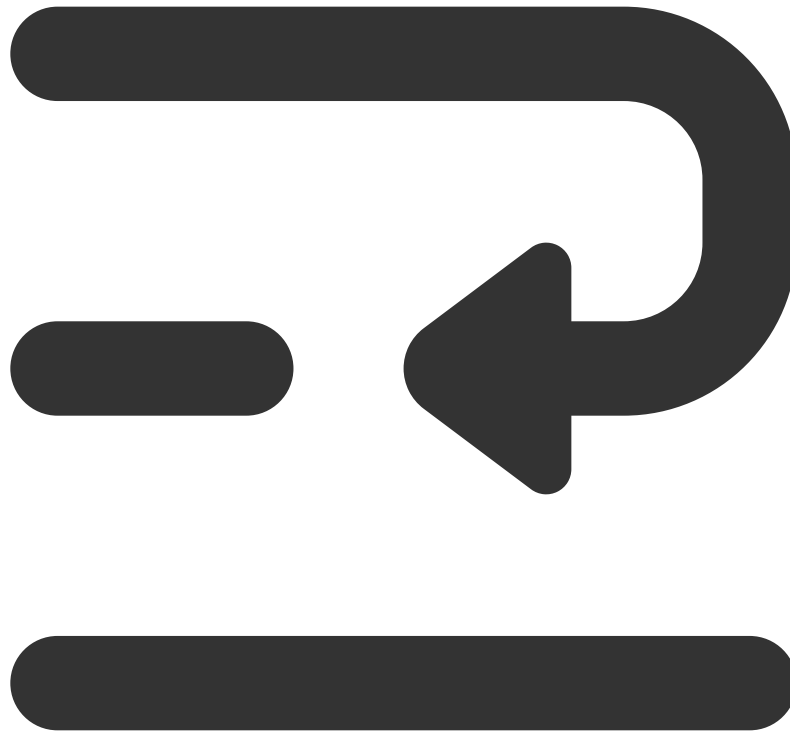


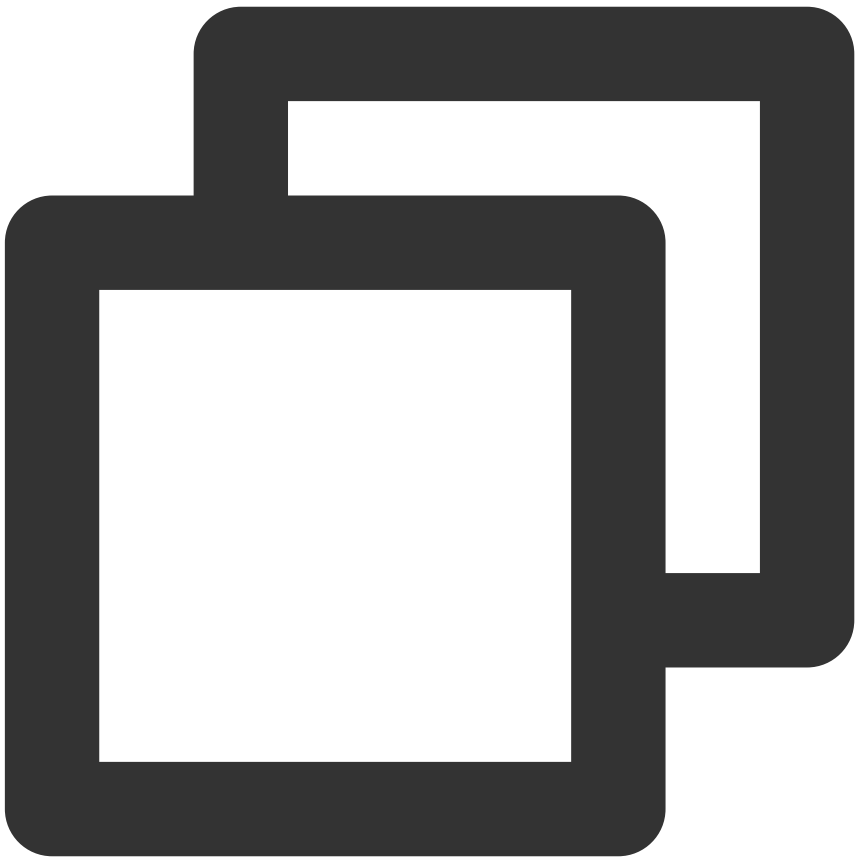


```
cannot lock /etc/passwd; try again later.
```

chpasswd:  
cannot open  
/etc/shadow

Log in to  
and execute  
`+i /etc`  
for repair.  
unable to  
instance,  
enter the  
and execute  
`+i /etc`  
following  
repair.

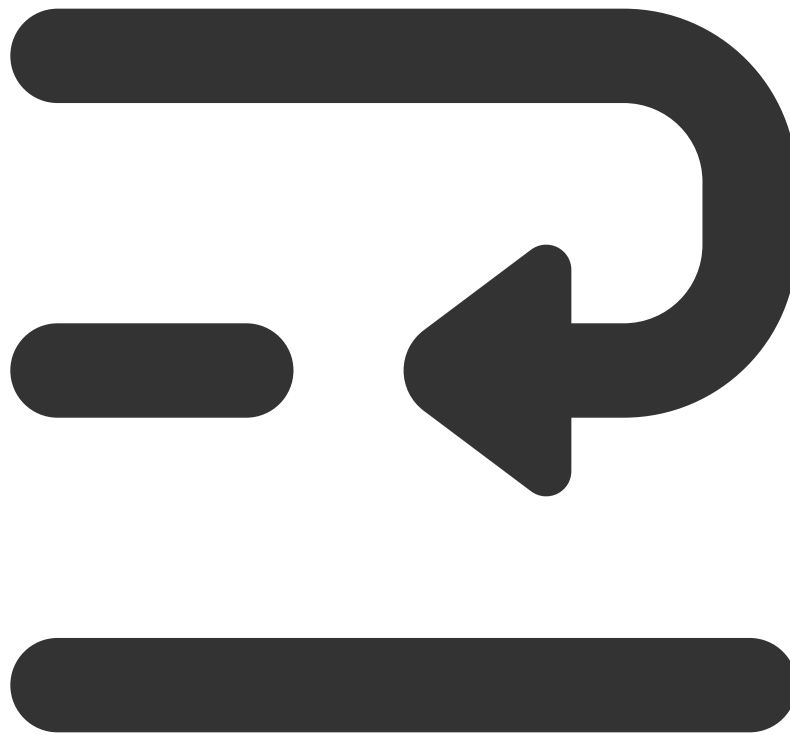


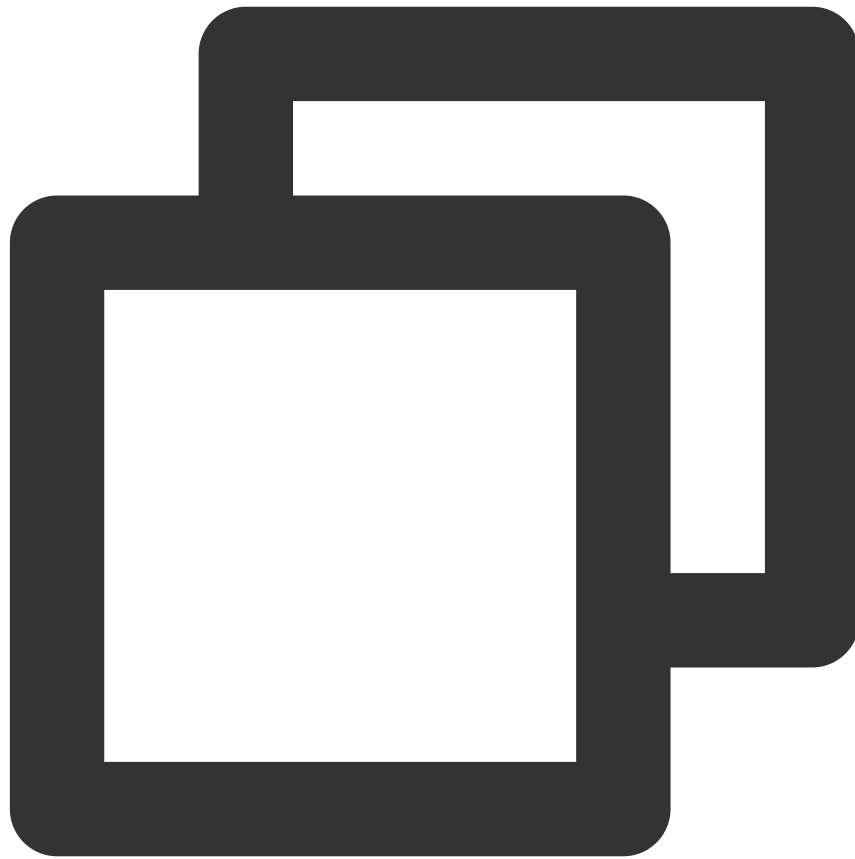


```
chpasswd: cannot open /etc/shadow
```

Errors are related to PAM authentication failed and other PAM related issues

Log in to and go to /etc/pa check if tl correspor configura modified. know hov you can b and then public im: configura cannot lo instance, enter the for repair.





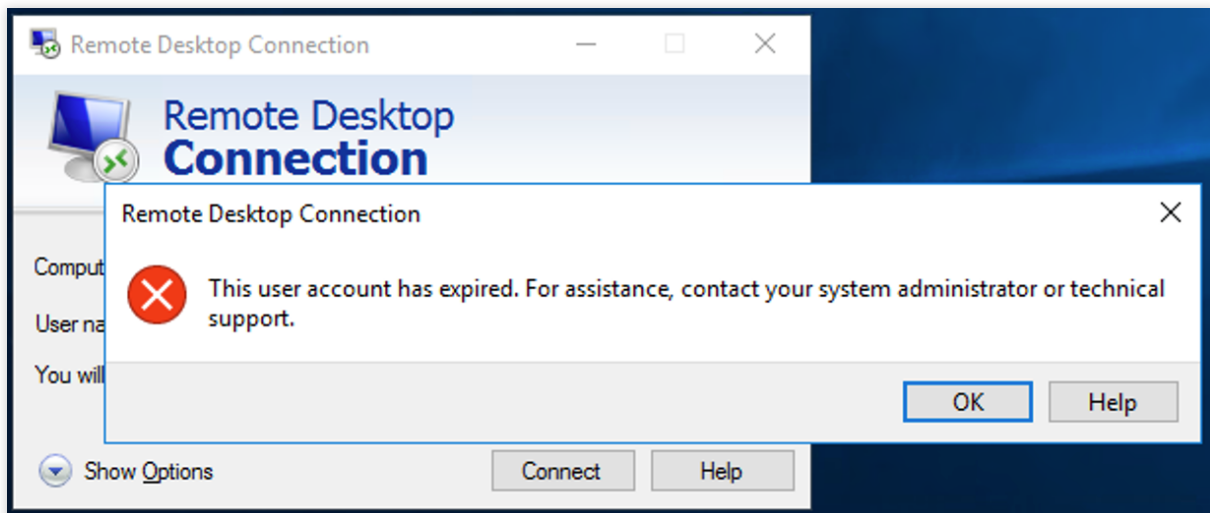
PAM authentication failed

## Windows Instances

### Success Prompt Scenario

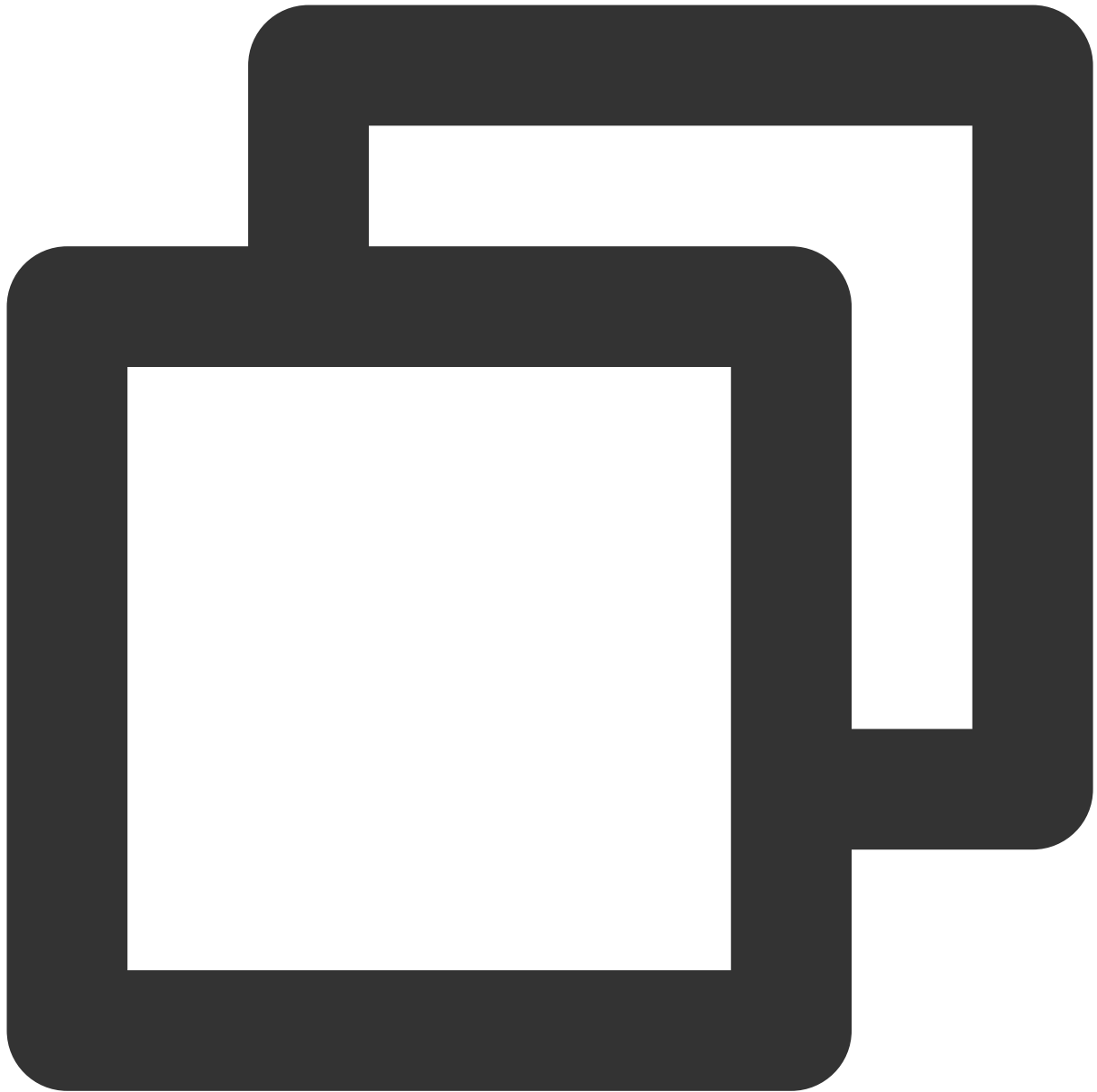
**Scenario one: the account has already expired, but the prompt for successful password reset is still displayed.**

Error prompt:



Solution: Use commands to set it to no expiration.



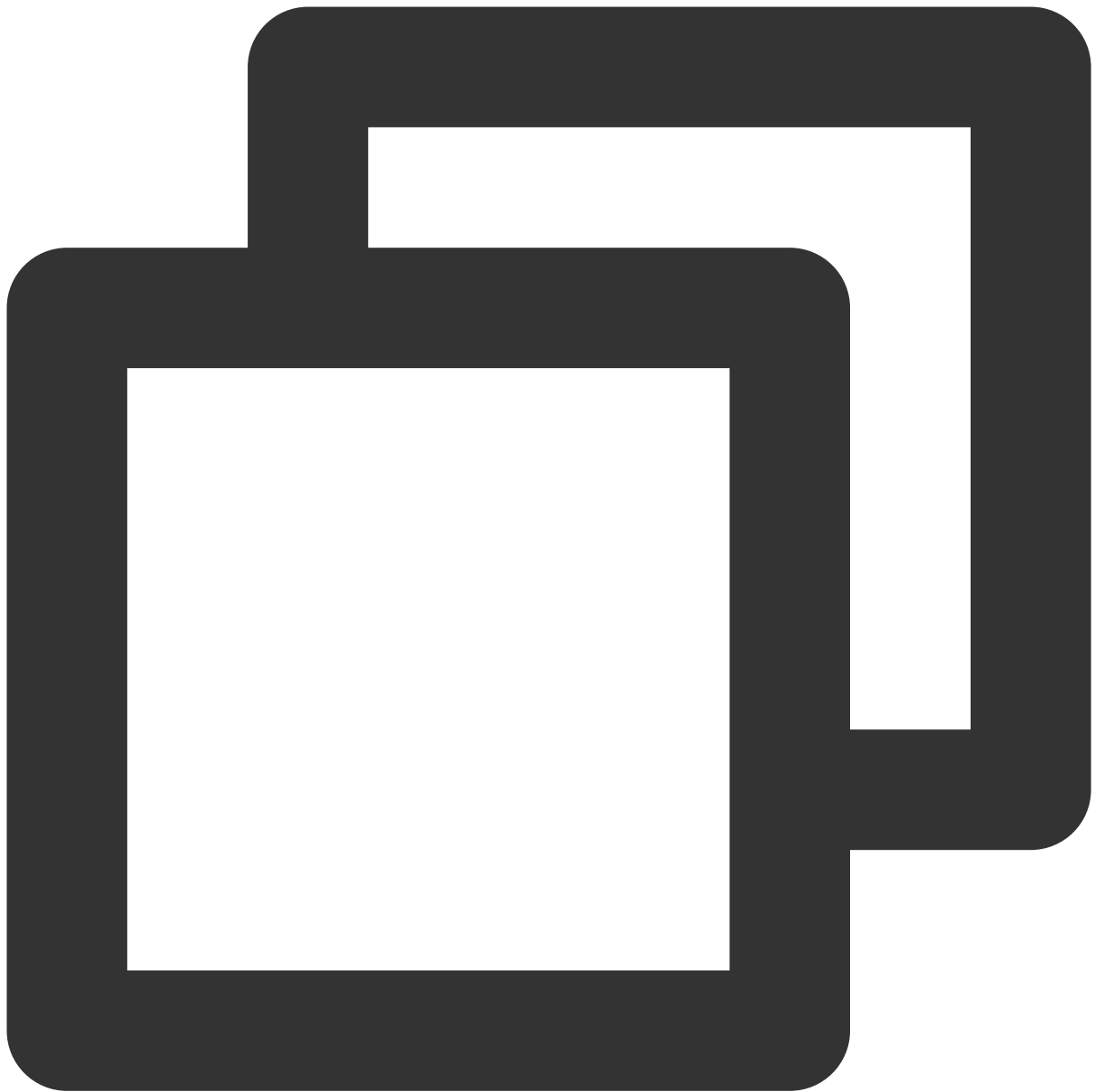


```
set-localuser Admin -AccountExpires "2099/6/6 20:53:35"
```

### Failure Prompt Scenario

**Scenario one: the username does not exist./entered username is incorrect.**

Error prompt:

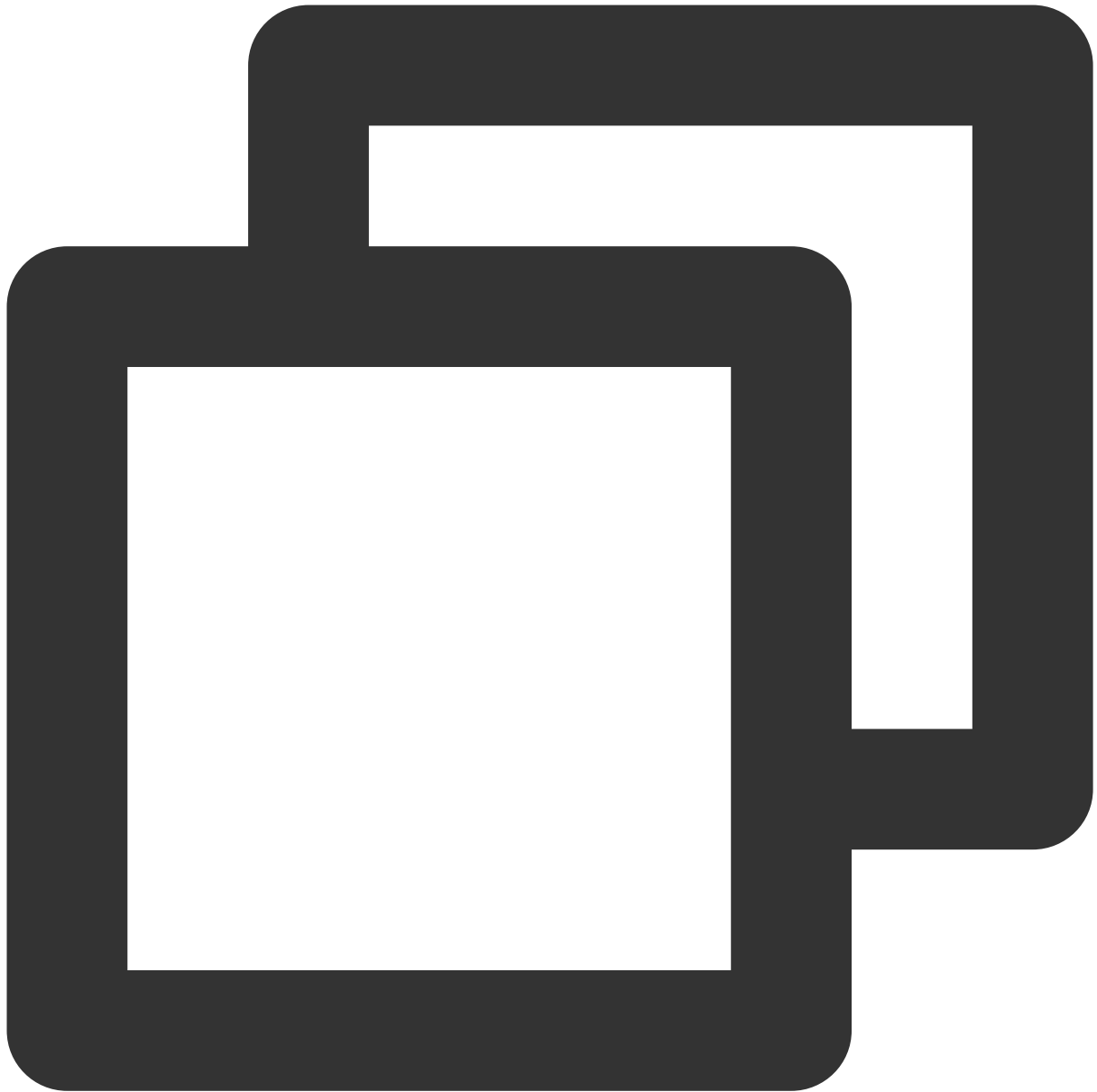


```
The user name could not be found.  
More help is available by typing NET HELPMSG 2221.
```

Solution: Remind the user to check whether the entered username exists and whether it is correct, and if it is incorrect, please enter the correct username.

**Scenario two: the password does not meet complexity requirements.**

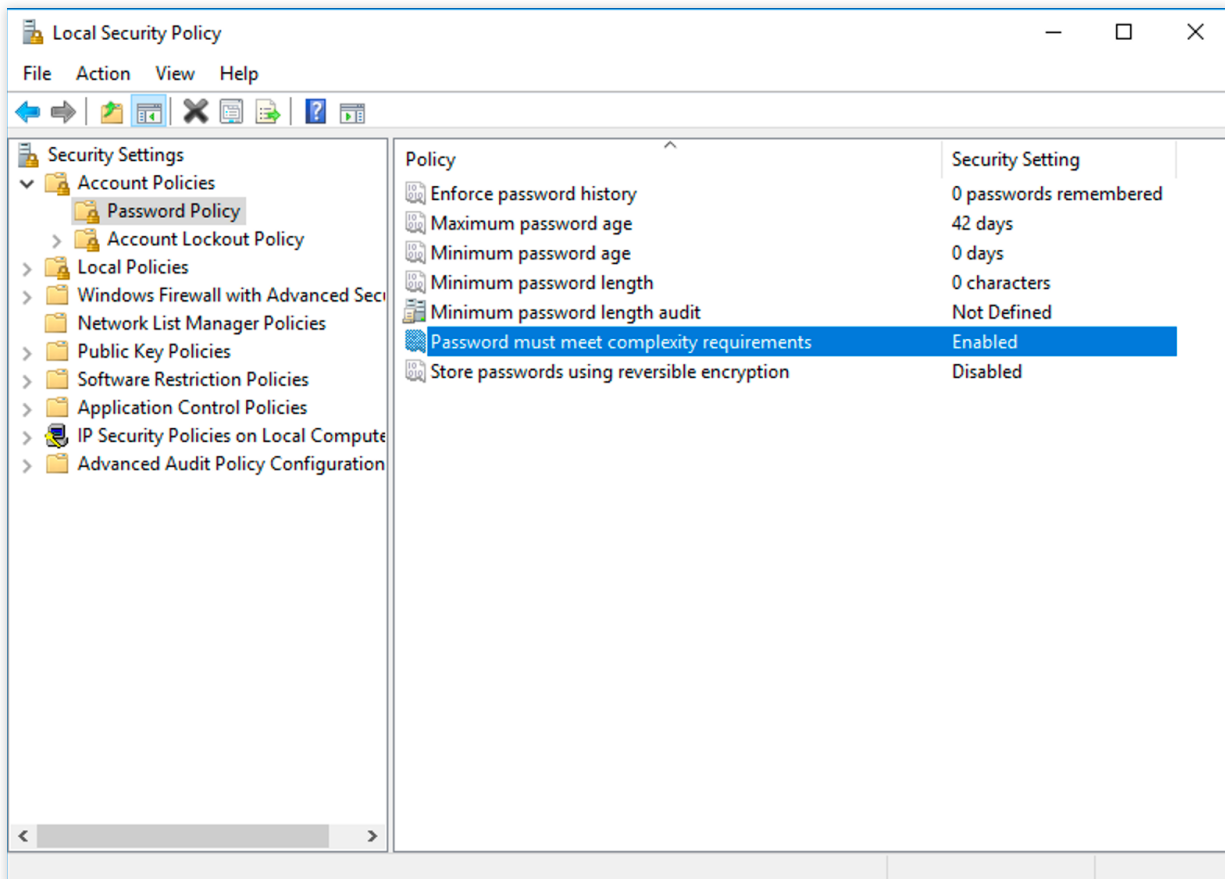
Error prompt:



The password does not meet the password policy requirements. Check the minimum pass  
More help is available by typing NET HELPMSG 2245.

**Solution:**

Run PowerShell as an administrator, enter `secpol.msc` and press Enter to open **Local Security Policy**. Expand Account Policies > Password Policy. Then, you can see that **Password must meet complexity requirements** is enabled by default.

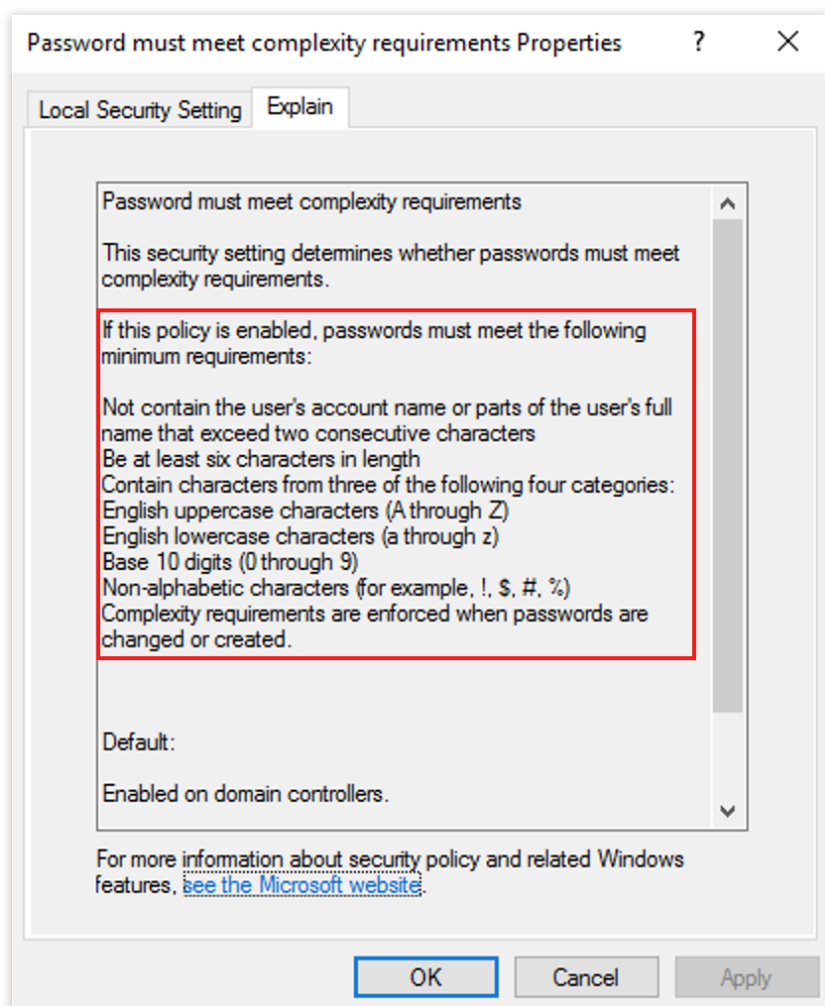


Right-click **Password must meet complexity requirements** and open **Properties**. The minimum password requirements are displayed:

The password cannot include the username (account name) string.

The password must contain a minimum of six characters.

The password must include at least three out of the four following categories: uppercase characters, lowercase characters, digits, and non-alphabetic characters.



# Troubleshoot the Issue That the Password Reset Fails To Be Reset Offline or Is Invalid for The Windows Instance

Last updated : 2024-02-21 15:11:02

This document takes Windows Server 2012 R2 operating system as an example to demonstrate the troubleshooting methods and solutions for failed or ineffective password resets on Windows Tencent Cloud Lighthouse instances.

## Symptom

After the instance password reset, you receive the message **\*\*Due to system congestion, your instance password reset failed (7617d94c)\*\***.

After the instance password reset, the new password does not take effect, and the login password is still the original one.

## Possible Causes

The possible causes for failure or ineffectiveness of instance password reset are as follows:

The `cloudbase-init` component in Tencent Cloud Lighthouse is damaged, modified, disabled, or not started.

If third-party security software such as 360 Total Security or Huorong Security is installed on Tencent Cloud Lighthouse, the `cloudbase-init` component for password reset may be blocked, resulting in instance password reset failures.

If Tencent Cloud Lighthouse has been invaded and encrypted causing the password to be invalid, it is recommended that you back up the data and reinstall the system.

## Directions

Based on the possible reasons for the unsuccessful password reset, two verification methods are provided:

### Checking the cloudbase-init Service

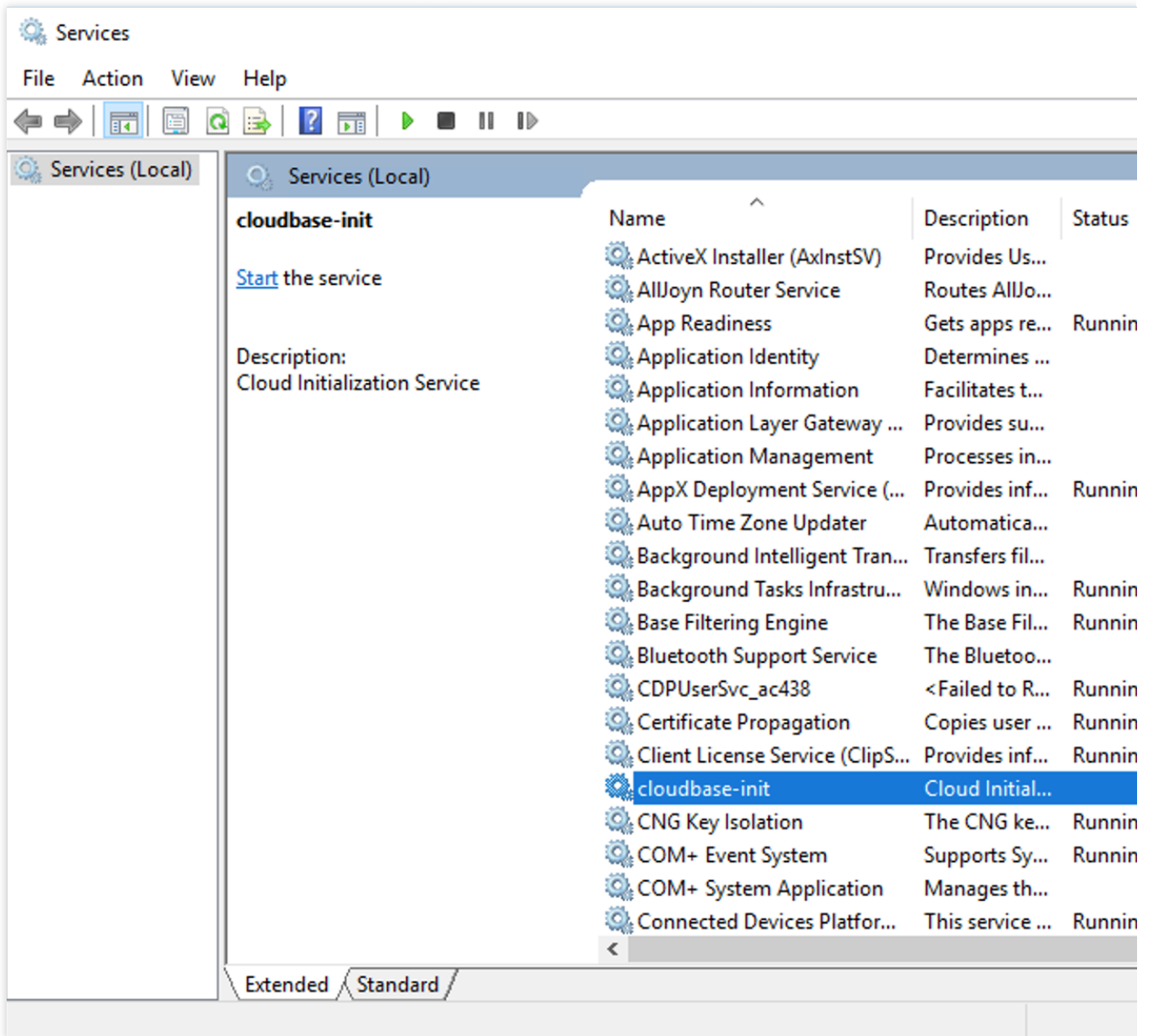
1. [Log in to the Windows instance via VNC](#).
2. On the operating system interface, right-click



and choose **Run** from the pop-up menu.

3. In the **Run** dialog box, enter **services.msc** and press **Enter** to open the **Services** window.

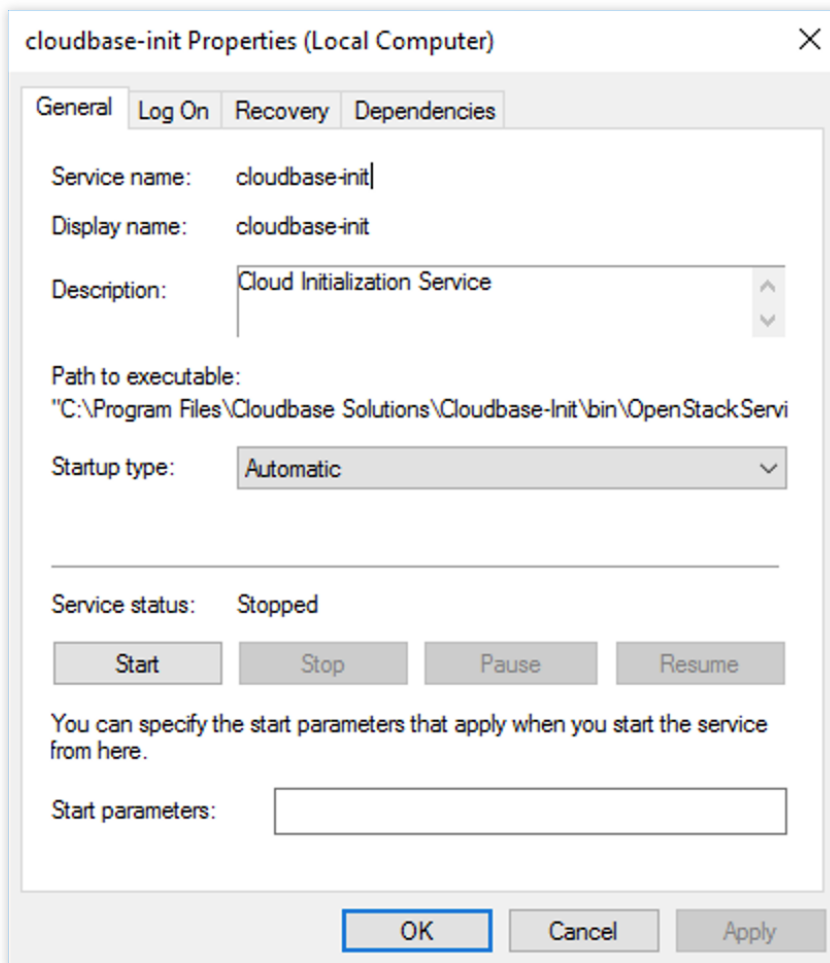
4. In the **Services** window, check whether the `cloudbase-init` service exists. See the following figure:



If yes, proceed to the next step.

If no, reinstall the `cloudbase-init` service. For further instructions, see [Installing Cloudbase-Init on Windows](#).

5. Double-click to open the properties of `cloudbase-init`. See the following figure:



6. Select the **General** tab and check whether **startup type** of `cloudbase-init` is set to **Automatic**.

If yes, proceed to the next step.

If no, set startup type of `cloudbase-init` to **Automatic**.

7. Switch to the **Log On** tab and check whether the login identity of `cloudbase-init` has been set to **Local System account**.

If yes, proceed to the next step.

If no, set the login identity of `cloudbase-init` to **Local System Account**.

8. Select the **General** tab and click **Start** under Service Status to manually launch the `cloudbase-init` service and check whether there are any errors.

If yes, proceed to [Checking the Security Software Installed on Tencent Cloud Lighthouse](#).

If no, proceed to the next step.

9. On the operating system interface, right-click

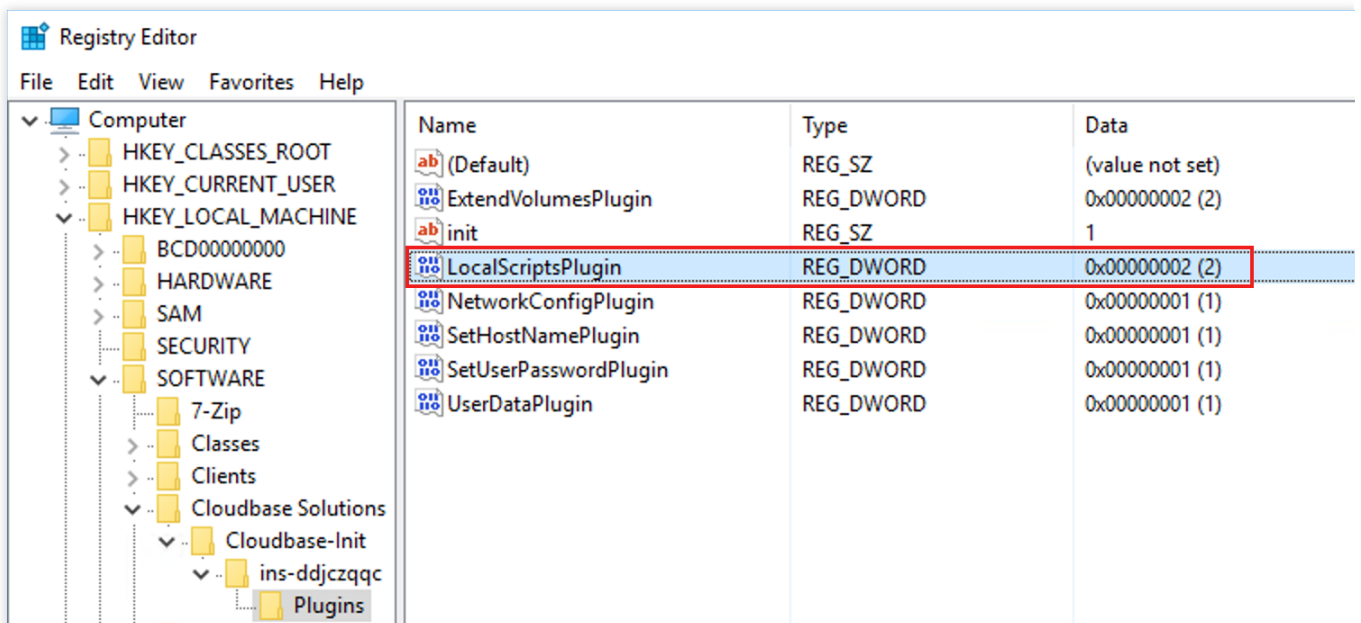


and choose **Run** from the pop-up menu.

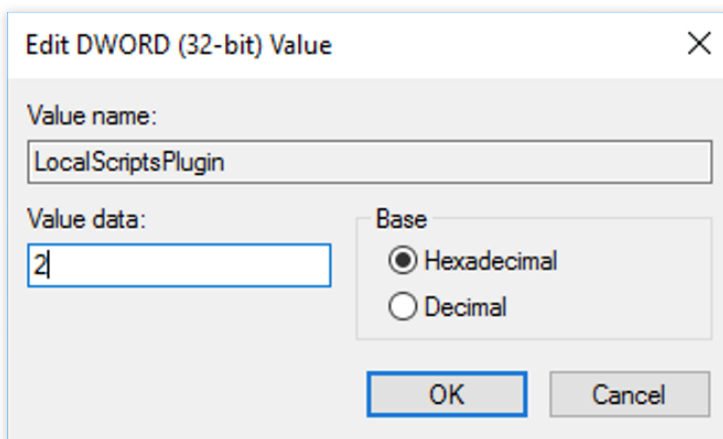
10. In the **Run** dialog box, enter **regedit** and press **Enter** to open the **Registry Editor window**.

11. In the **Registry Editor** window, in the registry navigation pane on the left, expand the directory of **HKEY\_LOCAL\_MACHINE > SOFTWARE > Cloudbase Solutions > Cloudbase-Init**.





12. Find and double-click all **LocalScriptsPlugin** registry keys under **ins-xxx**, and then check whether the value of LocalScriptsPlugin is 2. See the following figure:



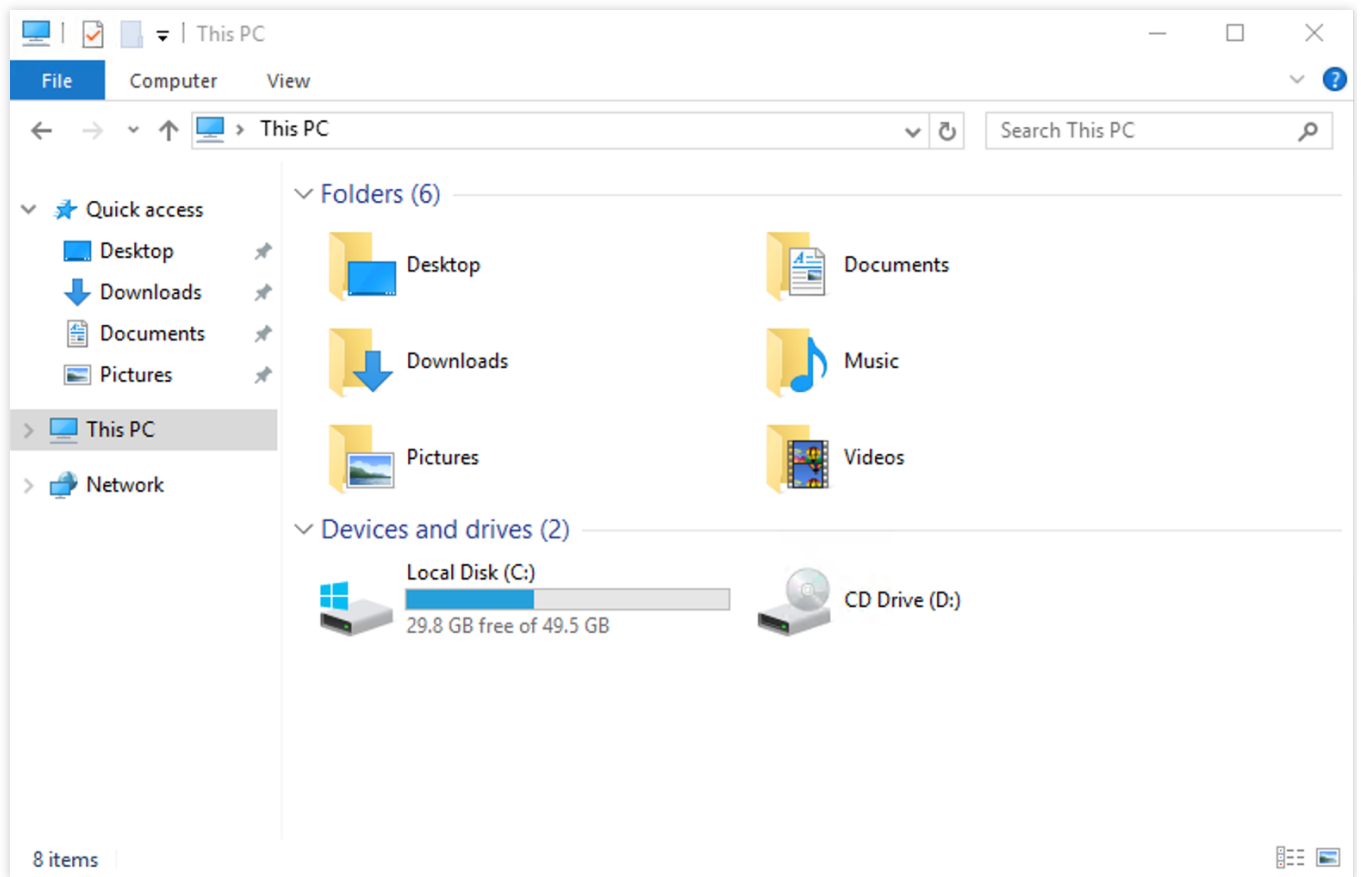
If yes, proceed to the next step.

If no, set the LocalScriptsPlugin value to 2.

13. In the operating system interface, click



, choose **This PC**, and check whether the CD drive is loaded in the device and drive. See the following figure:



If yes, [inspect the security software installed in Tencent Cloud Lighthouse](#).

If no, start the CD-ROM drive in Device Manager.

## Checking the Security Software Installed on Tencent Cloud Lighthouse

Use the installed security software to conduct a full scan, and check whether Tencent Cloud Lighthouse has vulnerabilities and whether the core components of `cloudbase-init` are blocked.

If Tencent Cloud Lighthouse has vulnerabilities, rectify them.

If core components are blocked, unblock them.

# Binding Key

Last updated : 2022-05-12 12:24:11

## Overview

This document describes how to bind the specified key to an instance on the instance details page in the Lighthouse console.

## Prerequisites

You can bind a key to only a Linux instance.

You have created and saved a key. For more information, see [Creating SSH key](#).

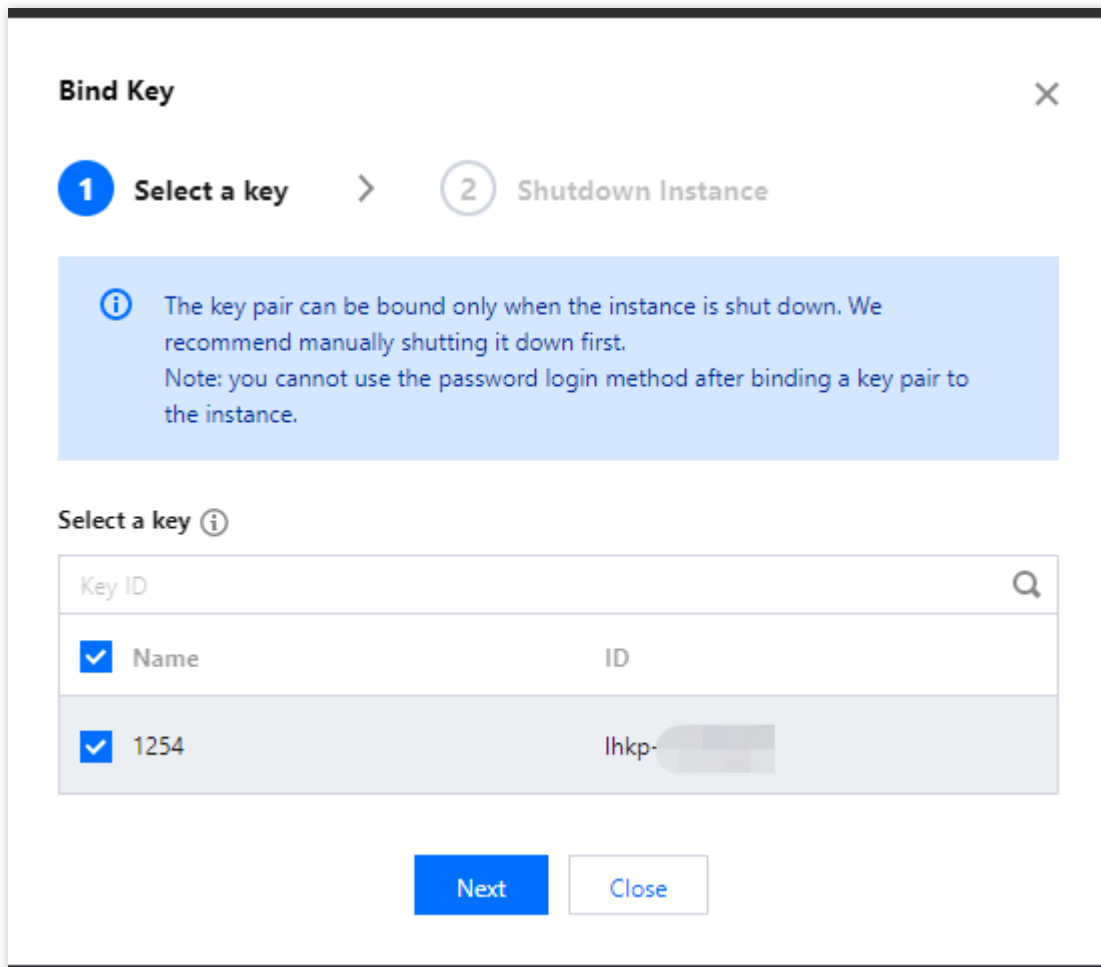
## Directions

1. Log in to the [Lighthouse console](#) and click the card of the target instance.
2. On the instance details page, select the **SSH key pair** tab and click **Bind Key Pair**.
3. In the **Bind key** pop-up window, perform the following operations based on the instance status:

Running instance

Shutdown instance

1. In the **Select a key** step, select the target key and click **Next** as shown below:



2. In the **Shutdown instance** step, select **Agree to a forced shutdown** and click **OK**.

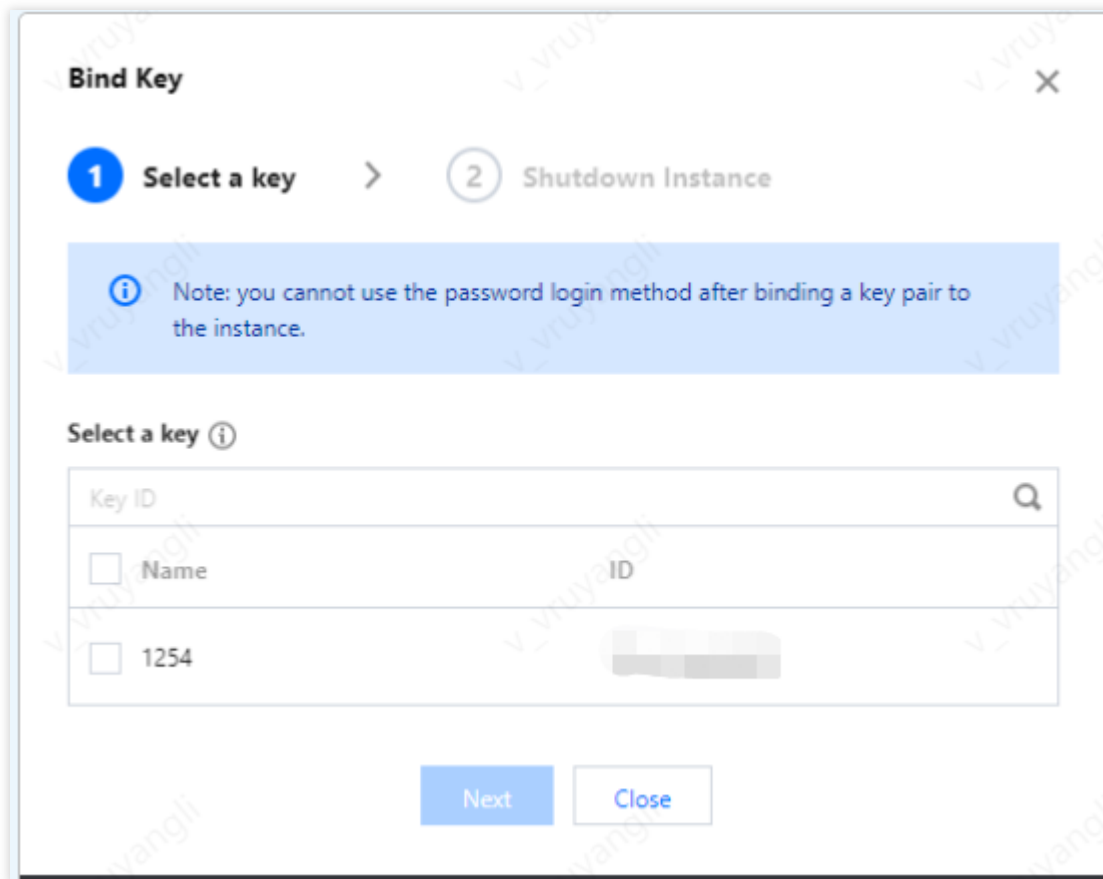
**Note:**

During the binding process, the instance will shut down first and then start up, and the business will be interrupted momentarily. We recommend you do so during off-peak hours.

If the instance fails to shut down normally, it will be forced to shut down. Forced shutdown may cause data losses or file system corruption. Therefore, perform forced shutdown with caution.

Forced shutdown may take a while. Please be patient.

1. In the **Select a key** step, select the target key and click **Next** as shown below:



2. In the **Shutdown instance** step, click **OK**.

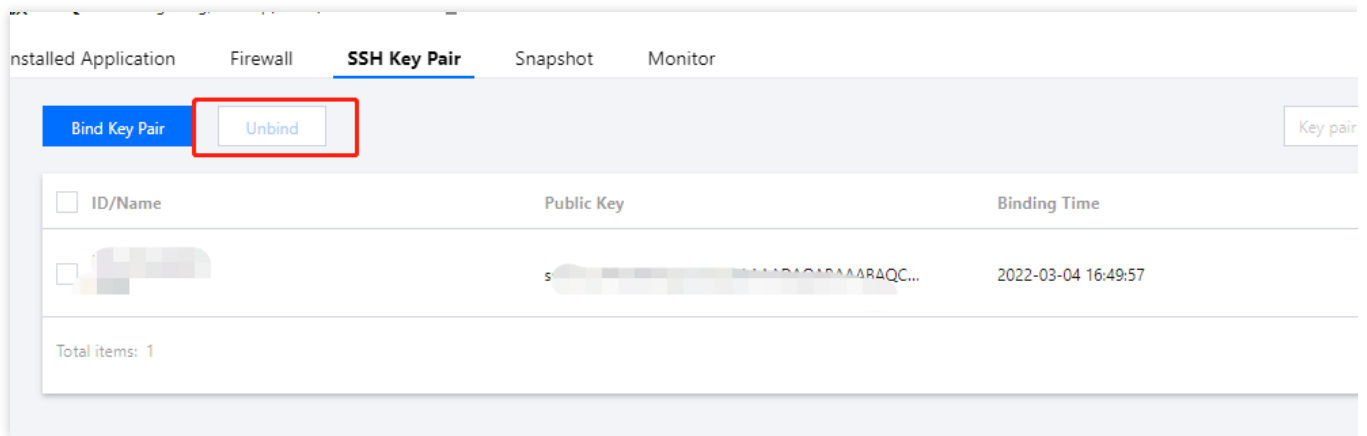
**Note:**

To improve the Lighthouse instance security, after a Linux instance is bound to a key, login to the `root` account with a password will be forbidden by default. If you want to keep the password login method, modify the configuration as instructed in [Modifying SSH configuration](#).

## Related Operations

### Unbinding key

1. Log in to the [Lighthouse console](#) and click the card of the target instance.
2. On the instance details page, select the **SSH key pair** tab.
3. Select the target key pair and click **Unbind** above the list as shown below:

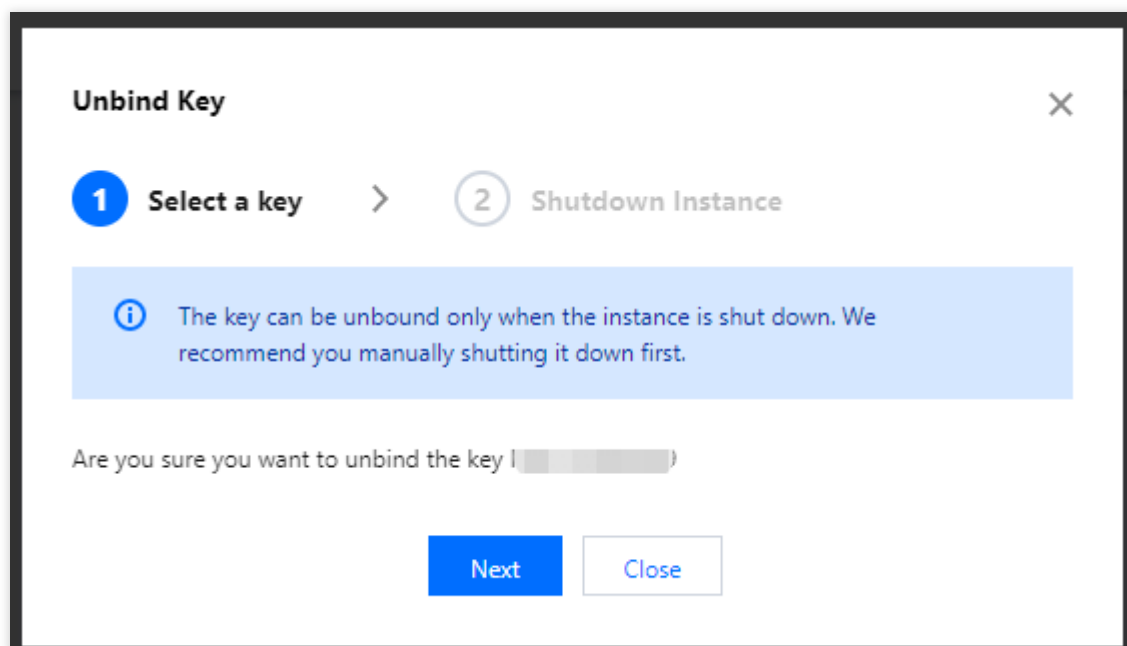


4. In the **Unbind key** pop-up window, perform the following operations based on the instance status:

Running instance

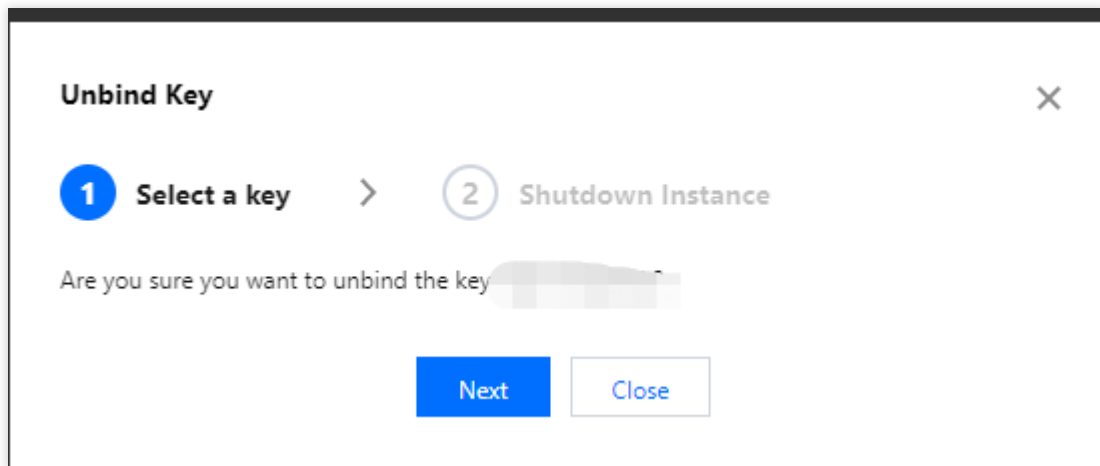
Shutdown instance

1. In the **Select a key** step, confirm the target key and click **Next** as shown below:



2. In the **Shutdown instance** step, click **OK**.

1. In the **Select a key** step, confirm the target key and click **Next** as shown below:



2. In the **Shutdown instance** step, click **OK**.

## References

[Managing Key](#)

[Logging in to Linux Instance via Remote Login Software](#)

[Logging in to Linux Instance via SSH Key](#)

# Viewing Instance Information

Last updated : 2022-06-16 19:07:35

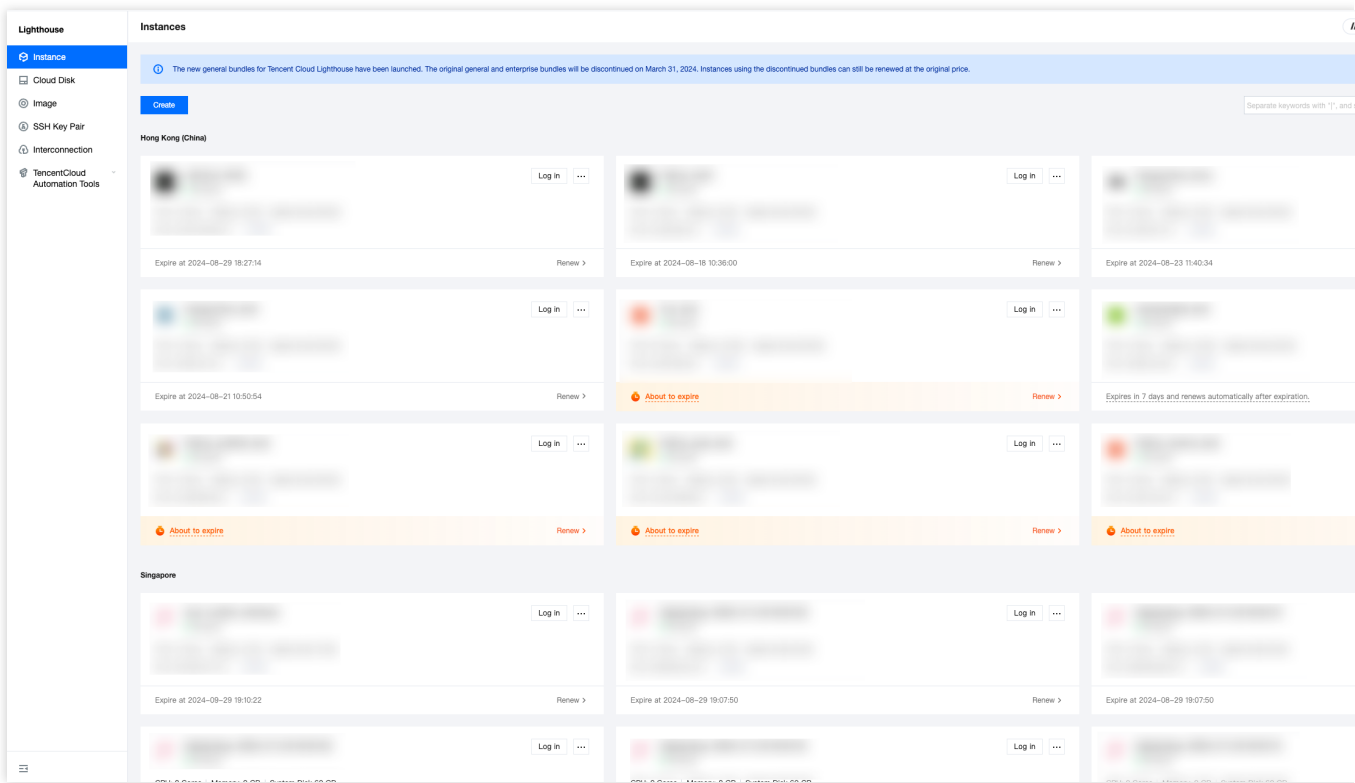
## Overview

After creating a Lighthouse instance, you can view its details in the console.

## Directions

### Viewing instance list information

Log in to the [Lighthouse console](#), and you can view instances in different regions and status on the instance list page as shown below:



### Viewing instance details

In the instance list, find the target instance and enter its details page to view its information.

View "overview" details

On this tab, you can view the basic, monitoring, network, image, application, image, and TencentCloud Automation Tools information of the instance as detailed below:

Information	Description
-------------	-------------



Category	
Instance information	<p>You can view the following basic instance information:</p> <p>Name/ID: The instance name can be modified.</p> <p>Region and availability zone: Instance region and AZ.</p> <p>Package type: Type of the package used by the instance.</p> <p>Instance specification: CPU and memory specification.</p> <p>System disk: Storage space of the system disk.</p> <p>Traffic package: Bandwidth and traffic package.</p> <p>Key pair: You can bind/unbind a Linux instance to/from a key.</p> <p>Tag: You can bind/unbind the instance to/from tags.</p>
Instance monitoring information	<p>You can view the following basic monitoring data of the instance:</p> <p>CPU utilization (%).</p> <p>Memory usage (MB).</p> <p>Public network (Mbps).</p> <p>System disk IO (KB/s).</p>
Remote login	You can select an instance login method as needed.
Resources	You can directly view the instance traffic package and system disk usage.
Network information	<p>You can view the following instance network information:</p> <p>IP: Public IP address (for instance access over the public network) and private IP address (for inter-instance communication).</p> <p>Firewall: You can configure instance firewall rules.</p> <p>DDoS attack protection: You can view and manage DDoS attack protection in the Anti-DDoS console.</p>
Image details	<p>You can view the following basic instance image information:</p> <p>Image name: Specific image name. You can reset the application or create a custom image.</p> <p>Image type: Specific image type.</p> <p>Operating system: Image operating system version.</p>
Application information	<p>You can view the instance application information:</p> <p>For an instance created by using an application image, you can view the pre-installed software information and manage applications on the application management page.</p>
Billing information	<p>You can view the following instance billing information and terminate the instance:</p> <p>Creation time: Instance creation time.</p> <p>Expiration time: Instance expiration time. To renew the instance, click Renew.</p> <p>Auto-renewal status: Whether auto-renewal is enabled for the instance. To set auto-renewal, click Enable.</p> <p>Upgrade package: You can click Upgrade package to upgrade the instance package.</p> <p>Terminate instance: You can select Terminate/Return to terminate the instance if you no longer need it.</p>

**TencentCloud  
Automation  
Tools**

You can view the TencentCloud Automation Tools status information and perform relevant operations on the **Run Commands** tab.

On this tab, you can perform operations including instance **shutdown, restart, password resetting, remote login, application resetting, and image creation.**

View "pre-installed application" details

On this tab, you can view the basic application information, such as the application name, version number, and instance status. You can also reset the application and shut down, restart, or log in to the instance.

In addition, the **Pre-installed Application** tab also displays the details of the pre-installed software in the application, such as configuration file directory, admin account and password, and application software installation path.

**Note:**

As custom images don't have a unified template and are created based on your own data, the instances created by using them don't have the **Pre-installed application** tab.

View "cloud disk" details

On this tab, you can view and manage instance data disks.

View "firewall" details

On this tab, you can view and manage instance firewall rules.

View "key pair" details

On this tab, you can view and manage key pairs bound to the instance.

View "snapshot" details

On this tab, you can view, manage, and create instance snapshots.

View "monitoring" details

On this tab, you can view instance CPU, memory, public network bandwidth, and disk usage monitoring data.

View "run commands" details

On this tab, you can view the command execution details of TencentCloud Automation Tools and create and run commands.

# Shutting down Instance

Last updated : 2022-05-12 12:24:11

## Overview

The instance can be shut down when you need to stop the service, or modify configurations that can be done only in the shutdown state. Shutting down an instance is like shutting down a local computer.

## Notes

You can shut down an instance by using system commands (such as the `shutdown` command on Windows and Linux) or in the Lighthouse console. We recommend you view the shutdown process in the console to check whether any problem occurs.

Once shut down, a Lighthouse instance will no longer provide service. Therefore, before the shutdown, make sure that the instance has stopped receiving service requests.

During the shutdown, the status of the instance will change from "Shutting down" to "Shutdown". If the shutdown process takes too long, there may be an exception.

After an instance is shut down, all disk data will be retained, but data in the memory will be lost.

Shutting down an instance does not change its physical attributes, so the instance public and private IPs will remain unchanged.

## Directions

### Note:

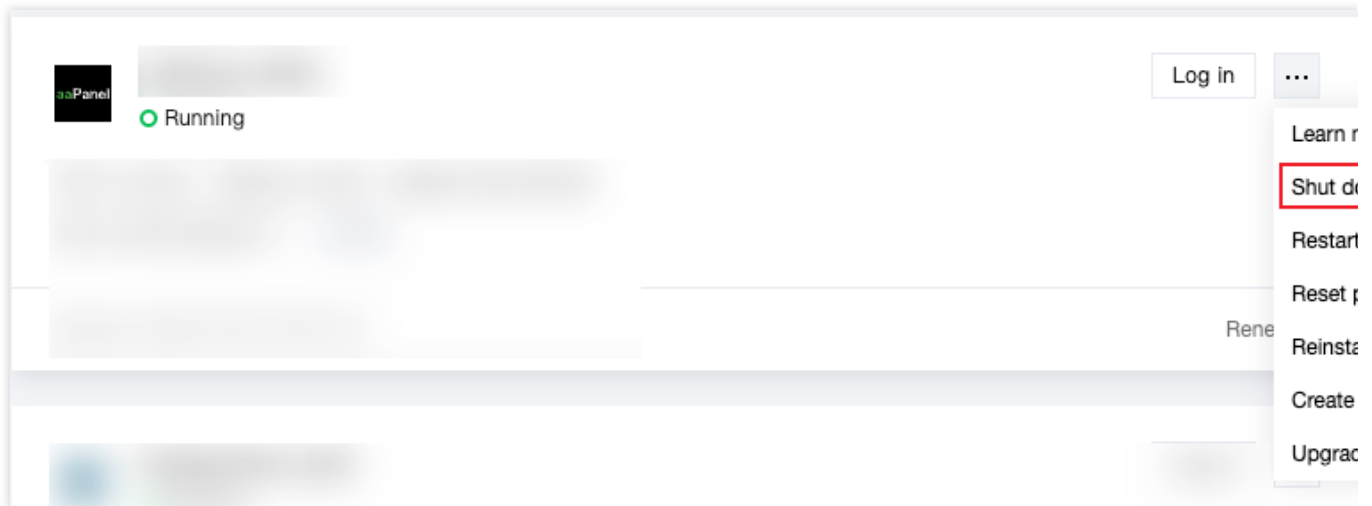
During instance shutdown, soft shutdown will be performed first by default. If the soft shutdown fails, forced (hard) shutdown will be performed automatically.

1. Log in to the [Lighthouse console](#).
2. Find the target instance in the instance list and select a shutdown method as desired.

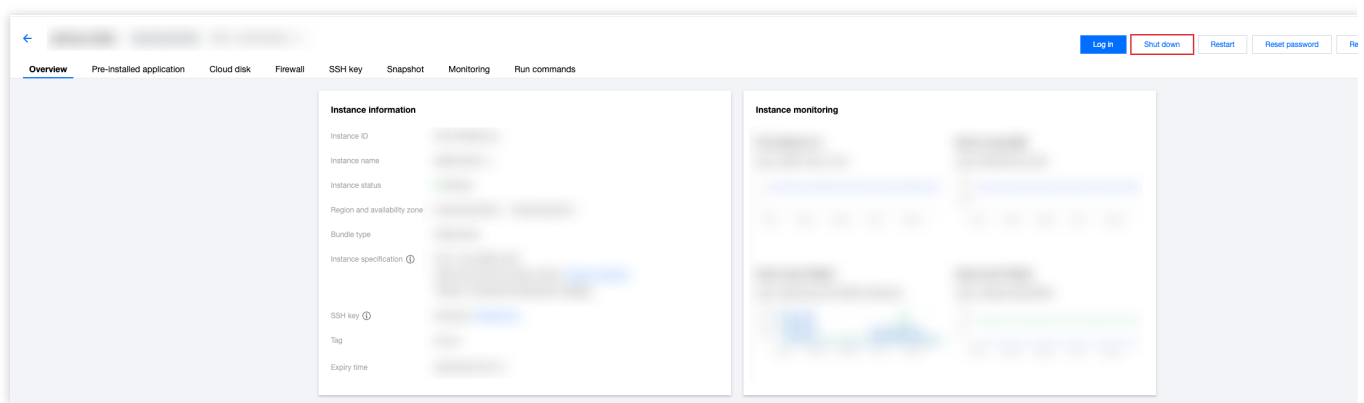
In the instance card in the instance list, click



> **Shut down** as shown below:



Enter the instance details page and click **Shut down** in the bottom-right corner on the page as shown below:



3. In the pop-up window, click **OK**.

For instances that cannot be shut down, the specific cause will be displayed on the page.

# Restarting Instance

Last updated : 2022-05-12 12:24:11

## Overview

Instance restart is a common maintenance method for Lighthouse and is similar to restarting the OS on a local computer.

## Notes

**Preparing to restart instances:** The Lighthouse instance cannot provide services during restart. Make sure before restarting the instance that it has stopped receiving service requests.

**How to restart instances:** We recommended you restart an instance by using the restart operations provided by Tencent Cloud instead of running the restart command in the instance (such as the relaunch command under Windows and the `Reboot` command under Linux).

**Restart time:** Generally, it takes just a few minutes from when the instance starts to execute the restart operation to when the operating system is completely started.

**Physical features of instances:** Restarting an instance does not change its physical features. Its public and private IP addresses as well as stored data will not be changed.

## Directions

### Note:

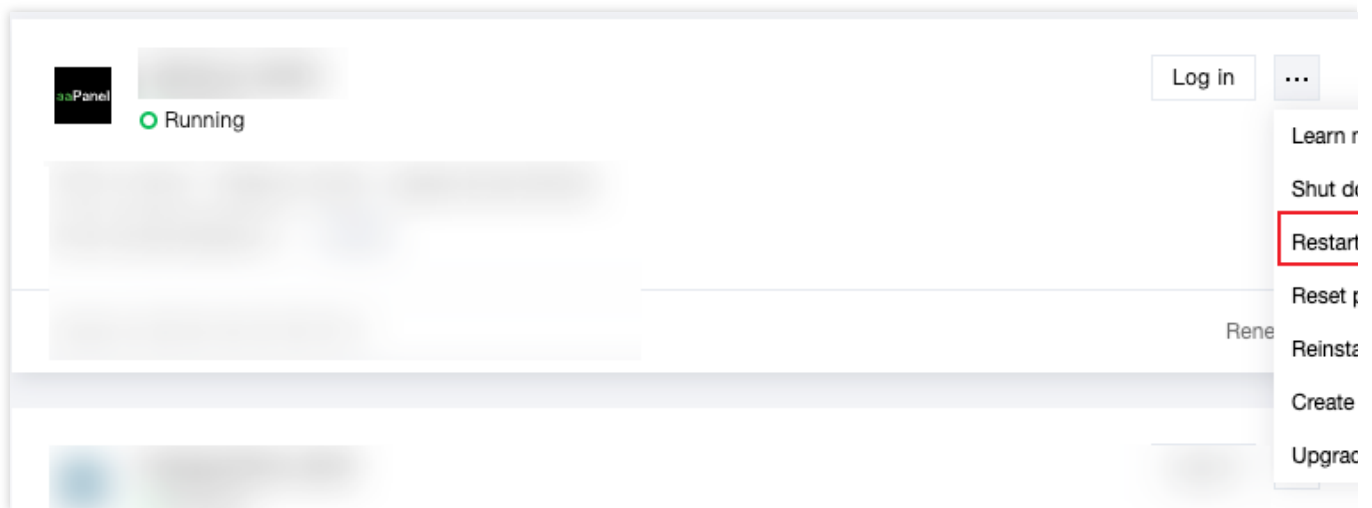
During instance restart, soft restart will be performed first by default. If soft restart fails, forced (hard) restart will be performed automatically.

1. Log in to the [Lighthouse console](#).
2. Find the target instance in the instance list and select a restart method as desired.

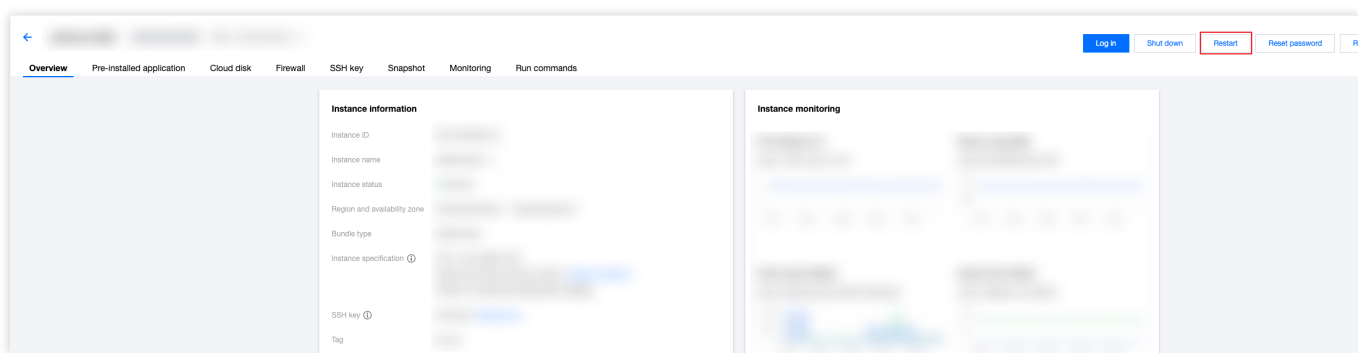
In the instance card in the instance list, click



> **Restart** as shown below:



Enter the instance details page and click **Restart** in the top-right corner on the page as shown below:



3. In the pop-up window, click **OK**.

# Terminating Instance

Last updated : 2022-05-12 12:24:11

## Overview

If you no longer need a Lighthouse instance, you can terminate it. Once its status becomes **Returned** or **To be repossessed**, it no longer incurs fees. For instances to be repossessed, you can renew (restore) or completely terminate them based on different scenarios and needs.

This document describes how to terminate Lighthouse instances in different status in the console.

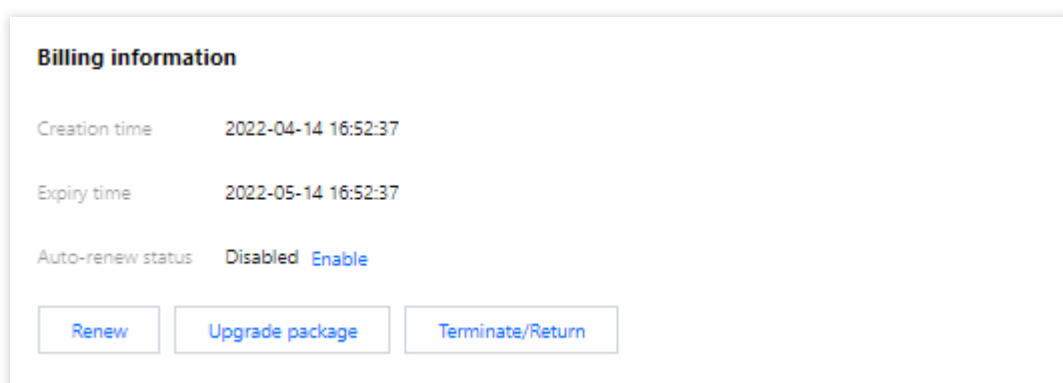
### Note:

Currently, Lighthouse supports the sensitive operation protection feature to effectively protect the security of account resources. It can be enabled in [security settings](#). Instance termination is a sensitive operation.

## Directions

### Terminating running/shutdown Lighthouse instances

1. Log in to the [Lighthouse console](#).
2. Find the target Lighthouse instance in the instance list and enter its details page.
3. In the **Billing information** section on the **Overview** tab on the instance details page, select **Terminate/Return** as shown below:



4. In the pop-up window, if the instance is mounted with data disks, you can select **Return data disks mounted to the instance** to terminate the data disks at the same time as shown below:

### Terminate/Return instance

You've selected 1 instance. [Collapse](#)

To be returned

Package configuration	Expiry time
CPU - 2-core MEM - 2 GB System disk: SSD cloud disks 50 GB Transfer - 2048 GB/month (Bandwidth 30M)	2022-05-14 16:52:37
▼ Data disk	
123455	2022-08-21 09:39:32

Confirm return

1. Returned instances will be retained for 7 days, during which, you can manually terminate them. Please back up data in advance.

2. For each Lighthouse service package, 5-day no-questions-asked refund can be applied to only one instance, and up to 30 instances can be returned for a refund per year. For more information, see [Refund Policy](#).

3. If you purchase at a discount price or with a voucher, then the discount and voucher amount is non-refundable.

Data disk ☒ Also return the data disks attached to the instance

Refund rules \* ☒ I have read and agree to [Refund Policy](#)

OKClose

5. Select **Read and agree to refund rules** and click **OK**.

6. Check and confirm the Lighthouse refund information and click **OK**. After the information is submitted, the system will refund and terminate the instance. Once terminated, the instance will enter the **To be repossessed** status.

**Note:**

If your instance is not renewed within seven (included) days after entering the **To be repossessed** status, the system will release it in around 24 hours. After release, all data on the instance will be cleared and cannot be recovered. Instances in **To be repossessed** status are unavailable, which indicates that they can neither be managed nor accessed.

If the Lighthouse instance to be terminated contains a renewal order that hasn't taken effect, the order will also be refunded after instance termination.

After a data disk is terminated, it will enter the **To be repossessed** status and be retained for seven days. If you confirm that you don't need to retain the data, you can completely terminate the cloud disk.

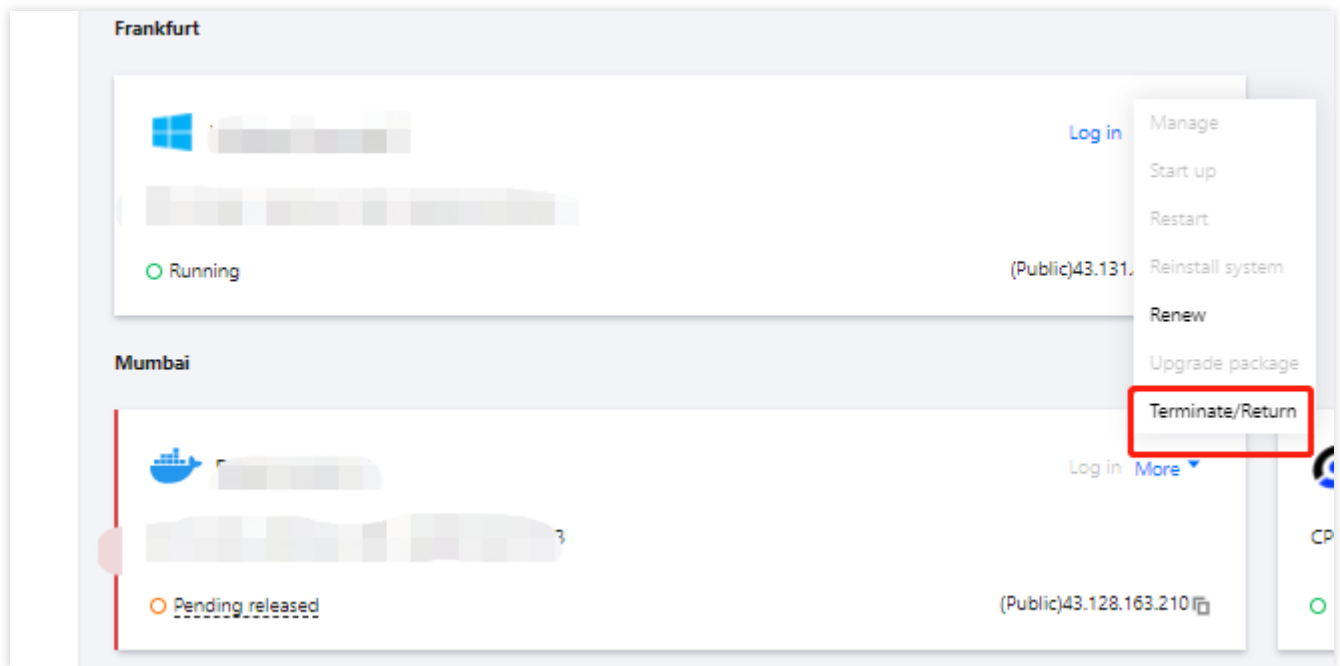


## Terminating to-be-reposessed Lighthouse instance

### Note:

This operation will terminate an instance completely from the account's instance list, and the instance cannot be restored through renewal or other methods. Therefore, proceed with caution.

1. Log in to the [Lighthouse console](#).
2. Find the target Lighthouse instance in **To be reposessed** status in the instance list and click **More >** **Terminate/Return** as shown below:



3. In the pop-up window, select **Read and agree** and click **OK** as shown below:

### Terminate/Return instance

You've selected 1 instance. [Collapse](#)

To be returned

Package configuration	Expiry time
CPU - 2-core MEM - 2 GB System disk: SSD cloud disks 30 GB Transfer - 1024 GB/month (Bandwidth 30M)	2022-05-08 09:35:34

Confirm return

1. The instance will be immediately eliminated from the instance list, which cannot be recovered.
2. The relevant cloud disks, snapshots, transfers, public IPs, firewall rules, and other associated resources will also be terminated.

Refund rules \*

☒ I have read and agree to

OK

Close

# Renewing Instance

Last updated : 2024-08-15 15:43:53

## Overview

This document describes how to renew a Lighthouse instance manually or set auto-renewal for it.

## Directions

### Manual Renewal

The following steps are recommended for you to renew an instance or batch renew multiple instances manually based on the instance status:

Renewing Running Instances

Renewing To-Be-Repossessed Instances

### Renewing one instance

1. Log in to the [Lighthouse console](#).
2. On the **Instances** page, enter the details page of the target instance.
3. Select **Renew** in the **Billing information** section. In the **Renew instance** pop-up window, select the renewal period in calendar month as shown below:

#### Note:

If cloud data disks are mounted to the instance, they will be renewed at the same time. You can also select **Align the data disk expiration time with that of the instance to xxxx** to align the instance's and cloud disk's expiration time.

### Renew instance

You've selected 1 instance. [Collapse](#)

To be renewed	Price										
<div><div>▼</div><table><thead><tr><th>Bundle configuration</th><th>Expiry time</th><th>New expiration t...</th><th>Discount</th><th>Price</th></tr></thead><tbody><tr><td></td><td></td><td></td><td></td><td></td></tr></tbody></table></div>	Bundle configuration	Expiry time	New expiration t...	Discount	Price						
Bundle configuration	Expiry time	New expiration t...	Discount	Price							

Instance renewal period

Associate Resource

It is recommended to renew the resources associated with the current instance at the same time to avoid service interruption due to resource expiration.

Discounted price

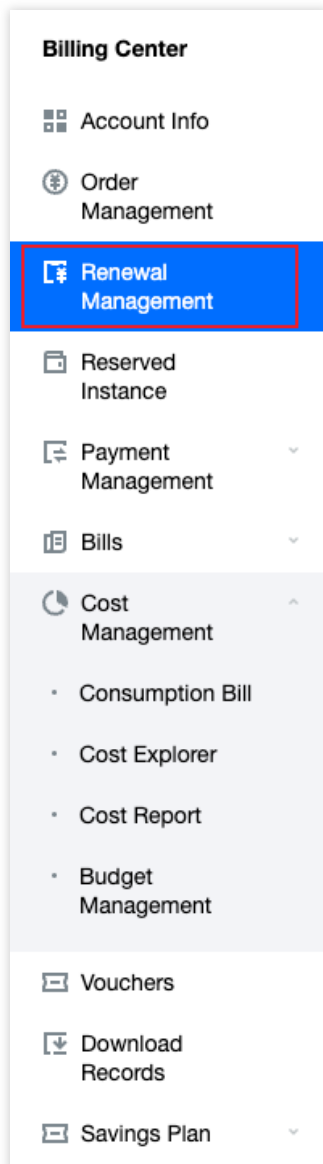
OK

Cancel

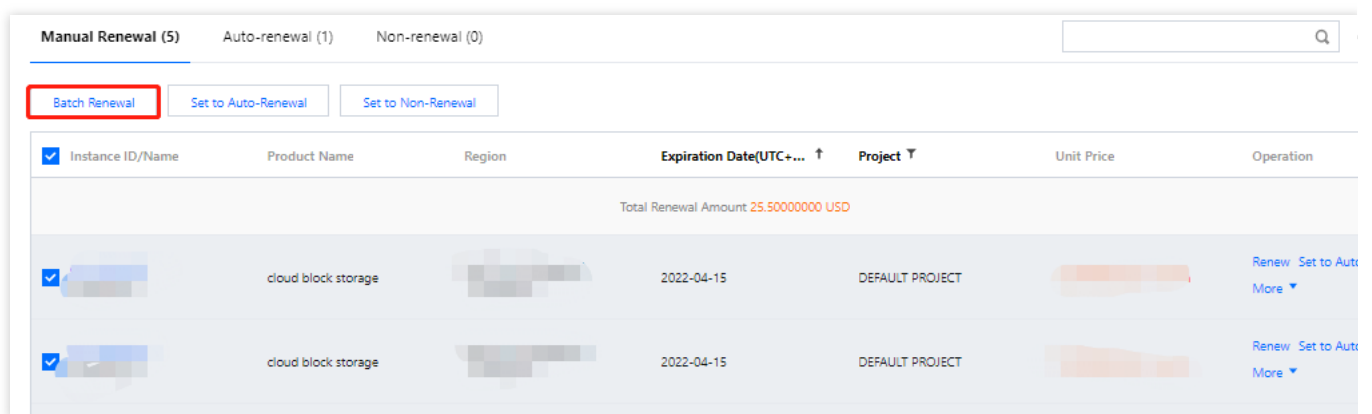
4. Click **OK** to enter the renewal order payment page, click **Submit order**, and make the payment as prompted.

### Batch renewing instances

1. Log in to the [Tencent Cloud console](#).
2. Click on **Billing Center** in the upper right corner to enter the Billing Center, then click on the **Renewal Management** tab in the left navigation bar.



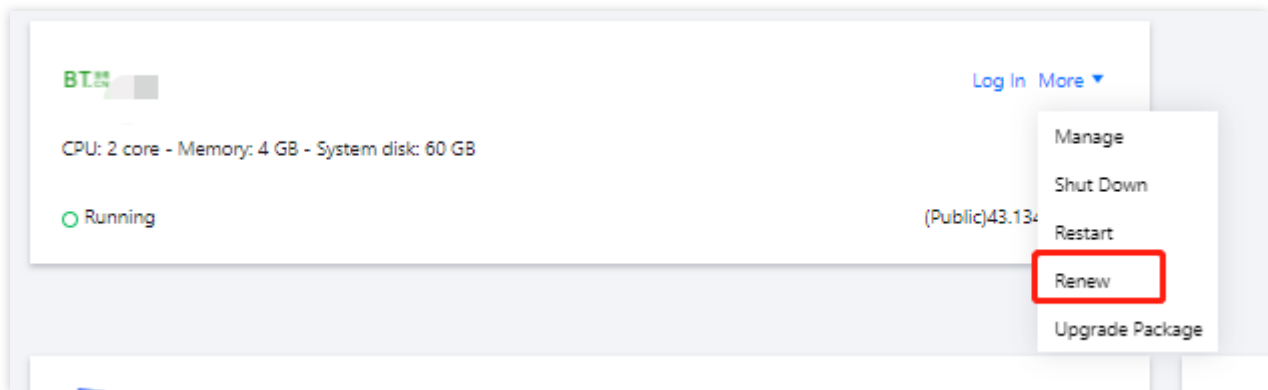
3. On the renewal management page, select the target instances and click **Batch renewal** above the list as shown below:



4. In the **Batch Renewal** pop-up window, select the renewal period, click **OK**, and make the payment for the renewal order.

### Renewing a Single Instance

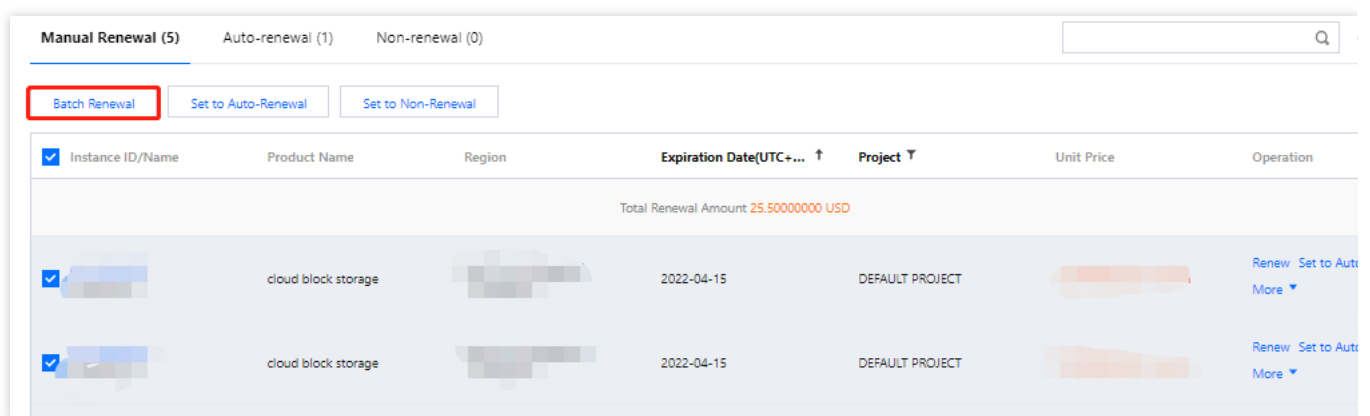
1. On the **Instances** page, find the target instance.
2. In the instance card found within the server list, select **Renew** at the bottom right corner, as illustrated below:



3. In the **Renew instance** pop-up window, select the renewal period and click **OK**.

### Renewing Instances in Batch

1. Log in to the [Tencent Cloud console](#).
2. Click **Fees** in the top-right corner. On the Fees Center page, click **Renewal Management** in the left navigation bar.
3. On the Renewal Management page, select the target instances and click **Batch Renewal** above the list as shown below:



4. In the **Batch Renewal** pop-up window, select the renewal period, click **OK**, and make the payment for the renewal order.

### Automatic Renewal

**Note:**

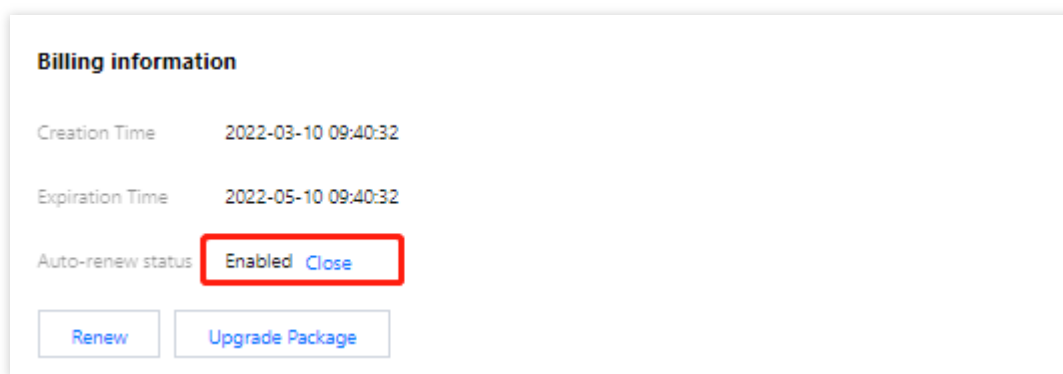
You can select **Auto-renew the device every month if my account has sufficient balance** during [instance purchase](#) to enable the auto-renewal feature. After successfully creating an instance, you can modify its auto-renewal settings in the following steps:

Choose the appropriate operation method based on your actual needs:

Setting Auto-renewal for a Single Instance

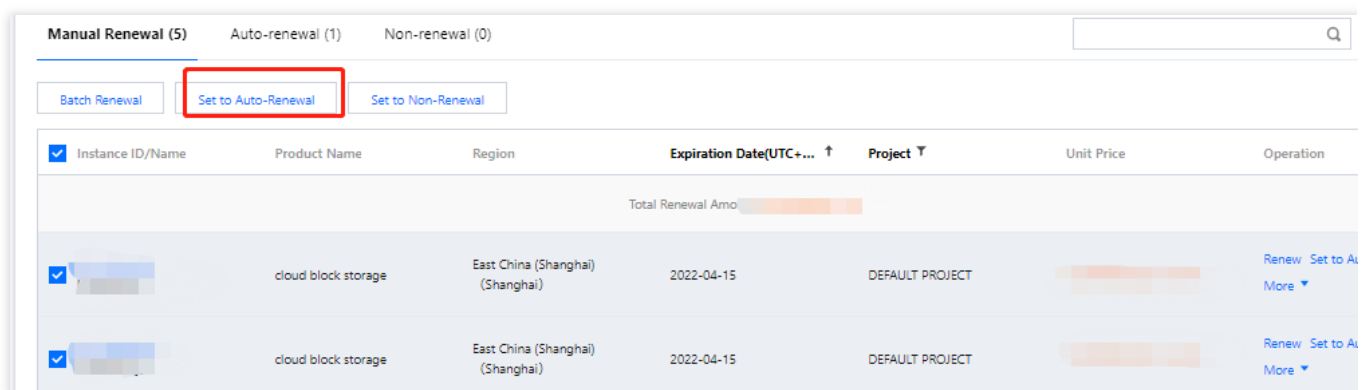
Setting Auto-renewal for Multiple Instances

1. Log in to the [Lighthouse console](#).
2. In the instance list, select the target instance to enter its details page.
3. In the **Billing information** section, you can **enable** or **disable** the instance auto-renewal feature as shown below:



4. In the **Enable/Disable auto-renewal** pop-up window, click **OK**.

1. Log in to the [Tencent Cloud console](#).
2. Click **Fees** in the top-right corner and click **Renew** in the drop-down list box.
3. On the renewal management page, select the target instances and click **Set to Auto-Renewal** above the list as shown below:



4. In the **Set to Auto-Renewal** pop-up window, click **OK**.

**Note:**

After auto-renewal is enabled, the instance will be automatically renewed on the expiration date. Make sure that your account balance is sufficient on the resource expiration date.

If your instance expires today, manually renew it.

If you manually renew an instance before the expiration date, Tencent Cloud will automatically renew it on the latest expiration date.

You can set auto-renewal, renew to a certain time, and perform other operations on the [renewal management page in the console](#).



# Reinstalling System

Last updated : 2022-05-12 12:24:12

## Overview

OS reinstallation is to reinstall the OS (and pre-installed applications) of a Lighthouse instance to restore it to the initial status or install a new system. This is a common way to recover the instance in the event of a system failure.

### Note:

Currently, Lighthouse supports the sensitive operation protection feature to effectively protect the security of account resources. It can be enabled in [security settings](#). OS reinstallation is a sensitive operation.

## Notes

### Cross-OS reinstallation:

Currently, only instances in the Chinese mainland support cross-OS reinstallation, for example, from Linux to Windows or vice versa. A Linux instance system disk must be at least 40 GB in size as required by the Windows Server image; otherwise, cross-platform reinstallation will fail.

Instances outside the Chinese mainland only support same-OS reinstallation.

**Data backup:** After OS reinstallation, the system disk will be cleared and reset to the initial status of a new image. Therefore, you need to back up important data in it before reinstallation.

**Instance IP:** After OS reinstallation, the instance public IP will remain unchanged.

**Forced shutdown:** During OS reinstallation, the instance will be automatically shut down (soft shutdown will be performed first by default, and forced (hard) shutdown will be performed if soft shutdown fails).

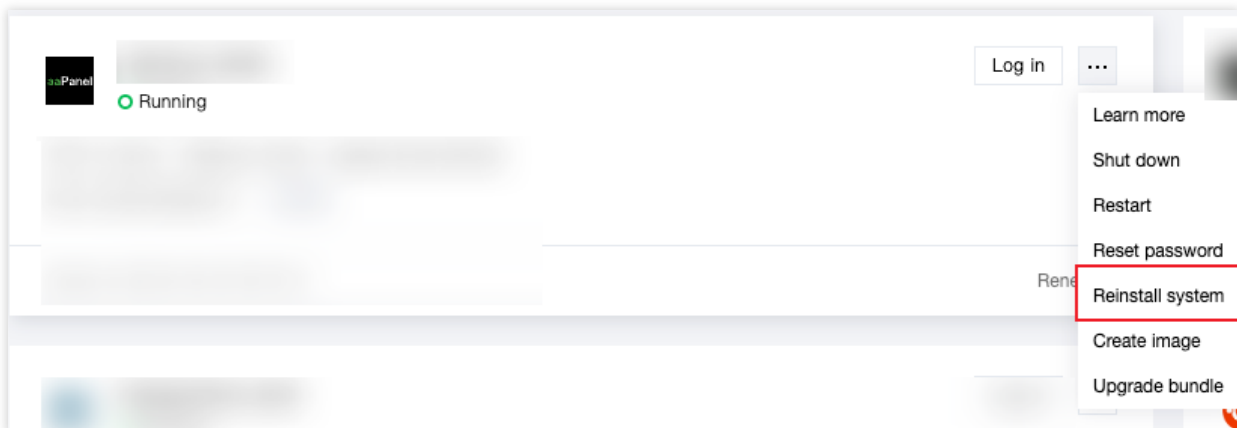
## Directions

1. Log in to the [Lighthouse console](#).
2. Find the target instance in the instance list and select a reinstallation method as desired.

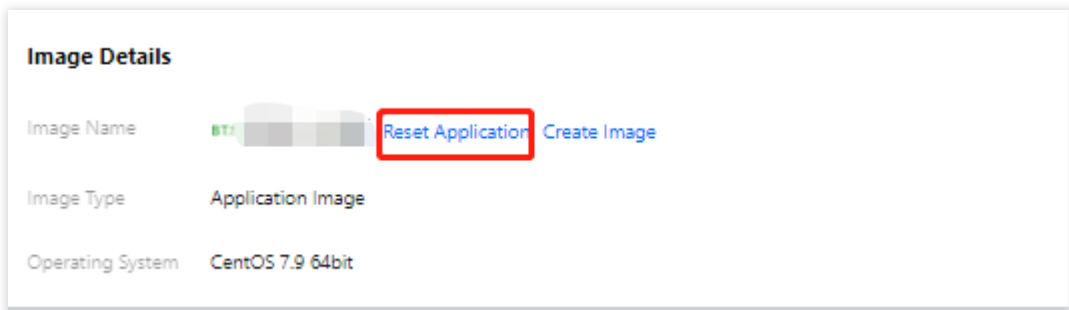
In the instance card, select



> **Reinstall system** as shown below:



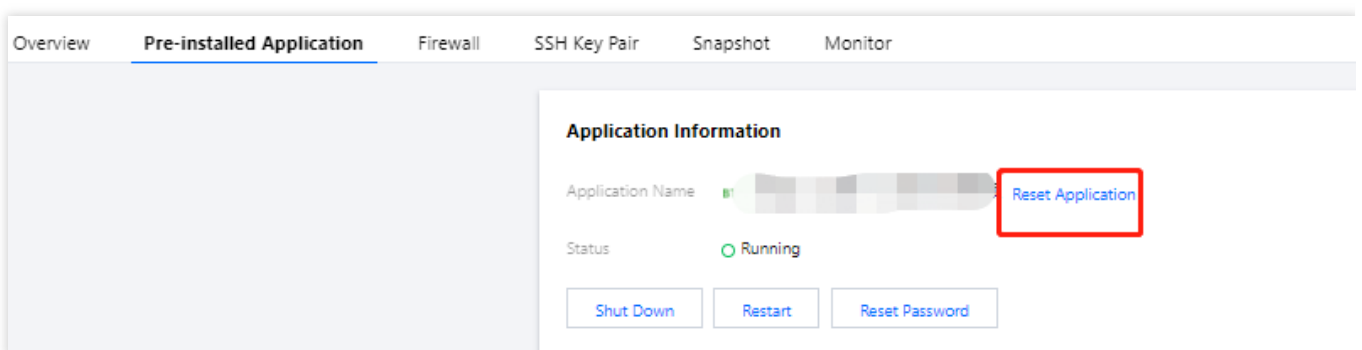
Click the instance card to enter the instance details page. On the **Overview** tab, click **Reset Application** in **Image details** as shown below:




Click the instance card to enter the instance details page. On the **Pre-installed Application** tab, click **Reset Application** in **Application information** as shown below:

**Note:**


If the Lighthouse instance doesn't use an application image, you cannot reinstall the OS in this way.




3. On the **Reset Application** page, select the target image (you can select a system, application, basic Docker, custom, or shared image), read the reinstallation notes, select **I have read and understand the above notes.**, and click **OK** as shown below:

**Application template**  
Create an application by using a...


- ✓ Out-of-box service
- ✓ For users who need to set up...


**OS image**  
Only the OS is pre-installed. You need...


- ✓ Custom configuration
- ✓ For users with sufficient related...


**Custom image**  
Build up applications with custom...


- ✓ Create applications with the existi...
- ✓ Duplicate and migrate applications


**OpenCloudOS**


**CentOS**

**CentOS Stream**

**Ubuntu**

**Debian**

**Windows Server**

OpenCloudOS 8

**OpenCloudOS 8**

OpenCloudOS inherits Tencent's more than 10 years of technical accumulation in operating systems and kernel level, with solid support in cloud-native, stability, performance, and hardware support. OpenCloudOS 8's basic library-level components are fully compatible with CentOS 8. After being verified by more than 10 million nodes on a large scale, its stability has increased by 70%, and the performance in specific scenarios has increased by 50%, providing a better solution compared to CentOS 8.

**Login credential** ⓘ

Custom password

SSH key

Configure after reinstallation

Username

root

Password

\*\*\*\*\*

Note: Your password satisfies the policy. However, we still suggest you set a stronger password with at least 12 characters of the following 4 character sets: [a-z], [A-Z], [0-9], and [!@#\$%^&\*~+=\_{}|;':<>., with at least 2 different characters of each set.

Confirm password

Enter the login password

**Notes** If you forget the password, please reset it in the Lighthouse console.

ⓘ Reminders

1. The instance will be shut down forcibly during the re-installation.
2. Note that after the re-installation, all data in the system disk will be cleared and cannot be recovered.
3. Previous keys will be unbound after the re-installation. You need to bind it again later the re-installation.
4. The re-installation does not affect data in the data disks. But you need to initialize the data disks again.

☐ I have read and understand the above notes.

Read and select first

OK

Cancel

# Upgrading Instance Package

Last updated : 2022-05-12 12:24:12

## Overview

Tencent Cloud Lighthouse Application Server can quickly and easily adjust instance configurations by upgrading existing packages, which shows its flexibility. This article introduces the operation method and precautions for upgrading the package.

## Notes

Lighthouse Application Server instance is only supported in upgrading packages, not in downgrading, which means the selected package's CPU, MEM, SSD system disk, bandwidth/peak bandwidth and monthly traffic should all be larger than the current package.

When upgrading your package, you cannot specify the CPU model of the underlying physical server; Instead, Tencent Cloud will randomly assign a physical CPU model that meets the selected package specification.

Upgrading package across availability zones are not supported.

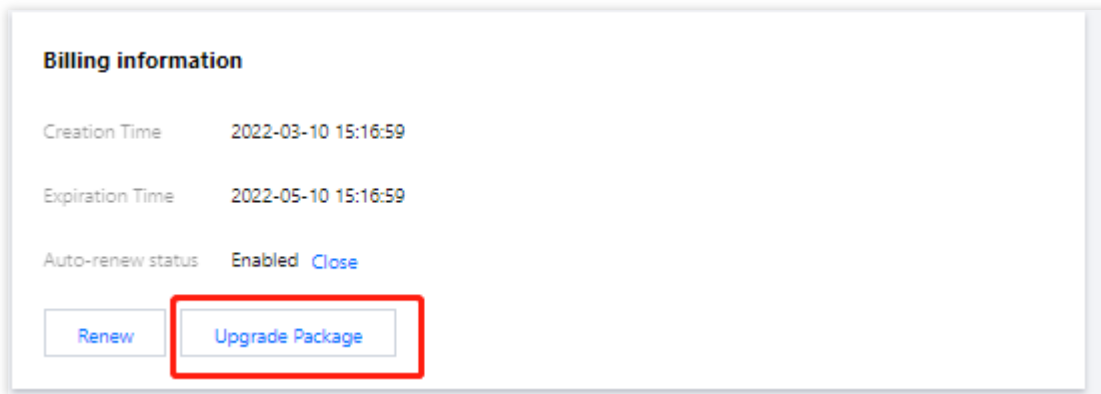
We support fixed bandwidth package (which has been taken offline, configured with 1 core, 1GB MEM, 20GB SSD system disk, 1Mbps bandwidth) to upgrade to traffic package.

Only when the selected package's CPU, MEM, SSD system disk, bandwidth/peak bandwidth and monthly traffic are all larger than the current package should cross-type upgrade package be available. That is, there is no package type restriction when the instance is upgraded to a package. For example, general package could be upgraded to storage package.

For directions and precautions on instance package upgrade, please refer to [Fees for Instance Package Upgrade](#).

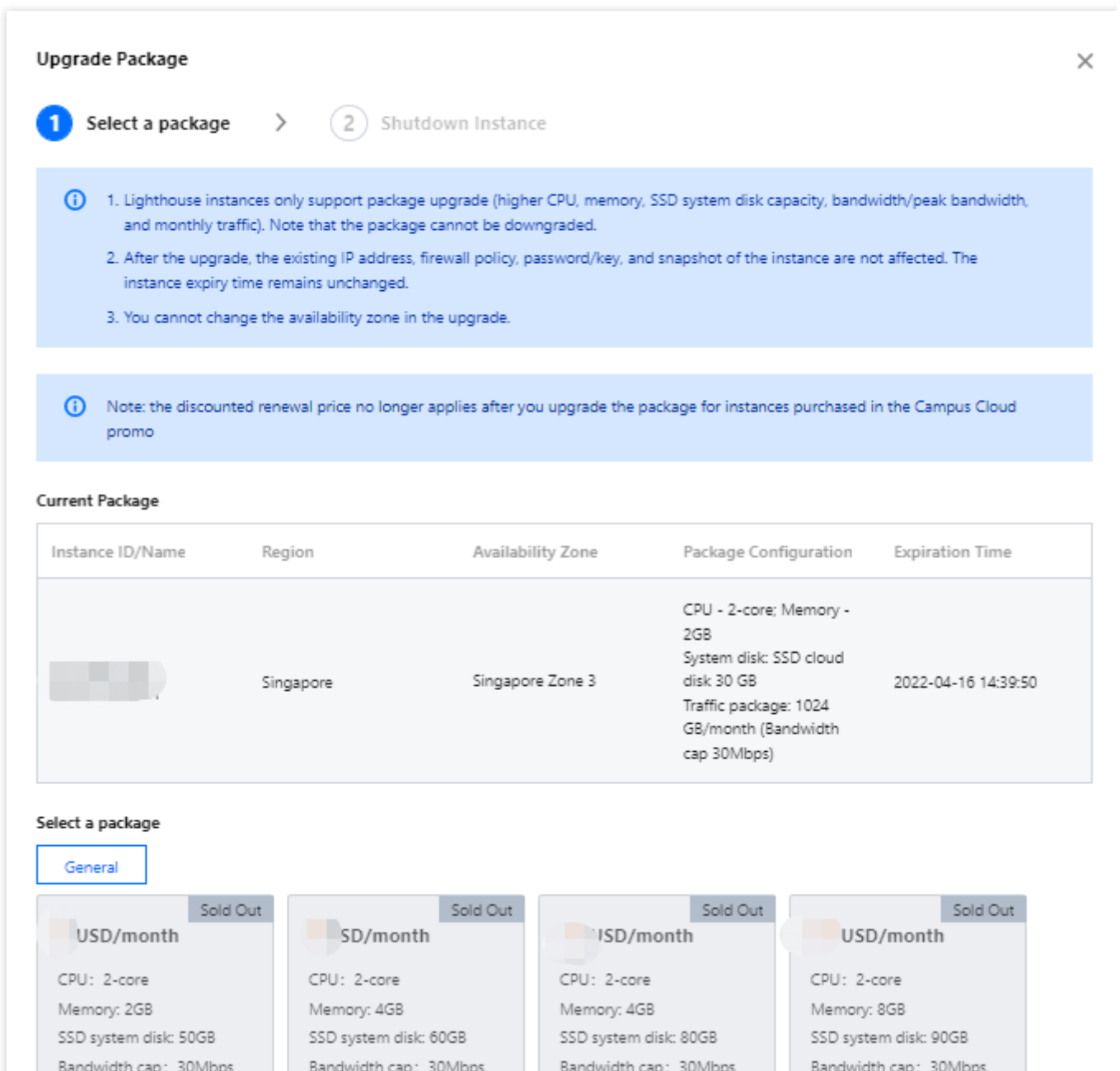
## Directions

1. Log in to the [Lighthouse console](#).
2. In the instance list, find and enter the details page of the instance for which to upgrade the package.
3. Select **Upgrade Package** in "Fee Information". As shown below:



4. In the "Upgrade Package" pop-up window, choose the selected package.

5. Read and tick "Instance Upgrade Descriptions" and click on **Next step: Shutdown tips**. As shown below:



Monthly traffic: 2048GB    Monthly traffic: 2560GB    Monthly traffic: 3072GB    Monthly traffic: 3584GB

**Sold Out**

**USD/month**

CPU: 2-core  
Memory: 8GB  
SSD system disk: 100GB  
Bandwidth cap: 30Mbps  
Monthly traffic: 4096GB

☒ Read and Agree [Fees for Instance Package Upgrade](#)

Next: Shut Down Instance    Close

6. In the "Shutdown tips" step, tick "Agree to force shutdown" and then click on **Start upgrade**.

**Note:**

Operating instance in shutdown status is supported. If you need to operate the instance in the power-on status, you need to confirm a forced shutdown, and it will take effect after restarting.

After upgrading, the current IP address, firewall policy, password/key settings will not be affected.

If the upgrade operation involves the expansion of the system disk of the instance, there is no need to manually expand the partition and file system operation after the package is successfully upgraded, and the original data will not be affected.

The current used traffic of the instance will not change, and the monthly traffic pack limit will be adjusted to the traffic pack limit of the upgraded package.

If the instance is upgraded from a fixed bandwidth to a traffic package, it will obtain a full traffic package limit and start calculating used traffic immediately after successful operation.

It usually takes 1-5 minutes for instance to finish upgrade. When it is done successfully, you can check the information about the package in the instance details page.

# Managing Instance Tag

Last updated : 2022-05-12 12:24:12

## Overview

**Tags** are key-value pairs provided by Tencent Cloud for easy resource identification. You can use tags to categorize and manage your Lighthouse resources.

This document describes how to manage instance tags in the Lighthouse console.

## Usage Limits

There are certain limits on the tag quantity and naming rules. For more information, see [Usage Limits](#).

## Directions

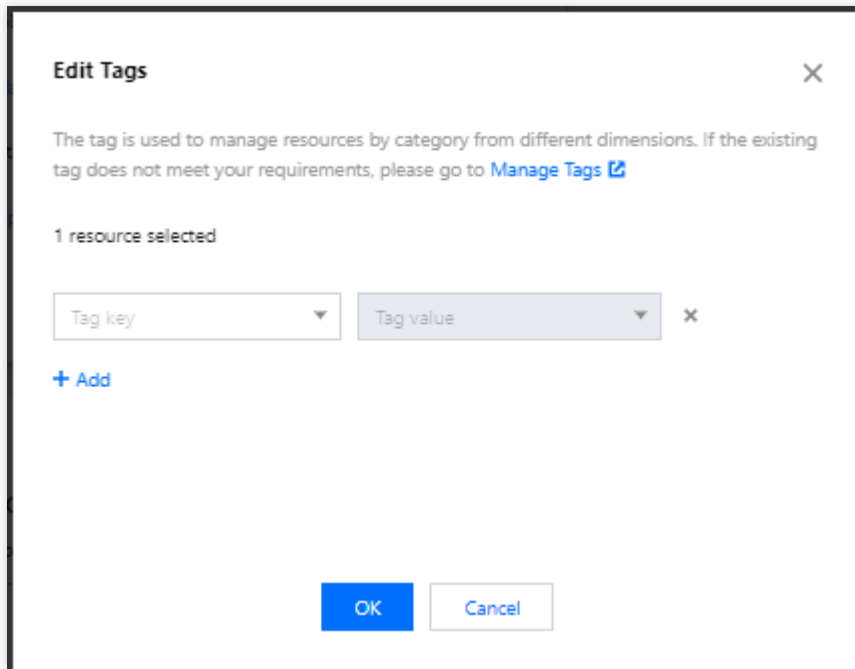
### Setting instance tag

1. Log in to the [Lighthouse console](#) and select an instance.
2. In **Instance information** on the overview tab, click



after **Tag**.

3. In the **Edit tag** pop-up window, select target instance tags as shown below:



4. Click **OK**.

5. After a message indicating that the edit was successful is prompted, click **OK**.

## Removing instance tag

1. In **Instance information**, click



after **Tag**.

2. In the **Edit tag** pop-up window, click



after the target tag as shown below:



**Edit Tags** ✕

The tag is used to manage resources by category from different dimensions. If the existing tag does not meet your requirements, please go to [Manage Tags](#) 🔗

1 resource selected

tets	qw	✕
Tag key	Tag value	✕

[+ Add](#)

**OK** Cancel

3. Click **OK**.

4. After a message indicating that the edit was successful is prompted, click **OK**.

## References

[Creating Tags](#)

[Querying Resources by Tag](#)

# Changing Instance Public IP

Last updated : 2022-09-26 11:28:02

## Overview

This document describes how to change the instance public IP in the Lighthouse console.

## Usage Limits

The public IP can be changed only once for each instance throughout its entire lifecycle.

You can change instance public IPs only three times per day in each region, and this quota is shared with other Tencent Cloud products using public IPs.

For example, if you have changed the public IP of three CVM instances in the one region under your account, you cannot change the public IP of any Lighthouse instance on the same day.

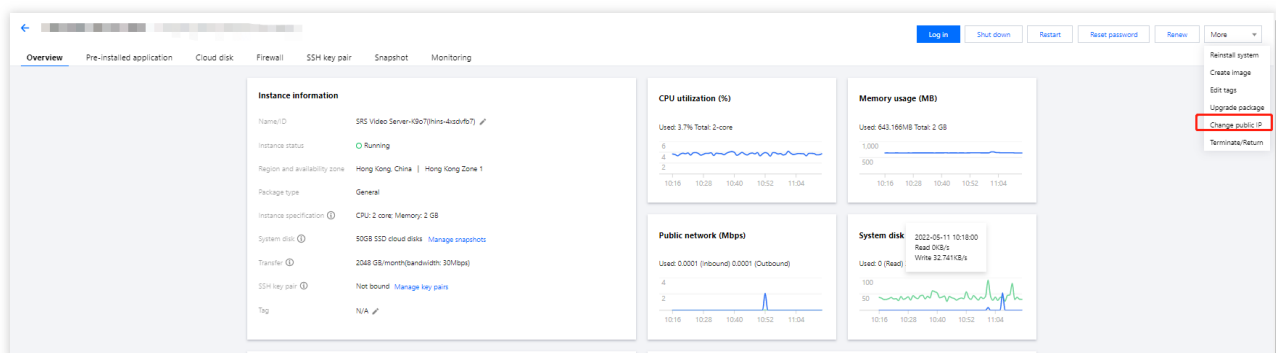
If an instance IP is blocked due to DDoS attacks and in the **Security Isolated** status, you need to wait 2–24 hours until it is unblocked before changing it.

The public IP cannot be changed when the instance status is Frozen, Blocked, or Pending released.

After the change, the previous public IP is released and cannot be restored.

## Directions

1. Log in to the [Lighthouse console](#) and select the target instance.
2. On the instance details page, select **More > Change public IP**.



3. In the **Change public IP** pop-up window, click **OK**.

# Batch Operations

Last updated : 2022-06-16 19:07:35

## Overview

This document describes how to perform batch operations on Lighthouse instances in the same region, such as starting and shutting down instances and resetting passwords.

## Notes

For a batch operation, all instances must be in the same region.

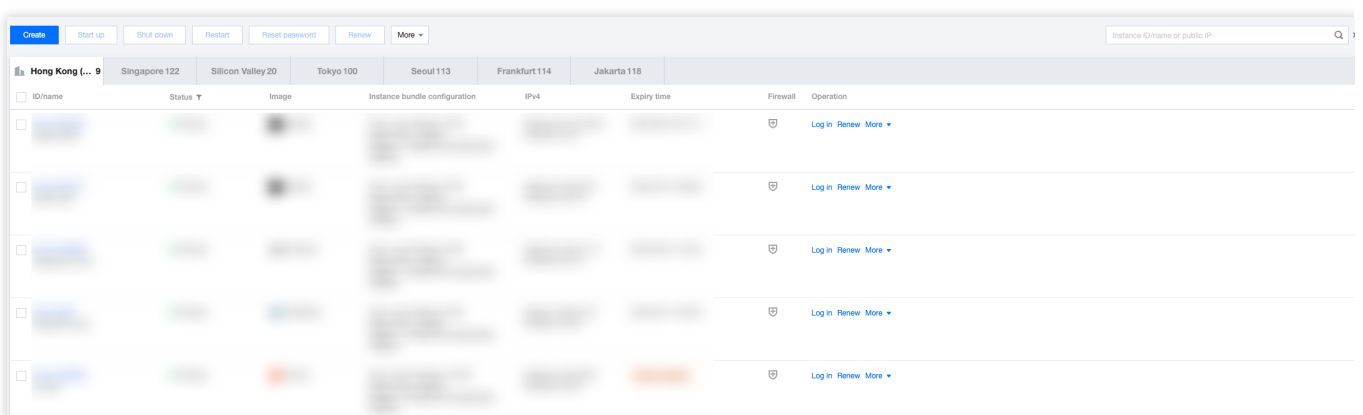
All selected instances must support the operation.

For example, Windows instances don't support SSH keys, so you cannot batch bind SSH keys when Windows and Linux instances are selected at the same time.

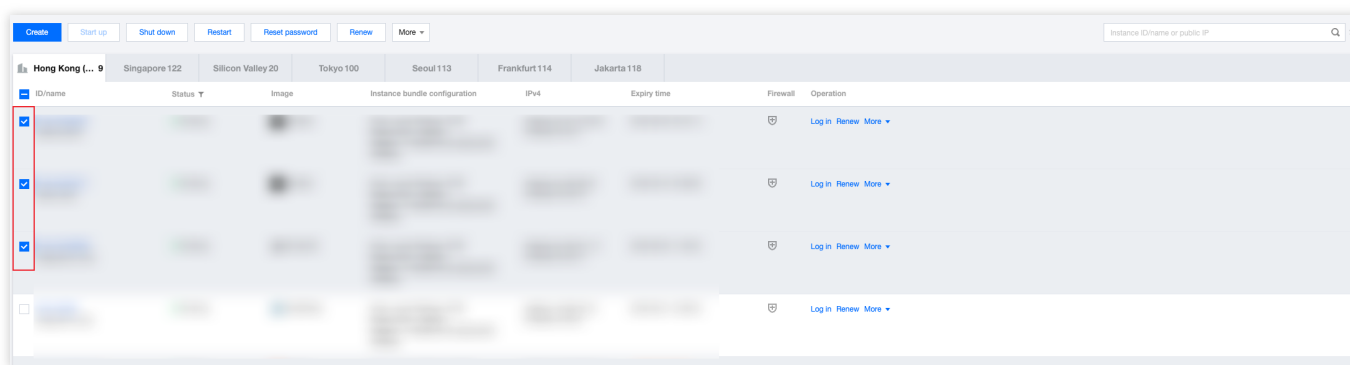
## Directions

This document describes how to batch shut down instances.

1. Log in to the [Lighthouse console](#) and switch to **List** view.



2. Check the instances to be operated under a certain region.



3. Select **Shut down** at the top of the page

4. In the **Shut down** pop-up window, click **OK**.

# Working with Cloud Disks

## Creating Cloud Disks

Last updated : 2022-05-13 16:43:39

### Overview

You can create a cloud disk and attach it to any Lighthouse instances in the same availability zone to use as a data disk. This document describes how to create a cloud disk in the Tencent Cloud Lighthouse console.

#### Note:

The [CBS cloud disks](#) used on Lighthouse instances are with the same performance as the ones used on CVM instances.

### Considerations

Cloud disks can be attached only to the instances in the same availability zone (AZ). Cross-AZ attaching is not supported, and the AZ of cloud disks cannot be changed.

Each region has a quota of 20 cloud disks.

### Directions

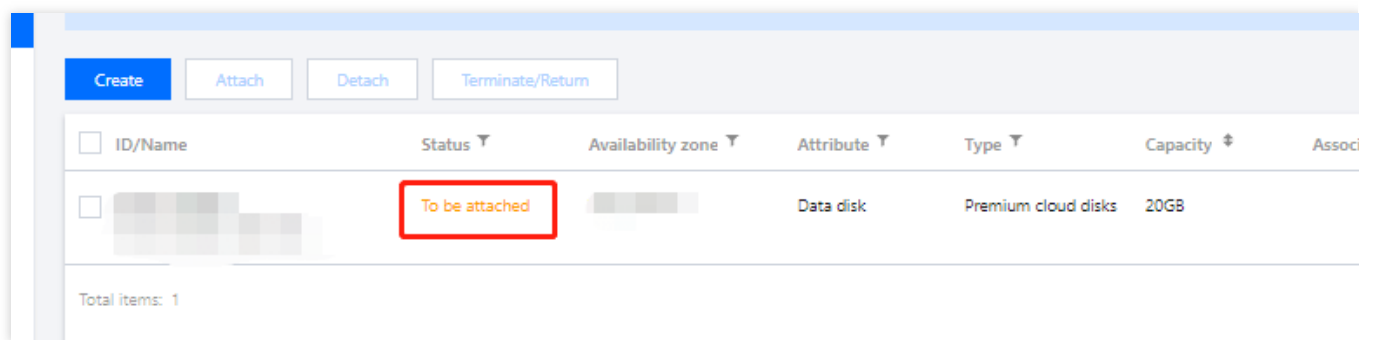
1. Log in to the Lighthouse console and click [Cloud Disk](#) on the left sidebar.
2. On the top of the **Cloud Disk** page, select a region, and click **Create**.
3. Configure the following parameters in the pop-up window:

Parameter Name	Description
Availability zone	The availability zone where the cloud disk is located. <b>Cross-AZ attaching is not supported, and the AZ of the cloud disk cannot be changed.</b>
Cloud disk type	Supports premium and SSD cloud disks. For more information, see <a href="#">Cloud Disk Types</a> .
Capacity	Cloud disk capacity. The adjustment increment is 10 GB. The specifications are as follows: Premium cloud disks: 10 - 1000 GB SSD cloud disks: 20 - 1000 GB

Disk name	Optional. The name can contain up to 60 characters. When it's left empty, the cloud disk ID is used by default.
Purchase quantity	It defaults to <b>1</b> . Up to 10 cloud disks can be created in a batch.
Purchase period	Valid range: 1 month (default) - 5 years.
Auto-renewal	When it's enabled, the cloud disk is automatically renewed on a monthly basis upon its expiration when your account has sufficient balance.

#### 4. Click **OK**.

You can view the created cloud disks on the [Cloud Disk](#) page. New cloud disks are "to be attached".



## See Also

[Attaching a Cloud Disk](#)

# Attaching Cloud Disks

Last updated : 2022-05-13 16:43:39

## Overview

This document describes how to attach a cloud disk to any Lighthouse instances in the same availability zone in the console.

### Note:

Up to 5 data disks can be attached to one Lighthouse instance.

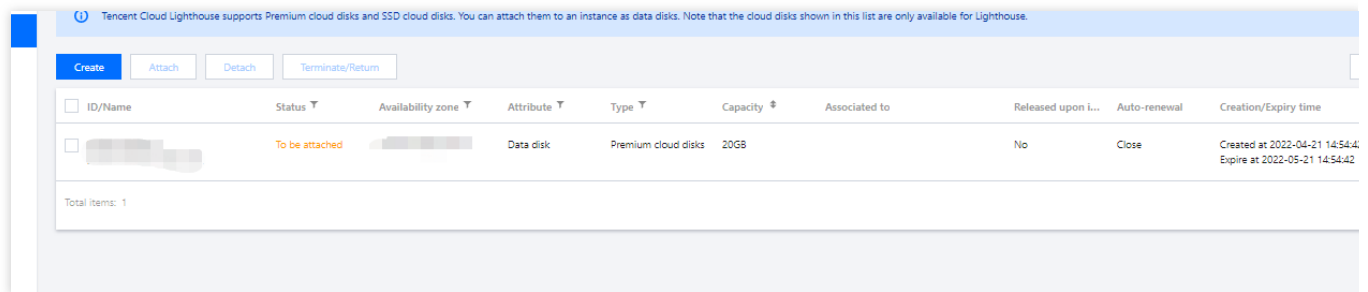
## Directions

You can attach the cloud disks in the following ways:

Select an instance to associate

Select a cloud disk to attach

1. Log in to the Lighthouse console and click **Cloud Disk** on the left sidebar.
2. Select a region at the top of the **Cloud Disk** page, find the target cloud disk, and click **More > Attach**.



3. Open **Attach to the instance > Select an instance**.

Select the target instance, and complete the parameters **Attaching options**.

Unified expiry time with the instance (XXX)

Monthly auto-renewal (**recommended**)

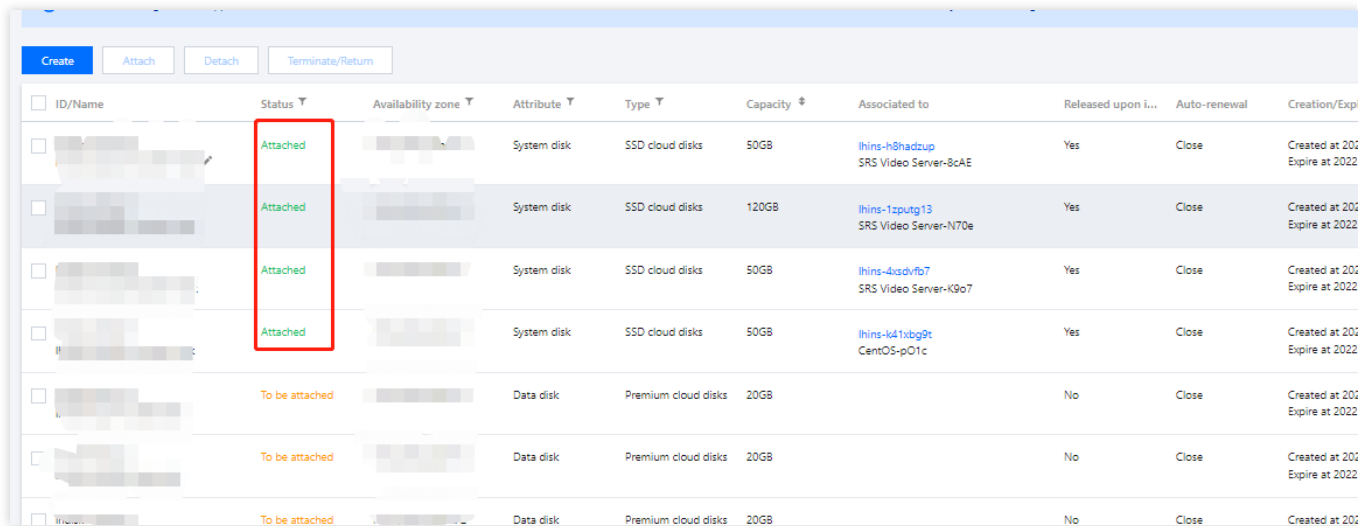
Attach directly

4. Click **Next**, and note the following in **Subsequent operations**:

After attaching the cloud disk, you need to log in to the instance and initialize the disk.

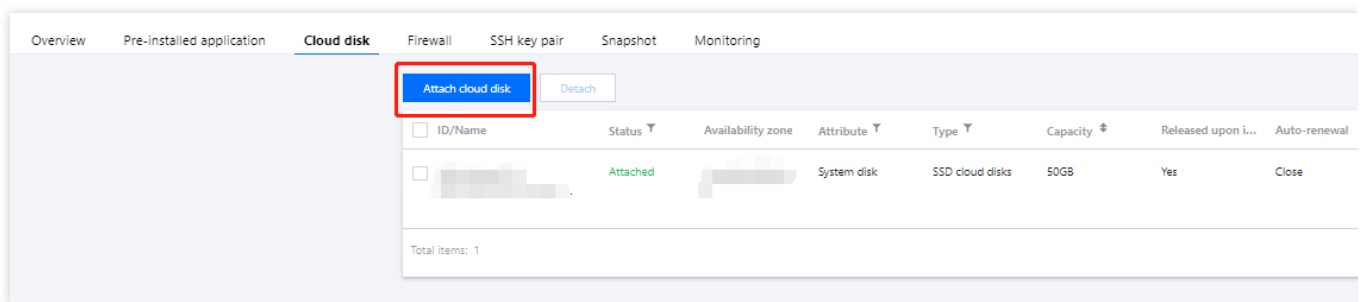
5. Click **Attach now**.

If the status of the cloud disk changes to **Attached**, the attachment is successful.



ID/Name	Status	Availability zone	Attribute	Type	Capacity	Associated to	Released upon i...	Auto-renewal	Creation/Exp
[blurred]	Attached	[blurred]	System disk	SSD cloud disks	50GB	lhins-h8hadzup SRS Video Server-8cAE	Yes	Close	Created at 201... Expire at 2022
[blurred]	Attached	[blurred]	System disk	SSD cloud disks	120GB	lhins-1zputg13 SRS Video Server-N70e	Yes	Close	Created at 201... Expire at 2022
[blurred]	Attached	[blurred]	System disk	SSD cloud disks	50GB	lhins-4xsdvfb7 SRS Video Server-K9o7	Yes	Close	Created at 201... Expire at 2022
[blurred]	Attached	[blurred]	System disk	SSD cloud disks	50GB	lhins-k41xbg9t CentOS-p01c	Yes	Close	Created at 201... Expire at 2022
[blurred]	To be attached	[blurred]	Data disk	Premium cloud disks	20GB		No	Close	Created at 201... Expire at 2022
[blurred]	To be attached	[blurred]	Data disk	Premium cloud disks	20GB		No	Close	Created at 201... Expire at 2022
[blurred]	To be attached	[blurred]	Data disk	Premium cloud disks	20GB		No	Close	Created at 201... Expire at 2022

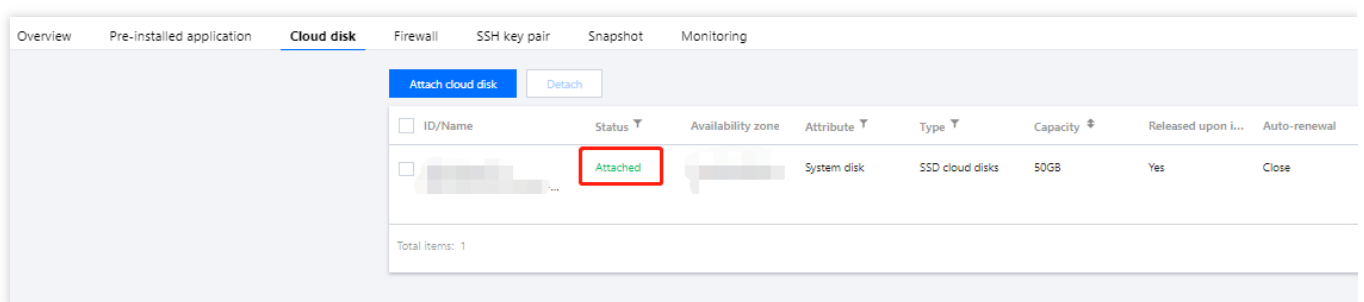
1. Log in to the [Lighthouse console](#) and select the target instance and enter the details page.
2. Select the **Cloud disk** tab, and click **Attach cloud disk**.



ID/Name	Status	Availability zone	Attribute	Type	Capacity	Released upon i...	Auto-renewal
[blurred]	Attached	[blurred]	System disk	SSD cloud disks	50GB	Yes	Close

Total items: 1

3. In the pop-up window, "select a cloud disk":  
 Select the cloud disk that needs to be attached, and complete the parameters **Attaching options**.  
 Unified expiry time with the instance (XXX)  
 Monthly auto-renewal (**recommended**)  
 Attach directly
4. Click **Next**,  
 After attaching the cloud disk, you need to log in to the instance and initialize the disk.



ID/Name	Status	Availability zone	Attribute	Type	Capacity	Released upon i...	Auto-renewal
[blurred]	Attached	[blurred]	System disk	SSD cloud disks	50GB	Yes	Close

Total items: 1



## Subsequent Operations

After attaching the cloud disk, you need to log in to the instance and initialize the disk first before using it. For details, see [Initializing a Cloud Disk](#).

# Initializing Cloud Disks

Last updated : 2023-05-10 14:17:34

## Overview

This document describes how to initialize a data disk in the Lighthouse console. After creating a cloud disk and attaching it to the Lighthouse instance as a data disk, you need to initialize the disk to use it.

## Prerequisites

Attach a cloud disk to your Lighthouse instance. See [Attaching a Cloud Disk](#).

## Considerations

Read [FAQs about cloud disk usage](#) before working with cloud disks.

Formatting a data disk will erase all data. Make sure that the disk does not contain data, or important data has been backed up.

To prevent service exceptions, ensure that the Lighthouse instance.

## Directions

Linux instance

Windows instances

Select the initialization method according to your actual use cases:

If the entire disk is presented as one independent partition (there is no logical disks such as vdb1 and vdb2), we strongly recommend that you not use partition, and directly [create the file system on bare devices](#).

If the entire disk needs to be presented as multiple logical partitions (there are multiple logical disks), you need to first partition the disk, and then [create the file system on a partition](#).

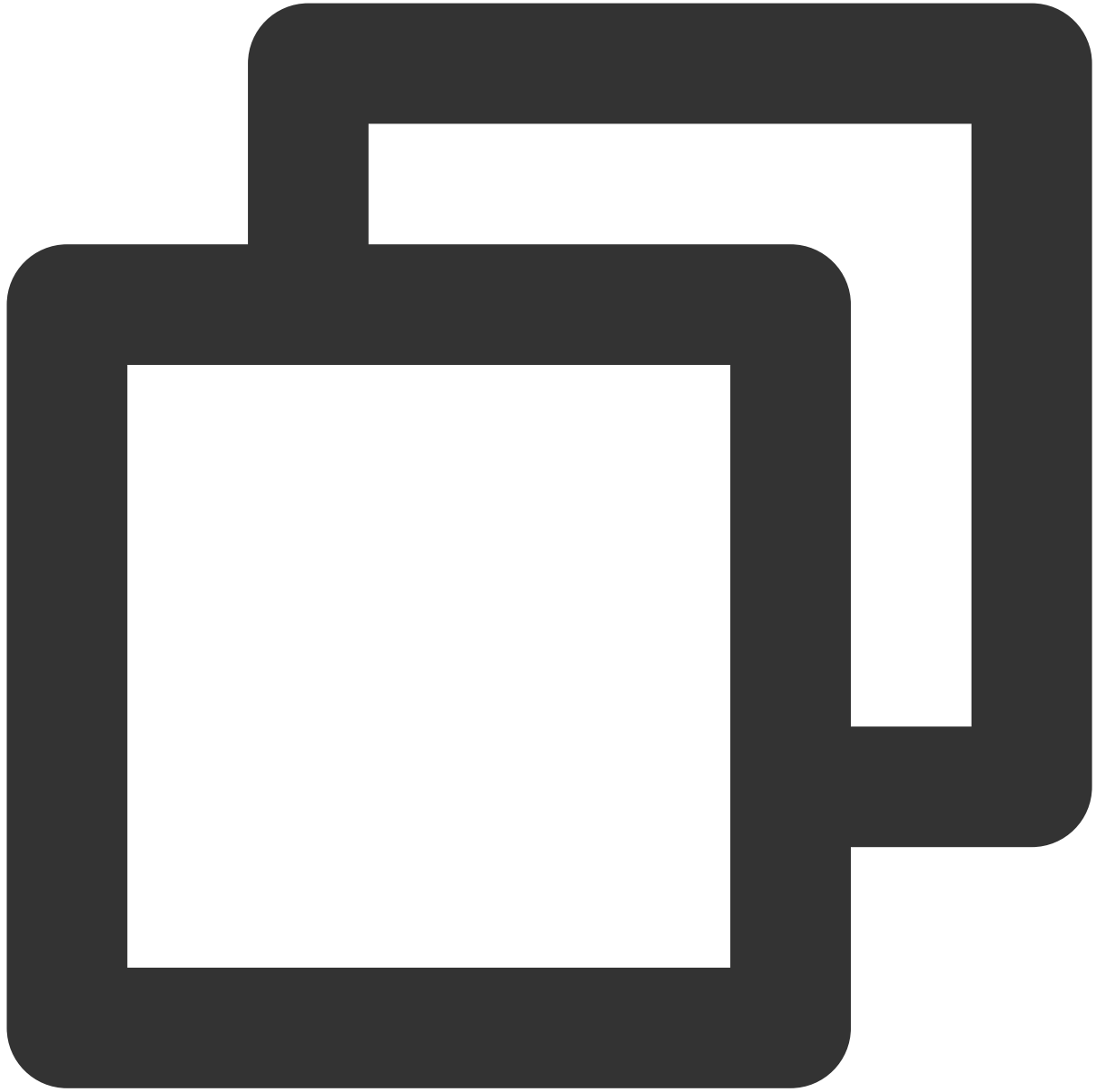
### Creating file systems on bare devices

#### Note:

This example uses a Lighthouse instance using CentOS 8.0 operating system. Note that the steps may vary according to the operating system version.

1. Log in to the Lighthouse instance. For details, see [Logging in to a Linux instance via WebShell](#).

2. Run the following command to view the disk name.



```
sudo fdisk -l
```

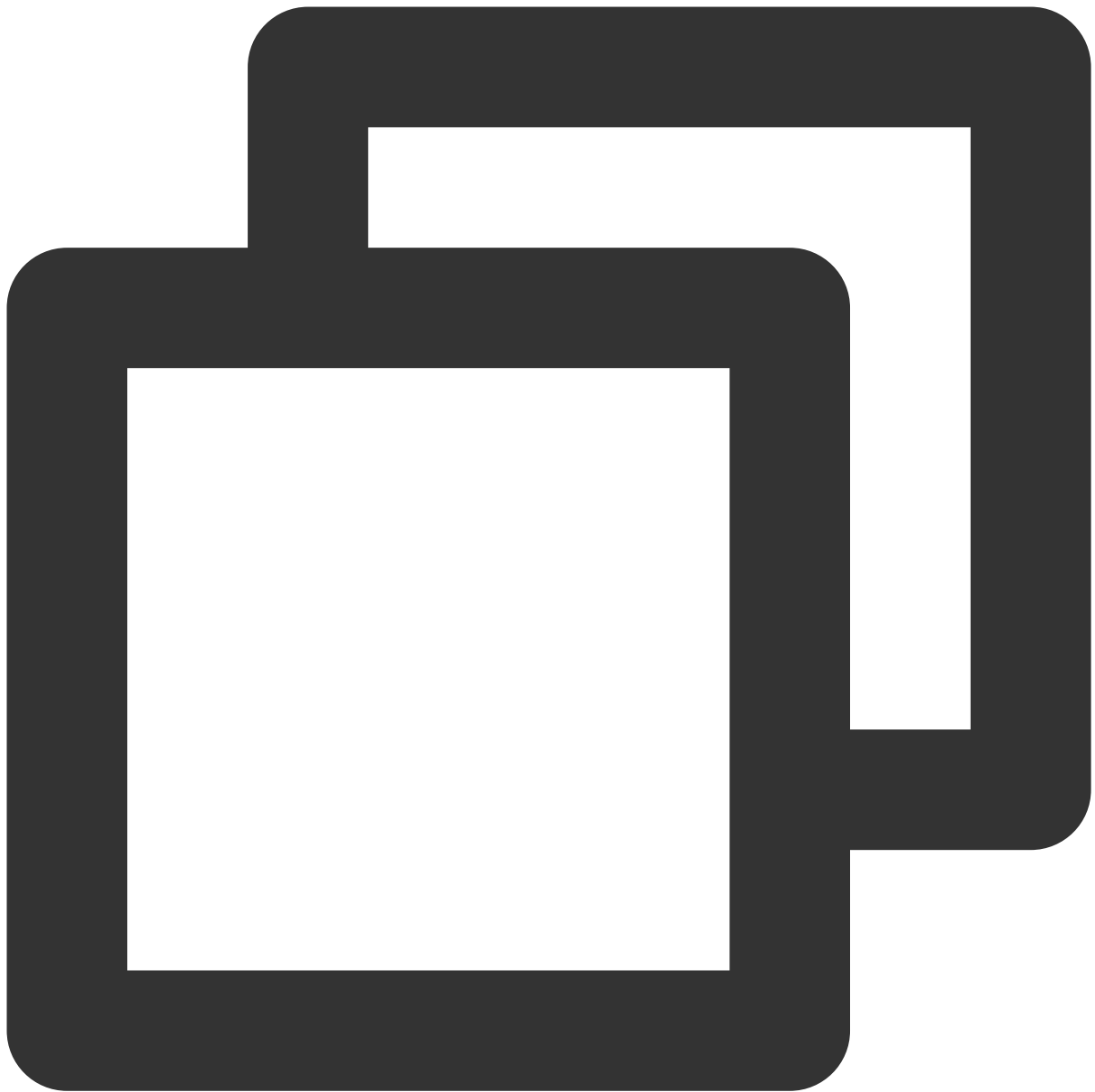
If the returned result is similar to what is shown below, the current Lighthouse instance has two disks, where `/dev/vda` is the system disk (40 GB) and `/dev/vdb` is the new data disk (20 GB).

```
[lighthouse@VM-20-8-centos ~]$ sudo fdisk -l
Disk /dev/vda: 40 GiB, 42949672960 bytes, 83886080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x89ee0607

   Device   Boot  Start      End  Sectors  Size Id Type
  /dev/vda1  *    2048 83886046 83883999   40G 83 Linux

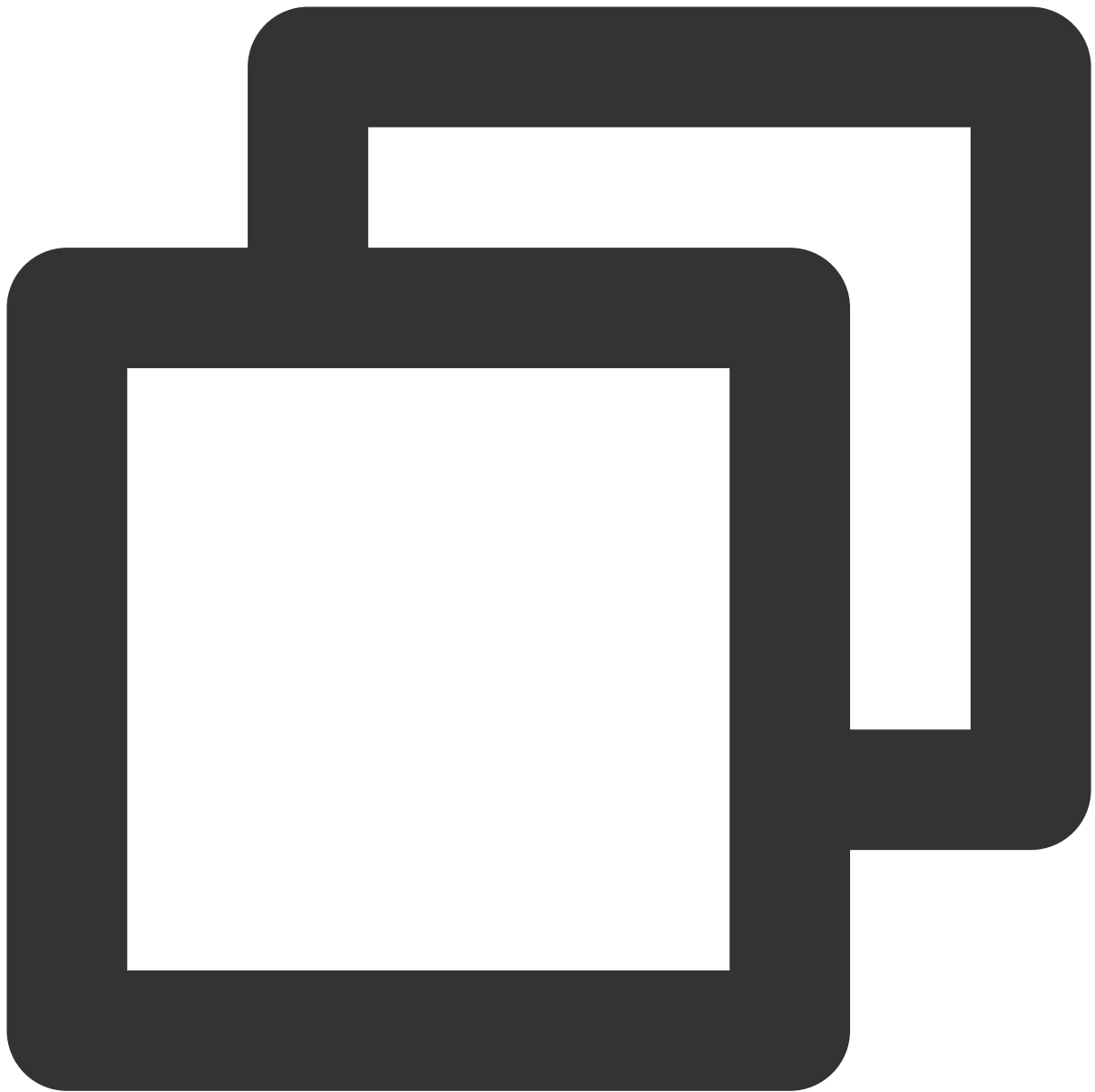
Disk /dev/vdb: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

3. Run the following command to create a file system on the `/dev/vdb` bare device.



```
sudo mkfs -t <File system format> /dev/vdb
```

The partition size supported by different file systems varies. Select an appropriate file system as needed. The following example takes `EXT4` as the file system:

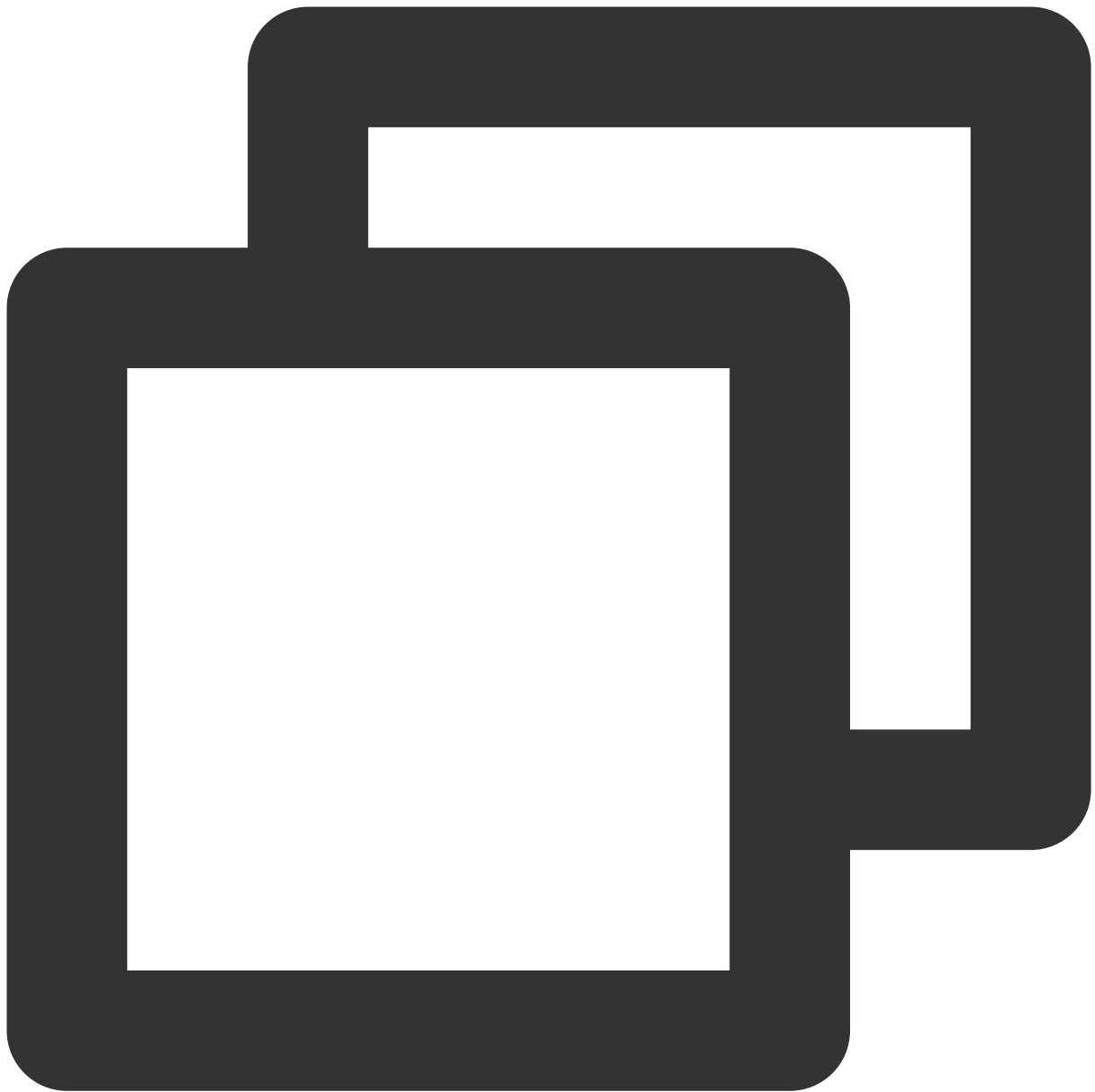


```
sudo mkfs -t ext4 /dev/vdb
```

**Note:**

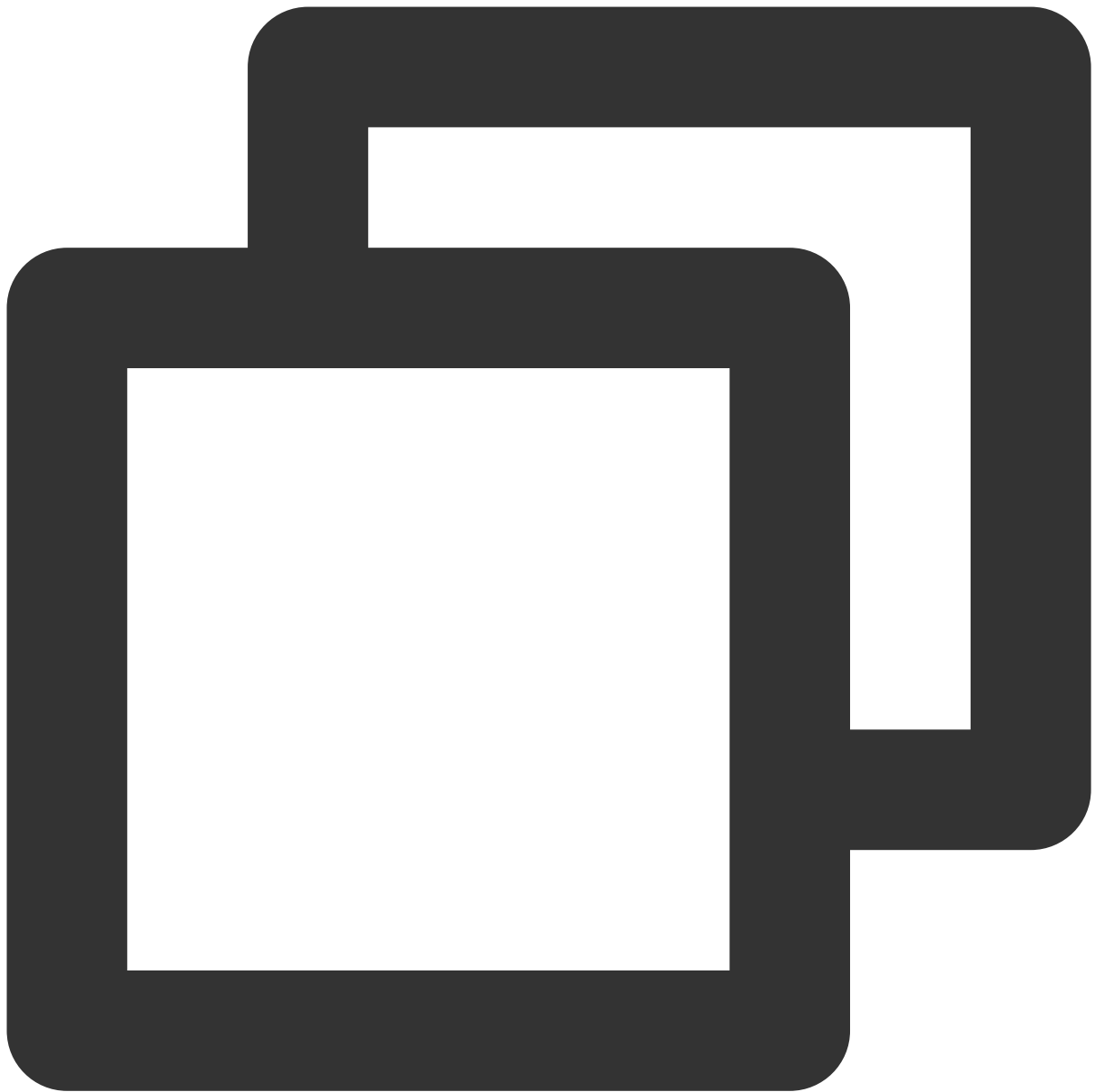
The formatting takes a while. Please pay attention to the system's running status and do not exit.

4. Run the following command to create a new mount point. The following example uses `/data` as the new mount point:



```
sudo mkdir /data
```

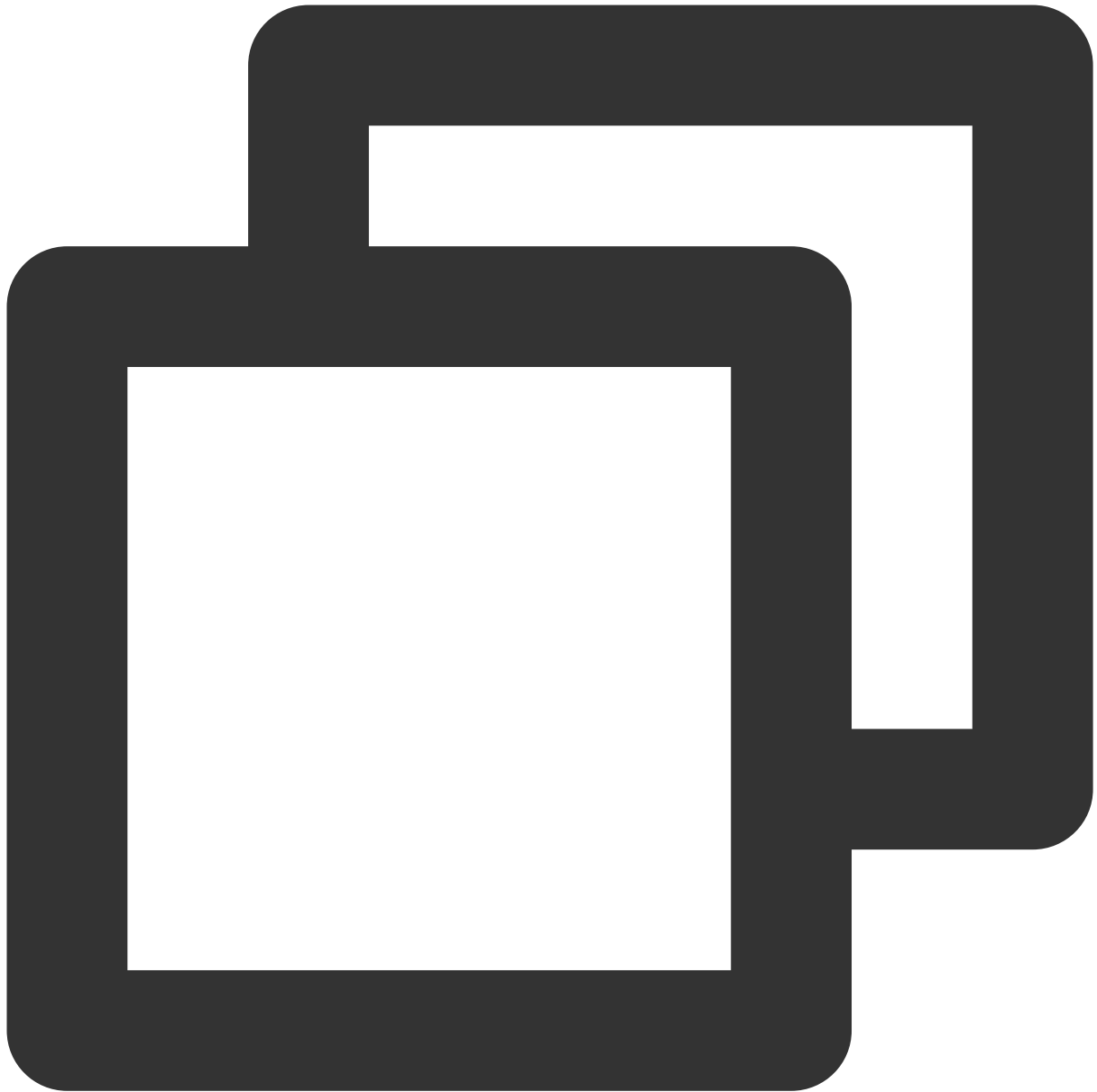
5. Run the following command to mount the device to a new mount point. The following example uses `/data` as the new mount point:



```
sudo mount /dev/vdb /data
```

6. Run the following command to view the mount result.





```
sudo df -TH
```

If the returned result is similar to what is shown below, `/dev/vdb` is mounted to `/data` successfully.

```
[lighthouse@VM-20-8-centos ~]$ sudo df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs  408M    0  408M   0% /dev
tmpfs           tmpfs     425M   25k  425M   1% /dev/shm
tmpfs           tmpfs     425M  463k  424M   1% /run
tmpfs           tmpfs     425M    0  425M   0% /sys/fs/cgroup
/dev/vda1       ext4      43G   3.4G   37G   9% /
tmpfs           tmpfs     85M    0   85M   0% /run/user/1000
/dev/vdb        ext4      22G   47M   20G   1% /data
tmpfs           tmpfs     85M    0   85M   0% /run/user/0
```

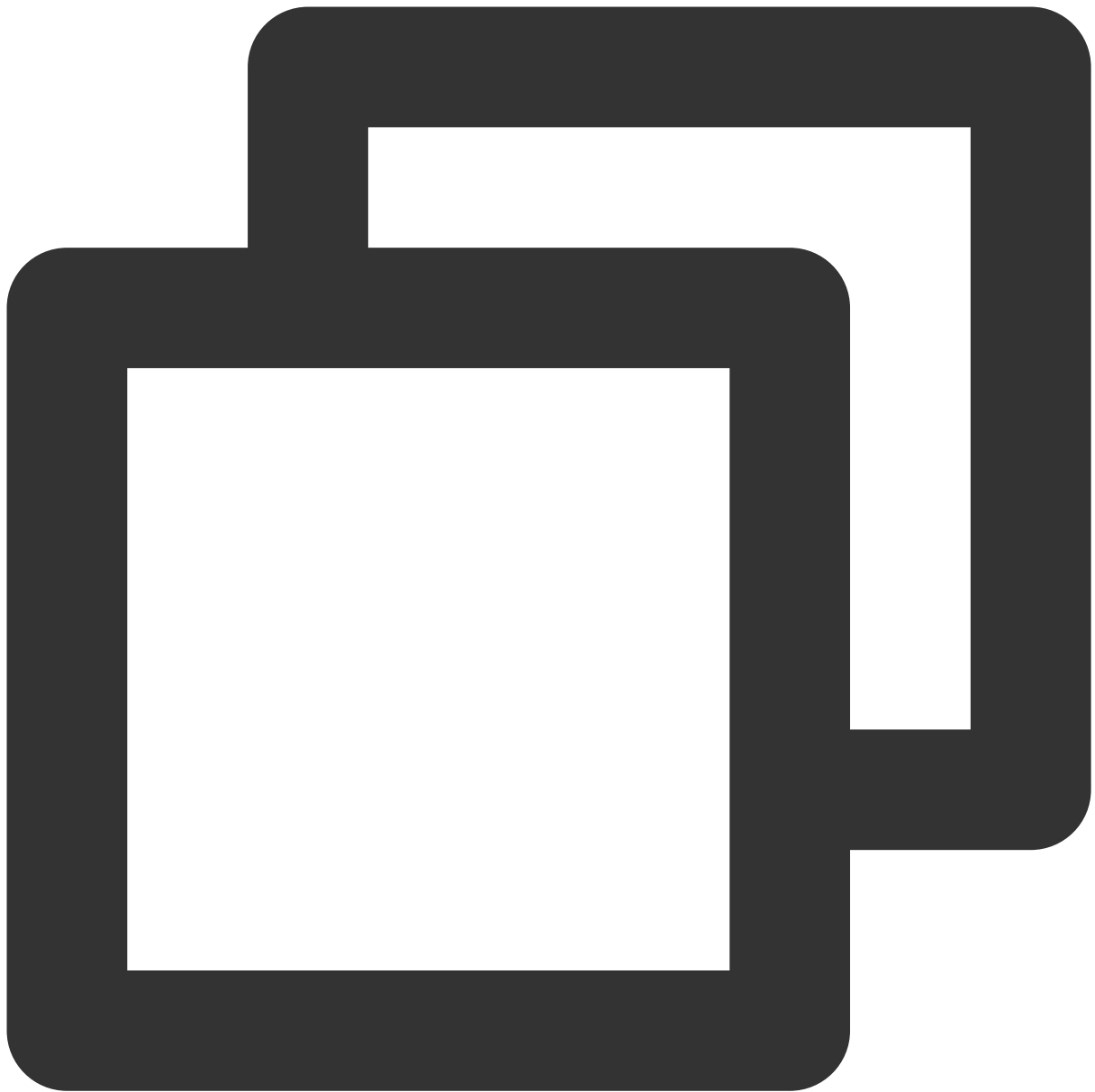
The disk needs to be mounted to the instance every time the instance starts up. To set the disk to be automatically mounted upon instance start-up, see [Auto-Mounting Disk upon Linux Instance Start-up](#).

## Creating a file system on a partition

### Note:

This example uses the parted partition tool in the CentOS 8.0 operating system to configure data disk `/dev/vdc` as the primary partition. MBR is used as the default partition format, EXT4 format as the file system, and `/data/newpart` as the mount point. Disk automount at startup is configured. Note that the formatting operation may vary according to the operating system.

1. Log in to the Lighthouse instance. For details, see [Logging In to a Linux instance via WebShell](#).
2. Run the following command to view the disk name.



```
sudo fdisk -l
```

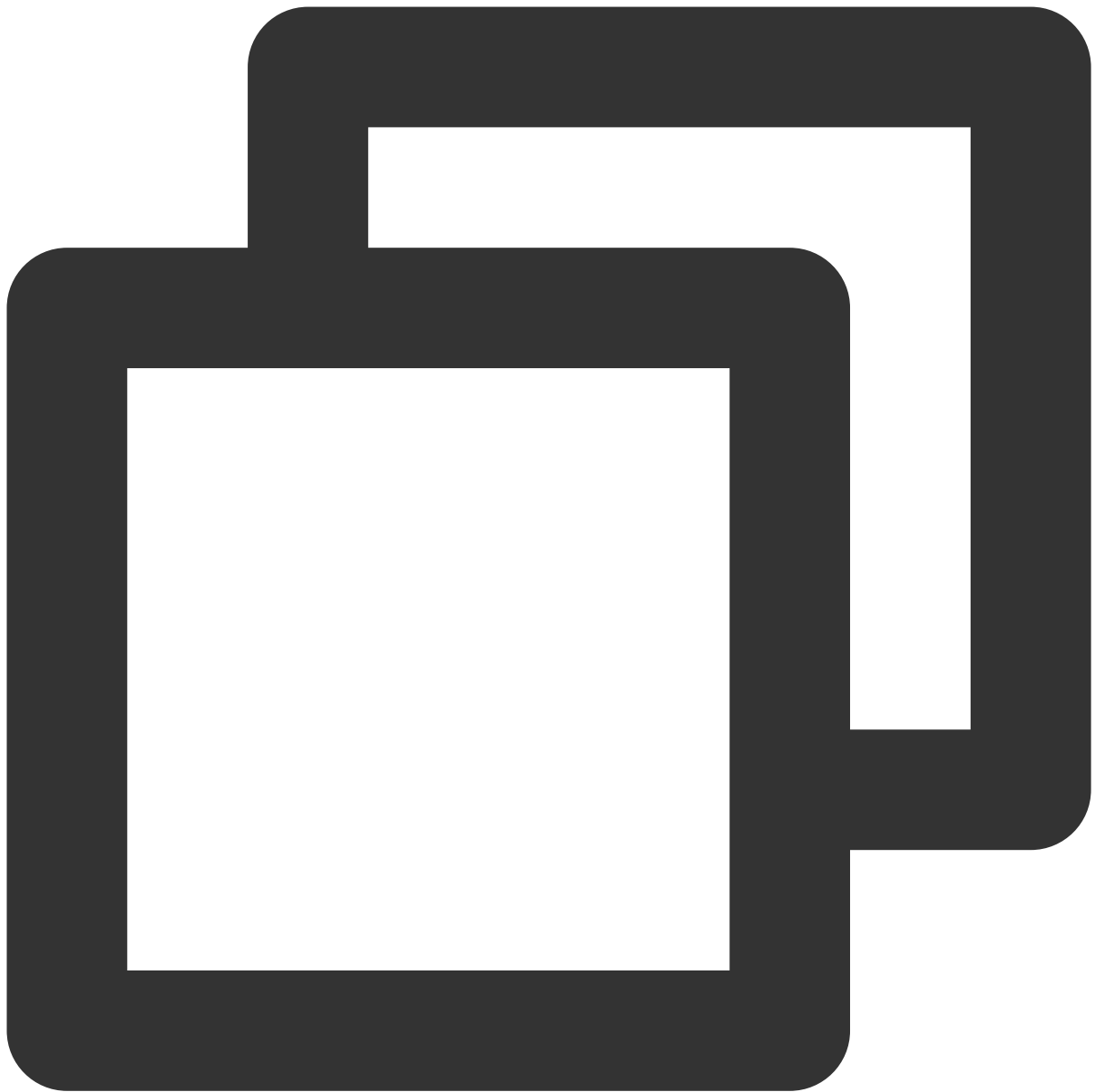
If the returned result is similar to what is shown below, the current Lighthouse instance has two disks, where `/dev/vda` is the system disk (40 GB) and `/dev/vdb` is the new data disk (20 GB).

```
[lighthouse@VM-20-8-centos ~]$ sudo fdisk -l
Disk /dev/vda: 40 GiB, 42949672960 bytes, 83886080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x89ee0607

   Device   Boot  Start      End  Sectors  Size Id Type
  /dev/vda1  *    2048 83886046 83883999   40G 83 Linux

Disk /dev/vdb: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

3. Run the following command to enter the fdisk partition tool and start partitioning the new data disk. The following example uses `/dev/vdb` as the newly attached data disk:



```
sudo fdisk /dev/vdb
```

The returned information is similar to what is shown below:

```
[lighthouse@VM-20-8-centos ~]$ sudo fdisk /dev/vdb

Welcome to fdisk (util-linux 2.32.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0xc0908d82.

Command (m for help):
```

4. Enter **n** and press **Enter** to start creating a partition. The following information is returned:

```
Command (m for help): n
Partition type
  p   primary (0 primary, 0 extended, 4 free)
  e   extended (container for logical partitions)
```

This indicates that the disk has two partition types:

p: Primary partition.

e: Extended partition.

5. Take creating a primary partition as an example. Enter **p** and press **Enter** to start creating a primary partition.

The following information is returned:

```
Select (default p): p
Partition number (1-4, default 1):
```

**Partition number** indicates the number of the primary partition. Valid range: 1-4.

6. Take partition 1 as an example. Enter the primary partition number **1** and press **Enter**. The following information is returned:

```
Partition number (1-4, default 1): 1
First sector (2048-41943039, default 2048):
```

**First sector** indicates the start sector. Valid range: 2048 (default value) - 41943039.

7. Take selecting the default start sector number 2048 as an example. Press **Enter**. The following information is returned:

```
First sector (2048-41943039, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-41943039, default 41943039):
```

**Last sector** indicates the end sector. Valid range: 2048 - 41943039 (default value).

8. Take selecting the default end sector number 41943039 as an example. Press **Enter**. The following information is returned:

```
Created a new partition 1 of type 'Linux' and of size 20 GiB.  
Command (m for help):
```

9. The partitioning is complete. A new partition has been created on the 20 GB data disk.

10. Enter **p** and press **Enter** to view the details of the new partition `/dev/vdb1`.

```
Command (m for help): p  
Disk /dev/vdb: 20 GiB, 21474836480 bytes, 41943040 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: dos  
Disk identifier: 0x08279334  
  
Device      Boot Start      End  Sectors  Size Id Type  
/dev/vdb1   2048 41943039 41940992   20G 83 Linux
```

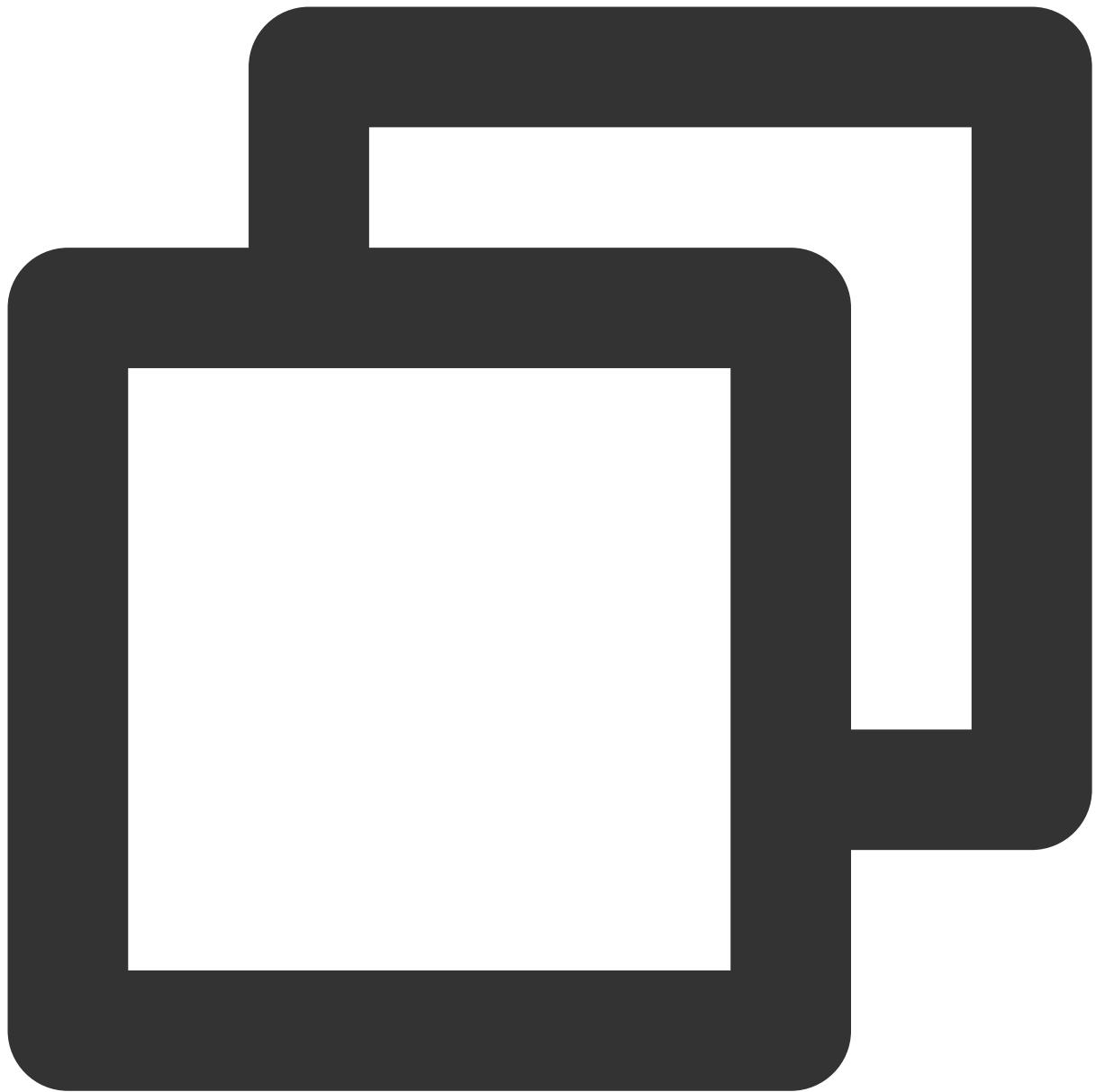
#### Note:

If an error occurs during the partitioning operation, enter **q** to exit the fdisk tool and the prior partition result will not be retained.

11. Enter **w** and press **Enter** to write the partition result to the partition table. The returned result is shown below, indicating that the partition creation is complete.

```
Command (m for help): w  
The partition table has been altered.  
Calling ioctl() to re-read partition table.  
Syncing disks.
```

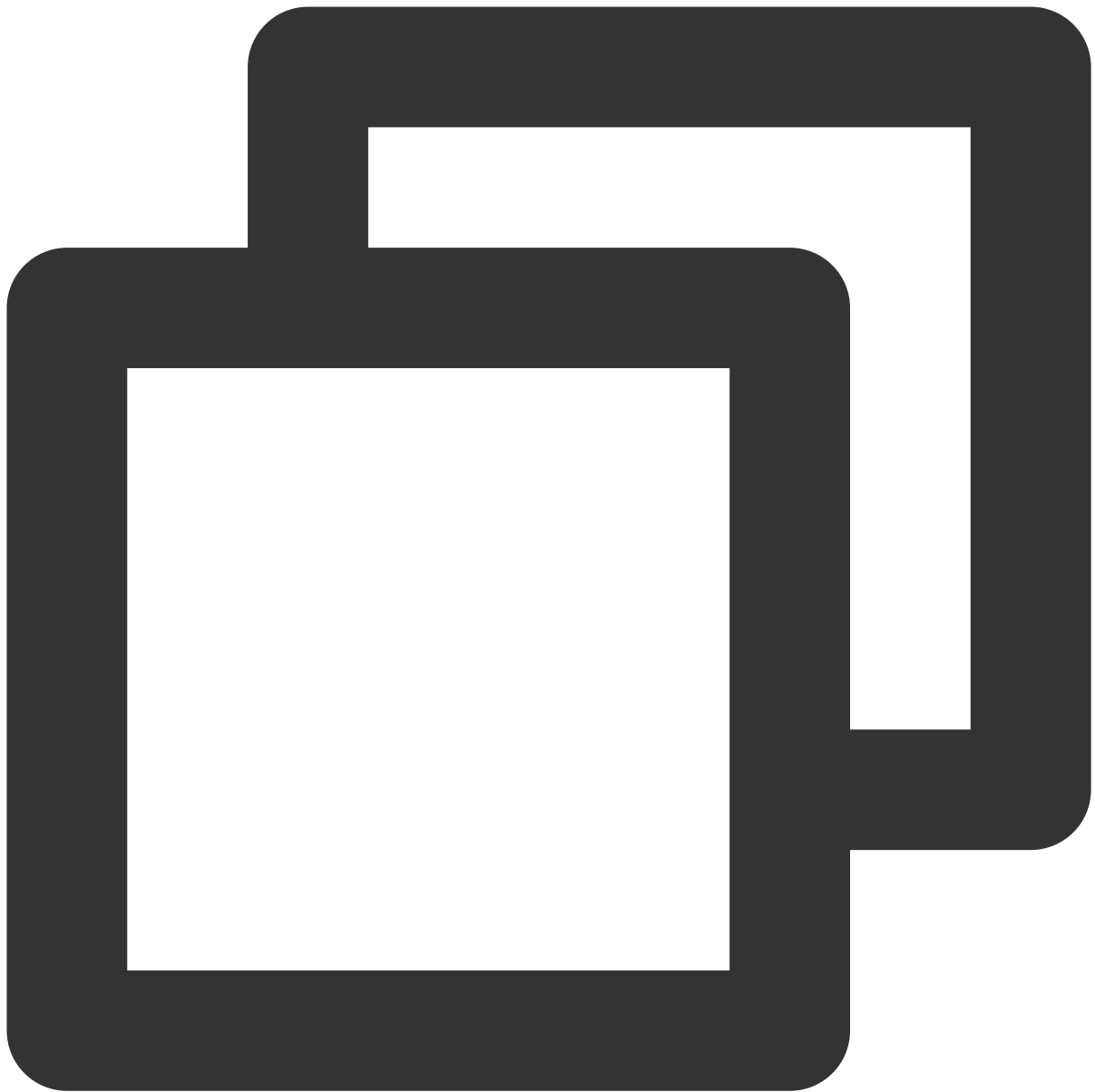
12. Run the following command to sync the partition table to the operating system.



```
partprobe
```

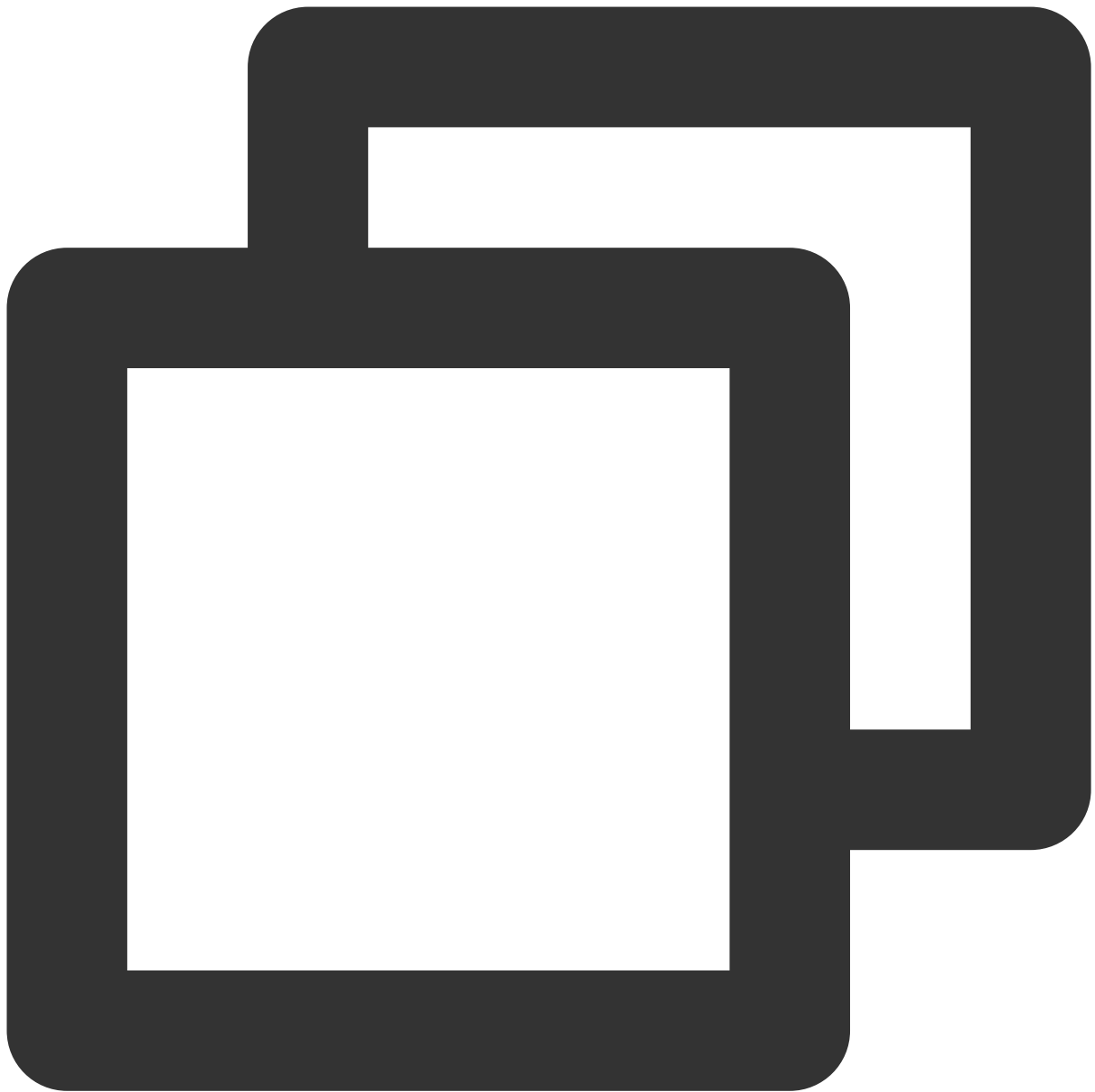
13. Run the following command to set the file system of the new partition to the format required by the system.





```
sudo mkfs -t <File system format> /dev/vdb1
```

The partition size supported by different file systems varies. Select an appropriate file system as needed. The following example takes `EXT4` as the file system:

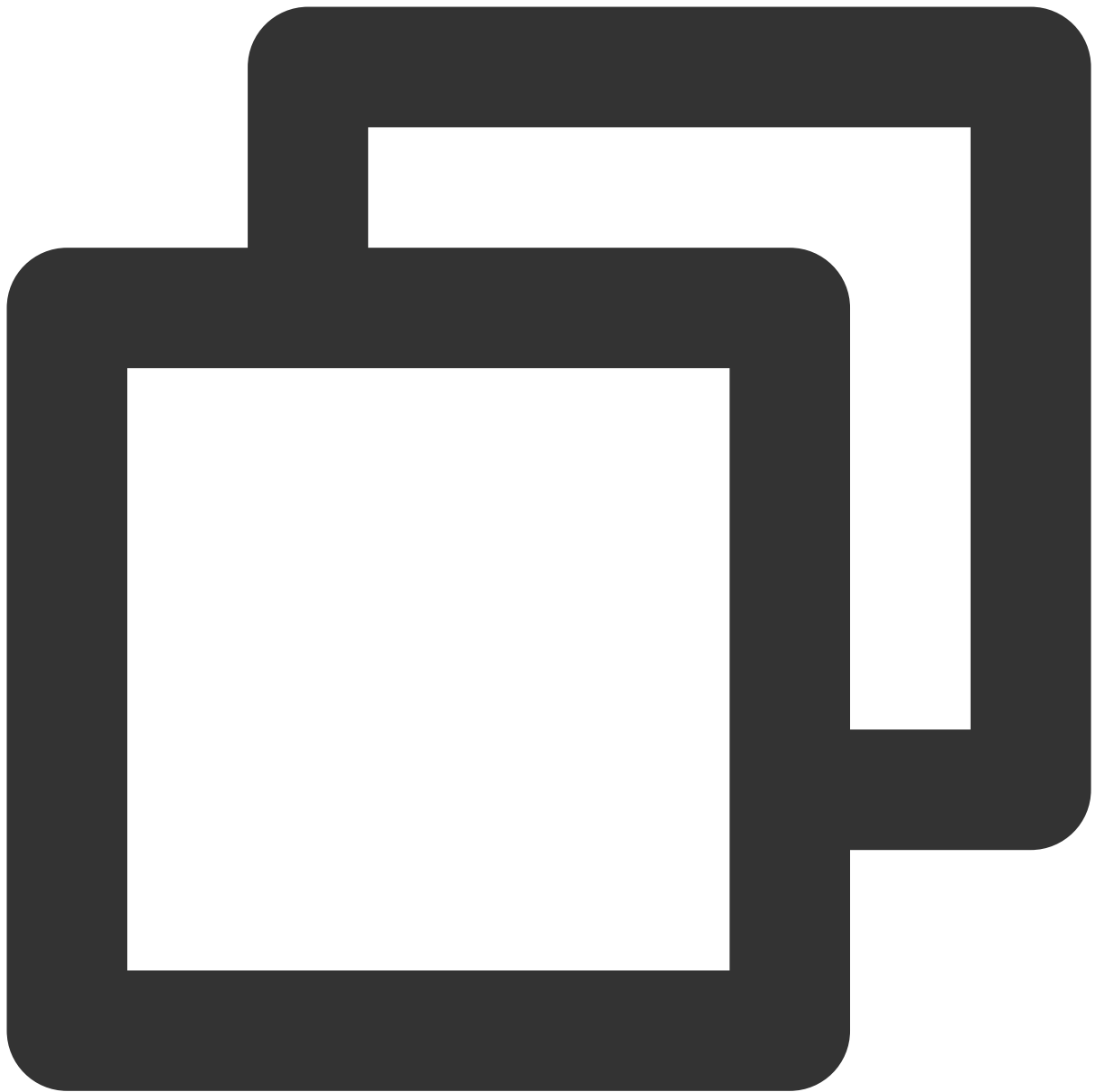


```
sudo mkfs -t ext4 /dev/vdb1
```

**Note:**

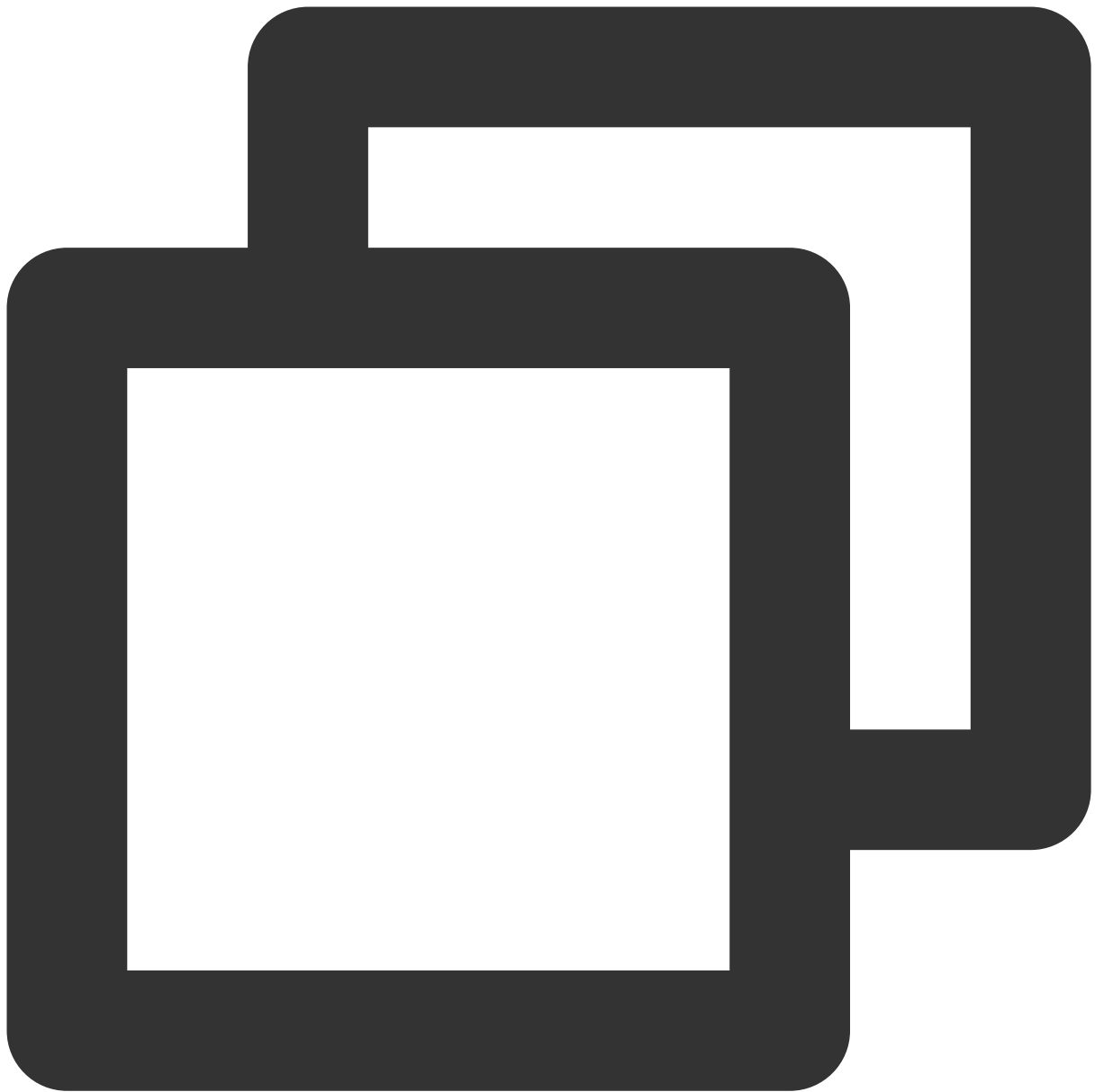
The formatting takes a while. Please pay attention to the system's running status and do not exit.

14. Run the following command to create a new mount point. The following example uses `/data/newpart` as the new mount point:



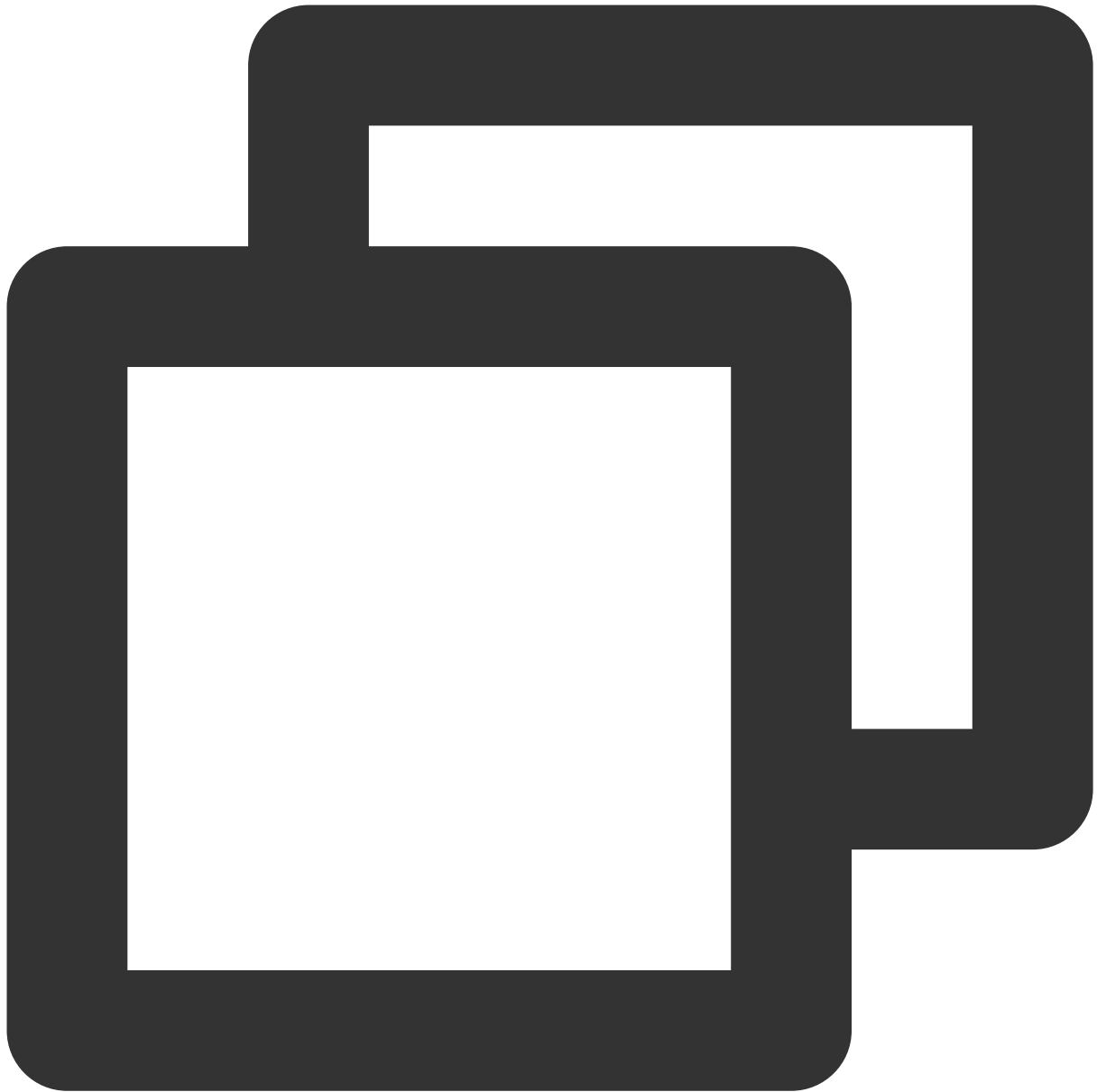
```
sudo mkdir /data/newpart
```

15. Run the following command to mount the new partition to a new mount point. The following example uses `/data/newpart` as the new mount point:



```
sudo mount /dev/vdb1 /data/newpart
```

16. Run the following command to view the mounting results.



```
sudo df -TH
```

The returned information is similar to what is shown below. This indicates that the partition `/dev/vdb1` has been mounted to `/data/newpart` .

```
[lighthouse@VM-20-8-centos ~]$ sudo df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs  408M   0    408M  0% /dev
tmpfs           tmpfs     425M  25k   425M  1% /dev/shm
tmpfs           tmpfs     425M  451k   424M  1% /run
tmpfs           tmpfs     425M   0    425M  0% /sys/fs/cgroup
/dev/vda1       ext4      43G   3.5G   37G   9% /
tmpfs           tmpfs     85M   0    85M  0% /run/user/1000
/dev/vdb1       ext4      22G   47M   20G   1% /data/newpart
```

The disk needs to be mounted to the instance every time the instance starts up. To set the disk partition to be automatically mounted upon instance start-up, see [Auto-Mounting Disk upon Linux Instance Start-up](#).

**Note:**

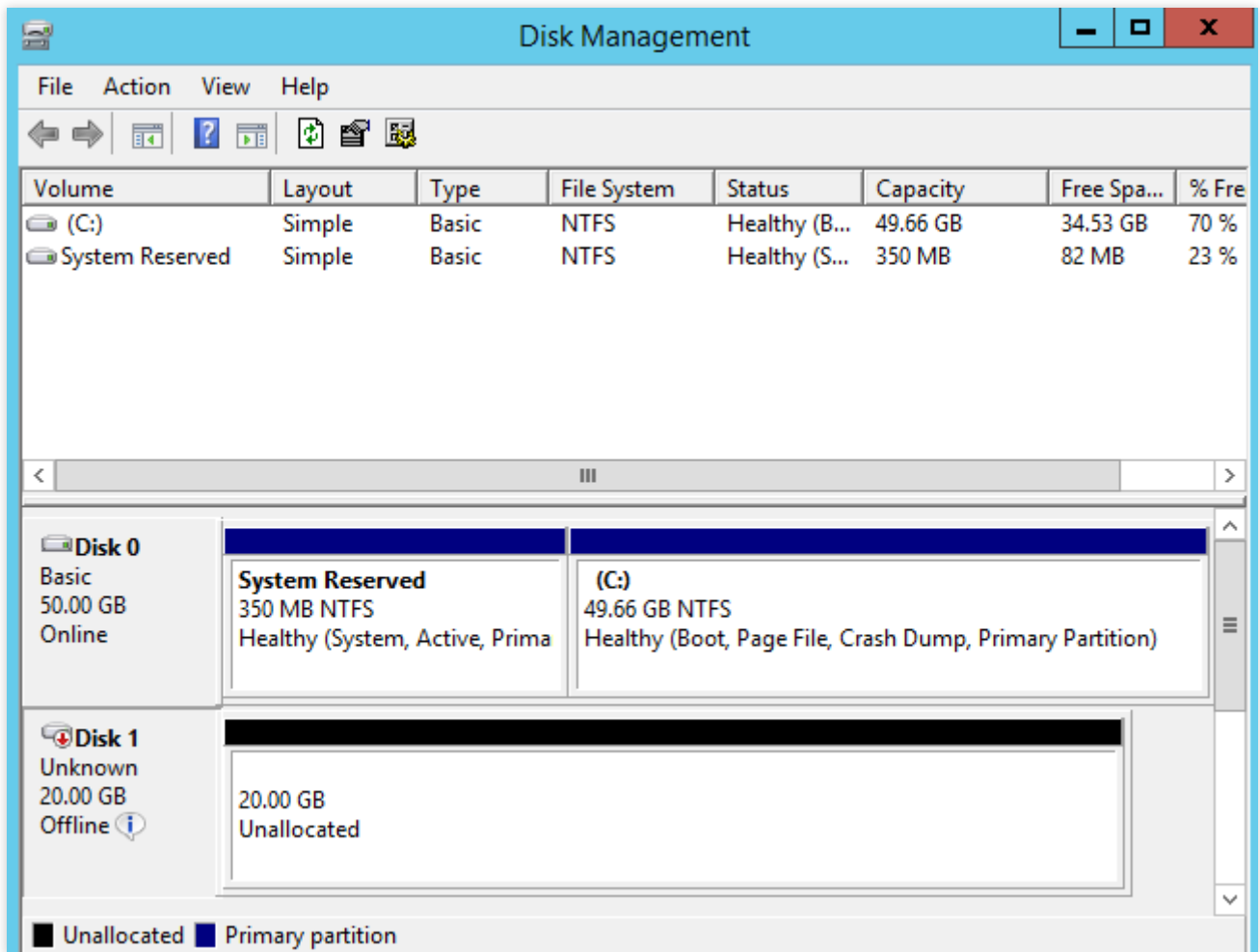
This example uses a Lighthouse instance using Windows Server 2016 R2 operating system. Note that the steps may vary according to the operating system version.

1. Log in to the Lighthouse instance. For more information, see [Logging in to a Windows Instance via VNC](#).
2. On the desktop, right-click



in the lower-left corner and click **Disk management** in the pop-up menu.

Open the **Disk management** window to view the data disk information.

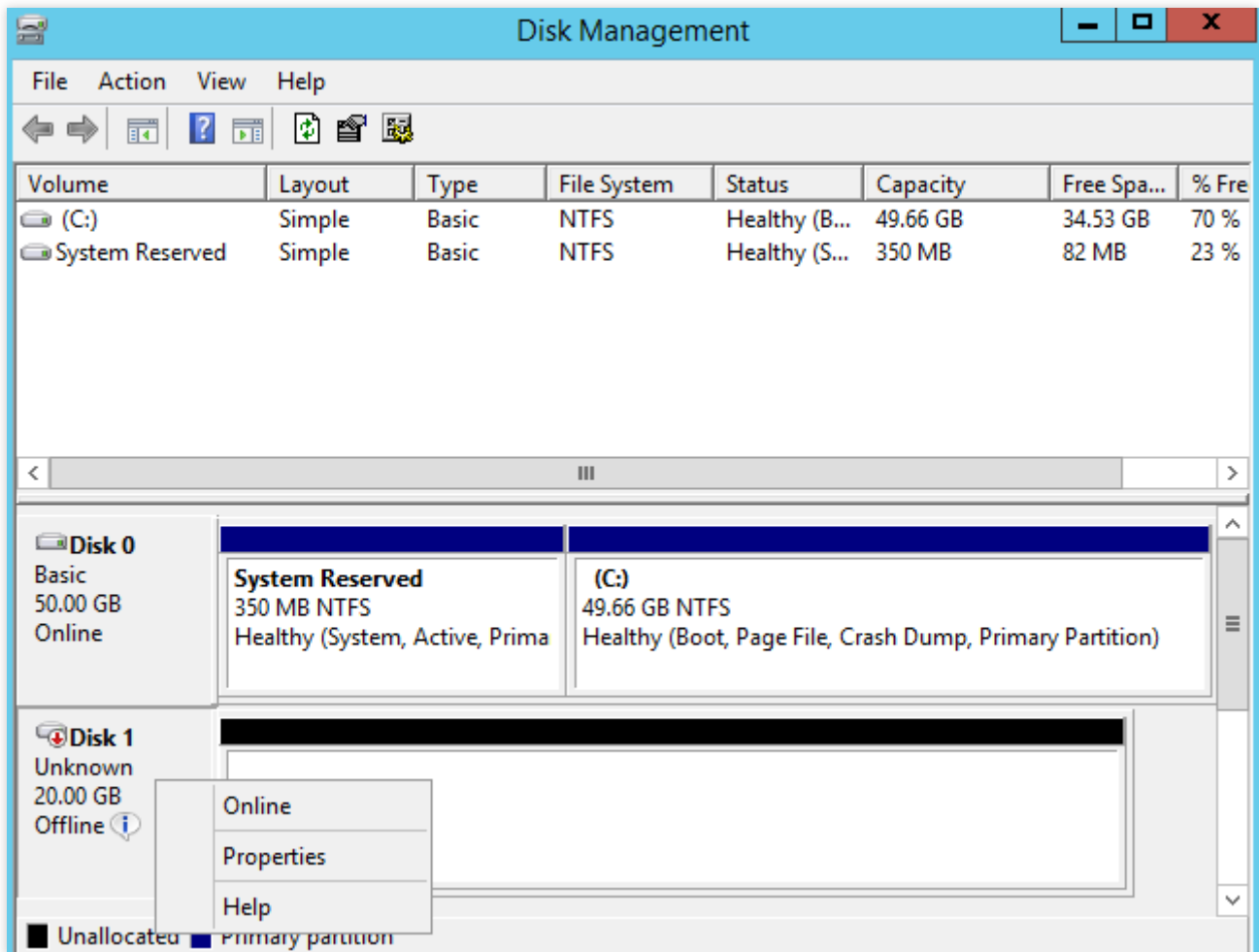
**Note:**

If the new disk is offline (as shown above), continue to [Step 3](#) to make it online. If it's already online, go to [Step 4](#).

3.

Right-click in the Disk 1 area

, and click **Online**.

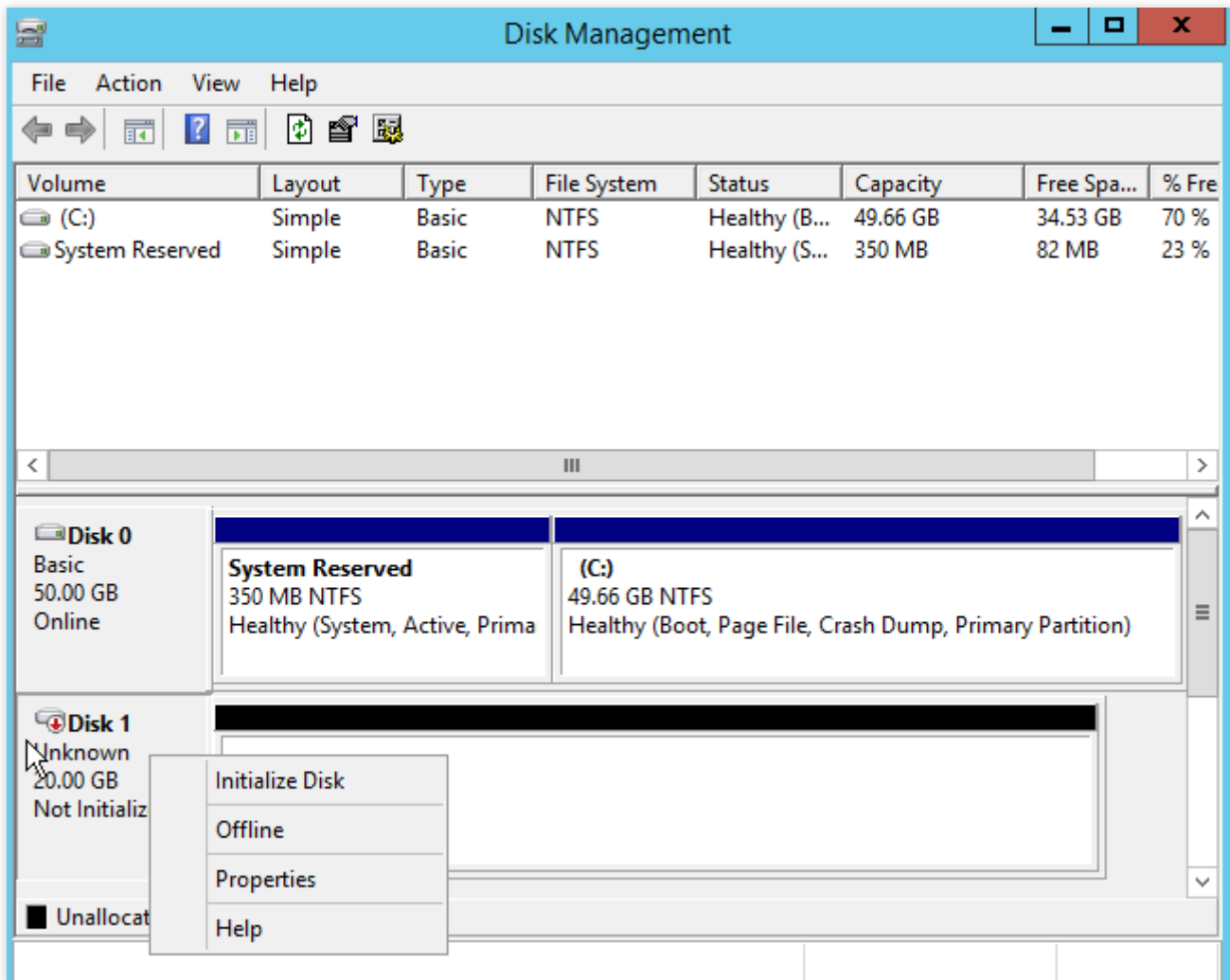


4.

Disk 1 changes from **Offline** to **Not Initialized**

. Right-click in the Disk 1 area and select **Initialize Disk**.

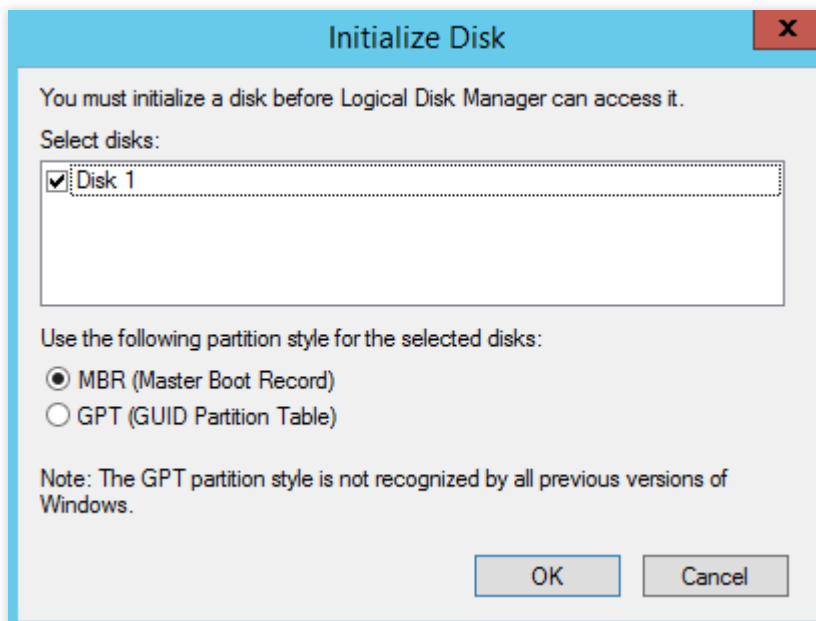




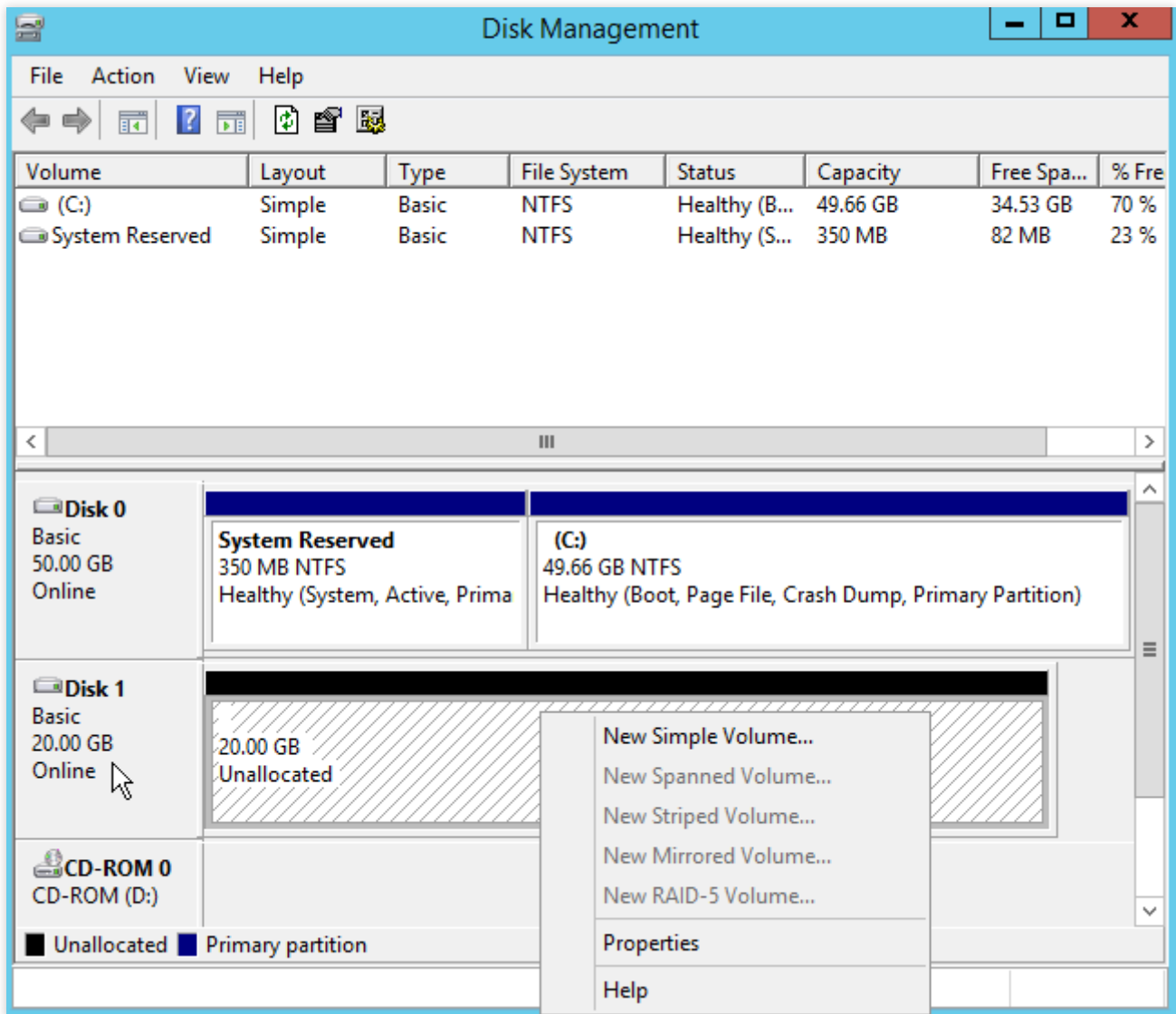
5. In the **Initialize Disk** window, select the target disk and the disk partition format, and click **OK**. In this example, **MBR (Master Boot Record)** is used.

**Note:**

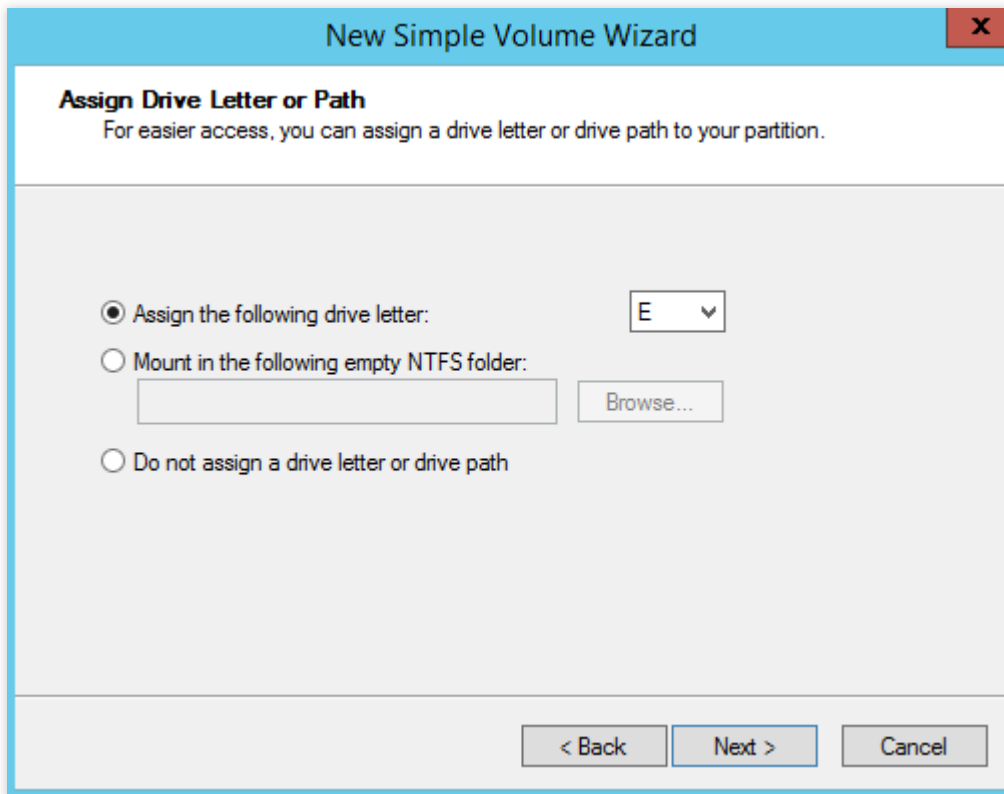
If the disk partition format is changed after the disk is put into use, the original data on the disk will be erased. Please select an appropriate partition format based on actual needs.



6. Right-click the free space of Disk 1, and select **New Simple Volume**.



7. In the welcome page of **New Simple Volume Wizard** pop-up window, click **Next**.
8. Specify the volume size as needed, which is the maximum value by default. Click **Next**.
9. Assign a drive letter, and click **Next**.



**New Simple Volume Wizard**

**Assign Drive Letter or Path**  
For easier access, you can assign a drive letter or drive path to your partition.

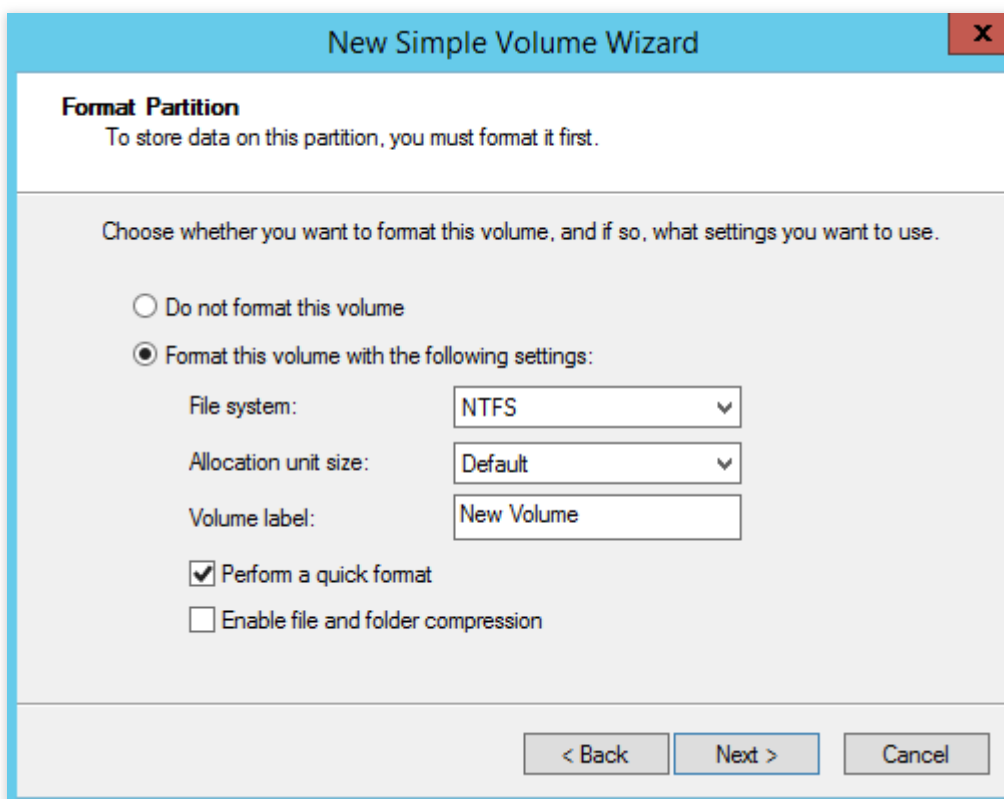
☒ Assign the following drive letter: E

☐ Mount in the following empty NTFS folder:  
 Browse...

☐ Do not assign a drive letter or drive path

< Back Next > Cancel

10. Select **Format this volume with the following settings**. Configure the parameters as needed, format the new partition, and click **Next**.



**New Simple Volume Wizard**

**Format Partition**  
To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

☐ Do not format this volume

☒ Format this volume with the following settings:

File system: NTFS

Allocation unit size: Default

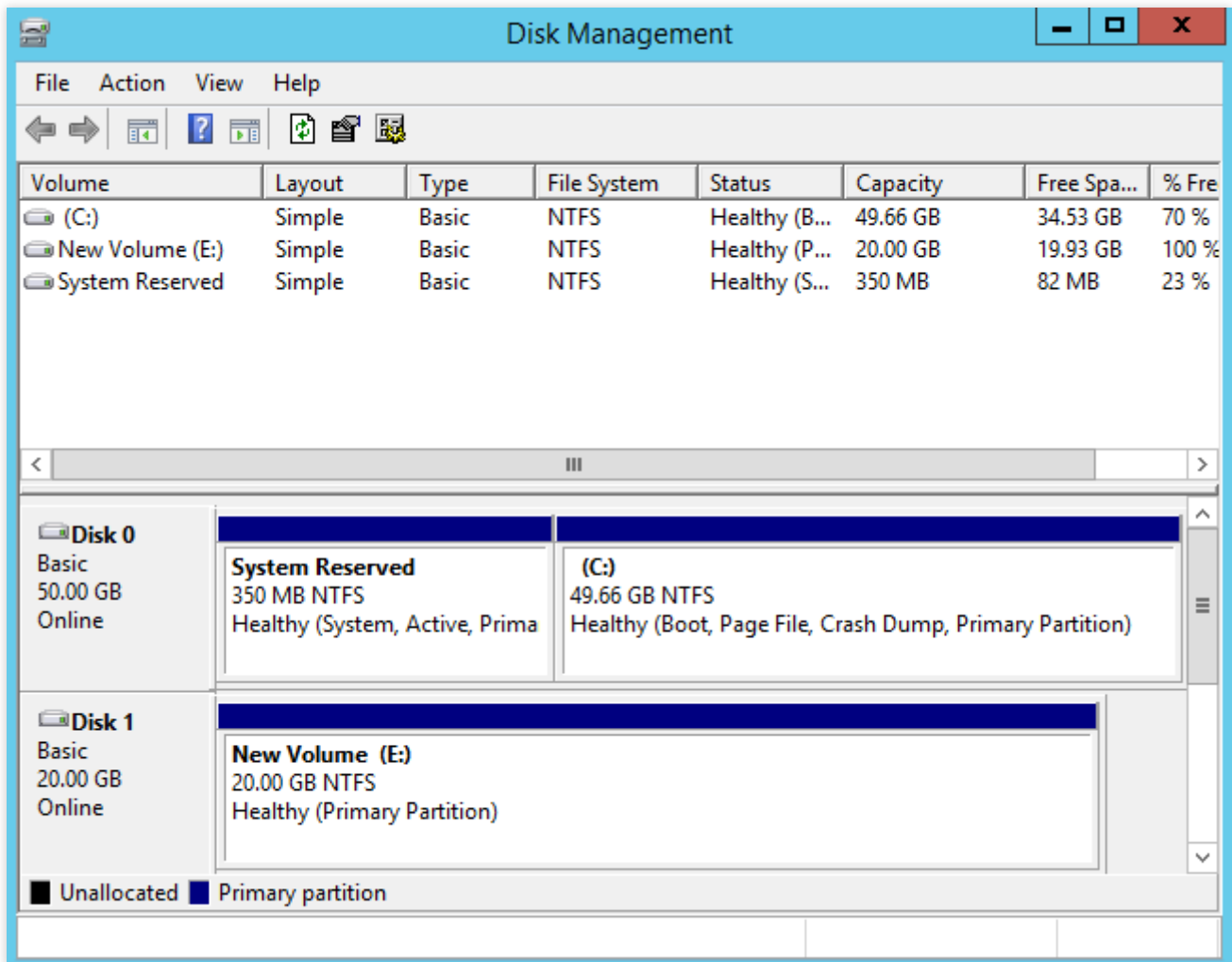
Volume label: New Volume

☒ Perform a quick format

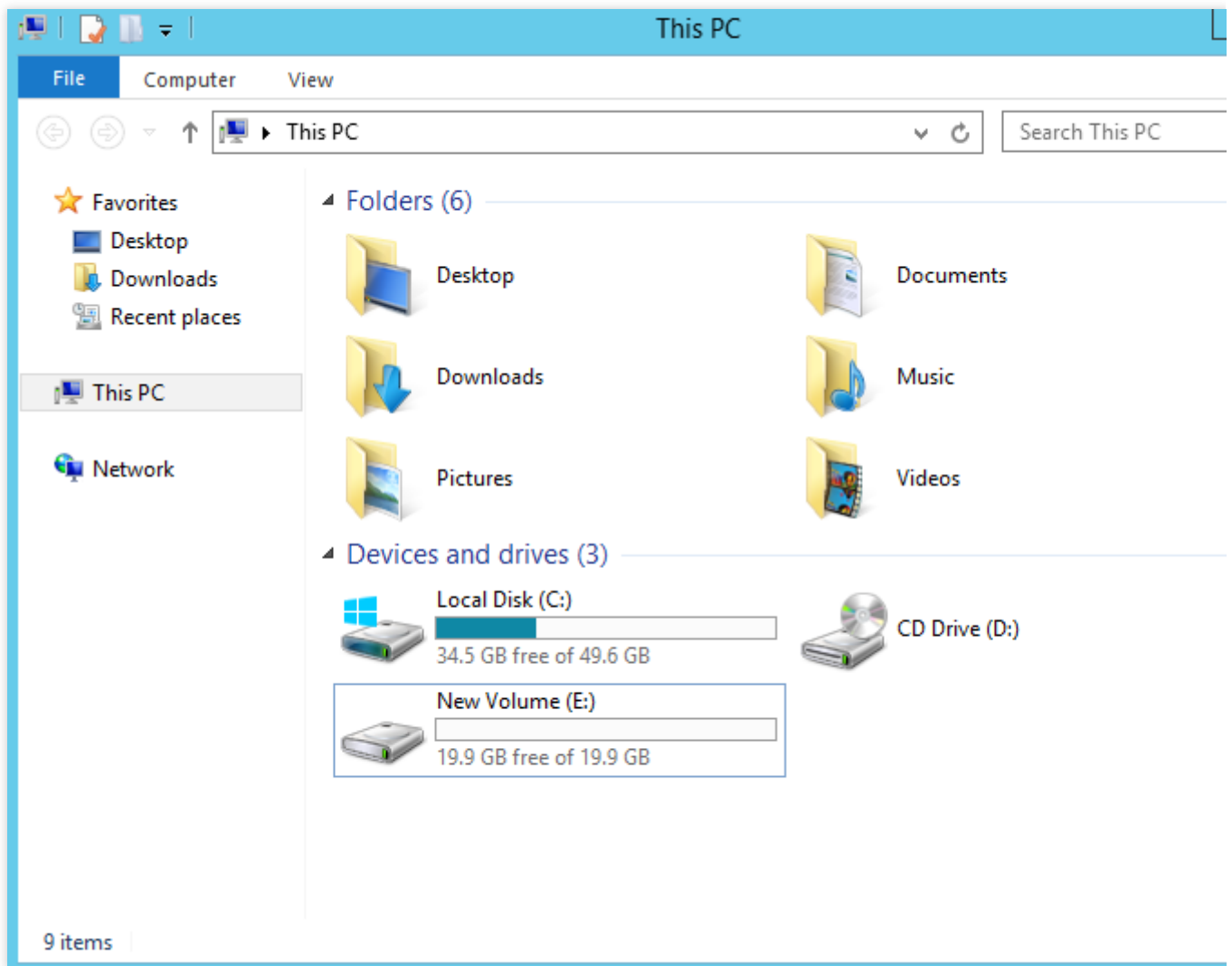
☐ Enable file and folder compression

< Back Next > Cancel

11. Click **Complete**. Wait for a while for the system to complete the initialization. When the volume status becomes "Healthy", the disk initialization is successful.



After the initialization is complete, enter the **PC** interface to view the new disk.



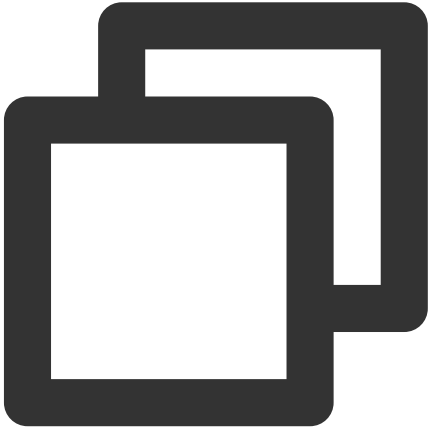
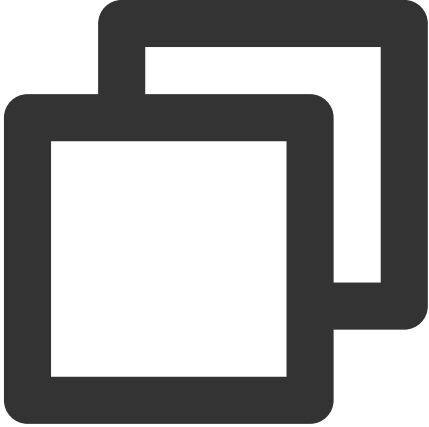
## Related Operations

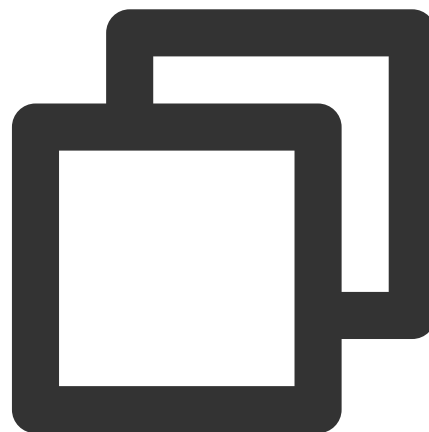
### Auto-mounting disks upon Linux instance start-up

1. Confirm the mounting method and obtain the corresponding information.

Based on business needs, you can use a cloud disk's soft link, file system's UUID (universally unique identifier), or device name to automatically mount a disk. The descriptions and information acquisition methods are as follows:

Mounting method	Pros and cons	Information acquisition method
Use the soft link of the cloud disk (recommended)	<p><b>Pros:</b> The soft link of a cloud disk is fixed and unique. It does not change with operations such as mounting, unmounting, and formatting partitions.</p> <p><b>Cons:</b> Only a cloud disk can use the soft link, which operates imperceptibly for the</p>	Run the following command to obtain the soft link of the cloud disk.

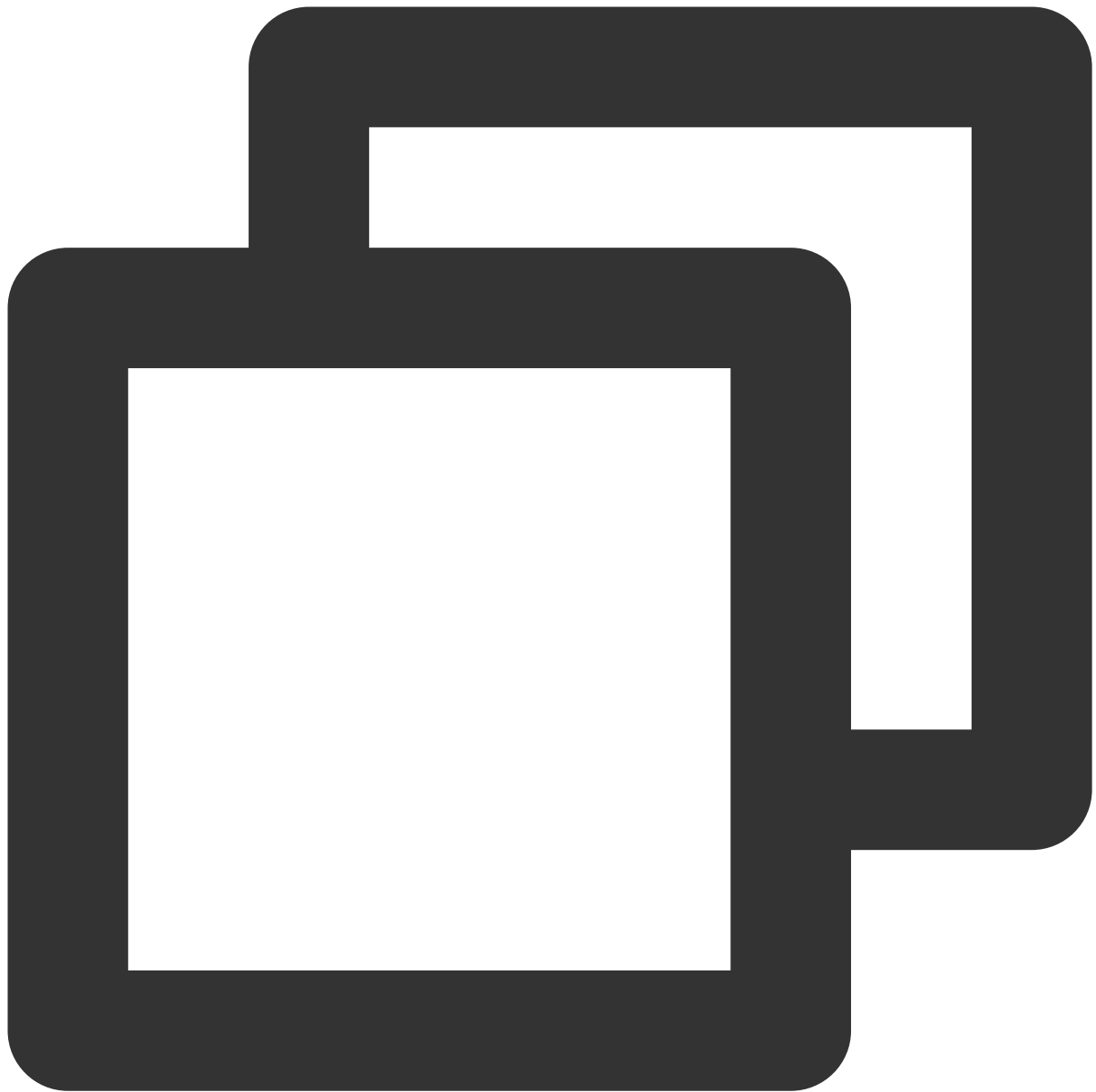
	partition formatting operation.	 <pre>sudo ls -l /dev/disk/by-id</pre>
Use the UUID of the file system	Auto-mounting configuration may fail due to changes in a file system's UUID. For example, reformatting a file system will change its UUID.	Run the following command to obtain the UUID of the file system.  <pre>sudo blkid /dev/vdb</pre>
Use device name	Auto-mounting configuration may fail due to changes in device name.	Run the following command to obtain the device name.



```
sudo fdisk -l
```

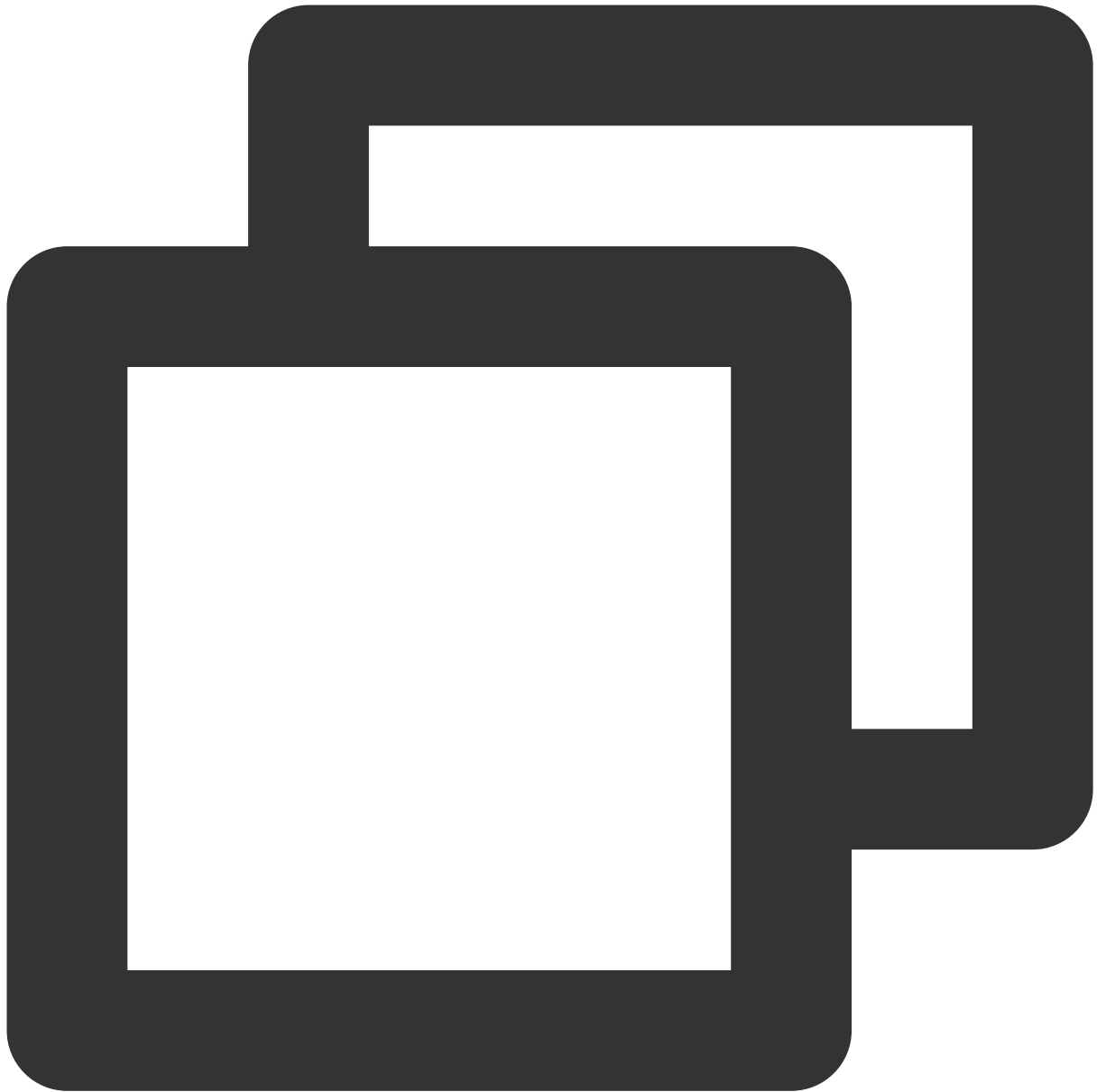
2. Run the following command to back up the `/etc/fstab` file to the `/home` directory, for example:





```
sudo cp -r /etc/fstab /home
```

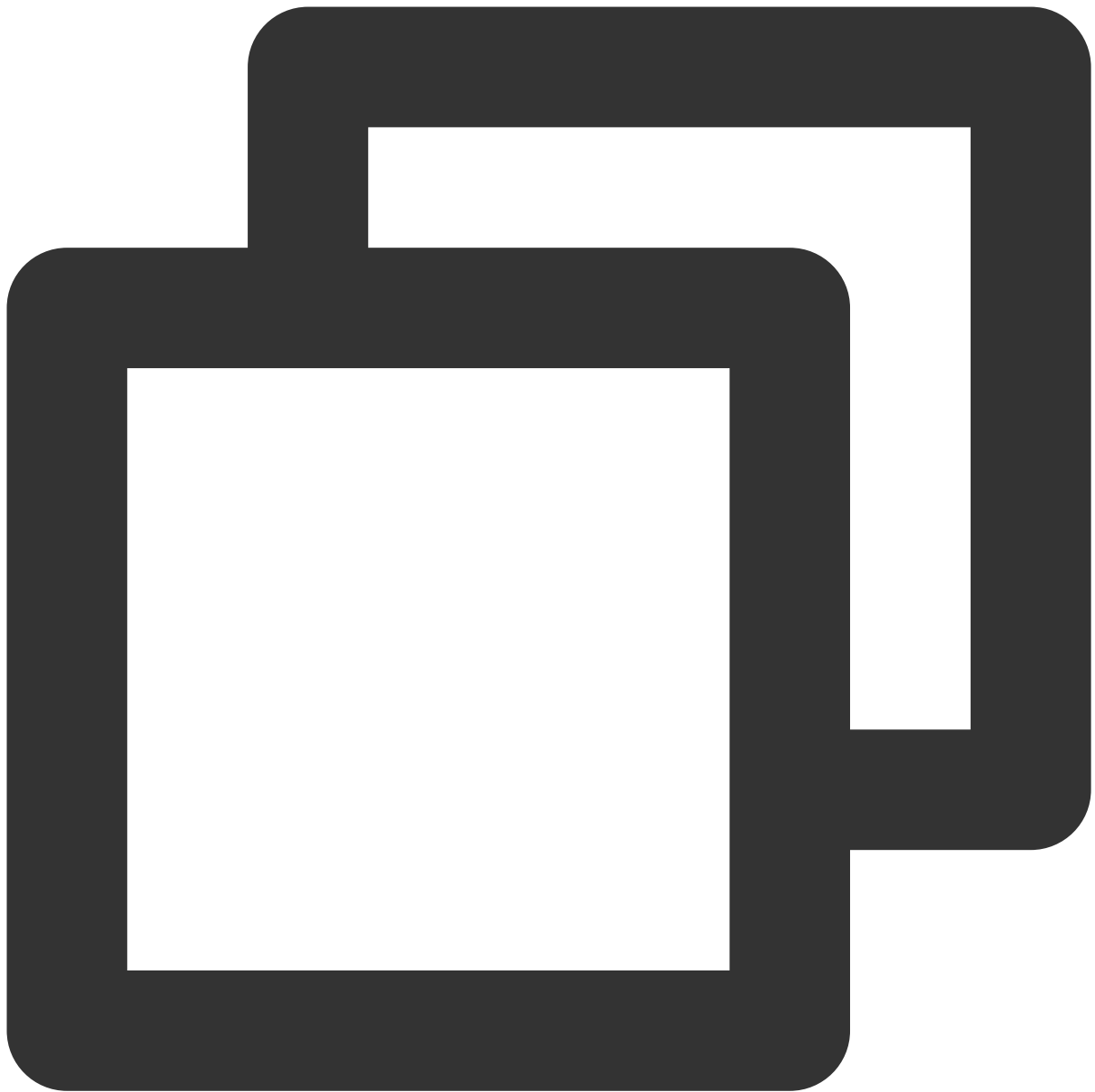
3. Run the following command to use VI editor to open the `/etc/fstab` file.



```
sudo vi /etc/fstab
```

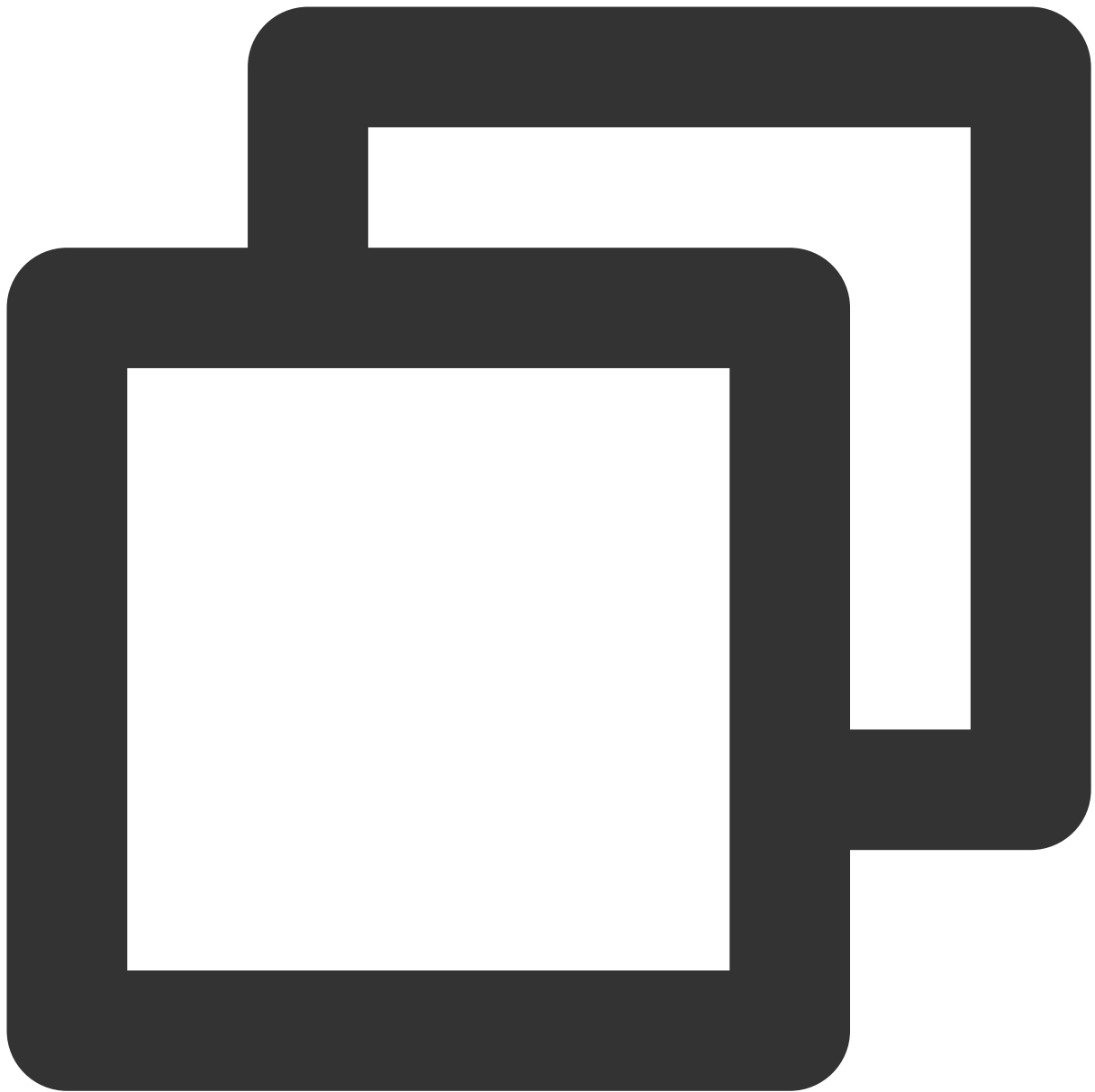
4. Press **i** to enter edit mode.

5. Move the cursor to the end of the file and press **Enter**, then add the following content.



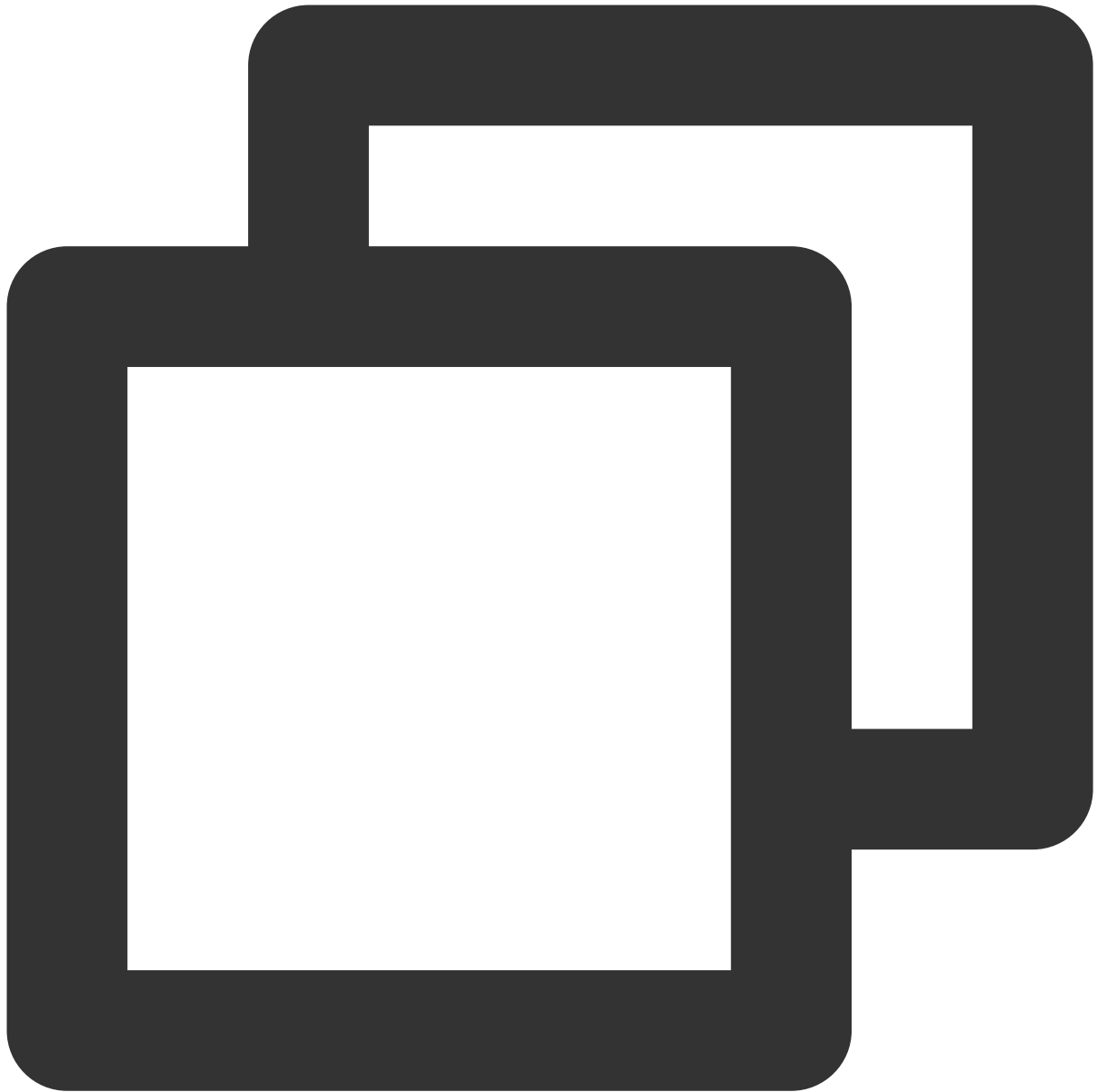
```
<Device information> <Mount point> <File system format> <File system installation o
```

(Recommended) Assume that you need to automatically mount a cloud disk by using a soft link:



```
/dev/disk/by-id/virtio-disk-xxxxx /data ext4 defaults 0 0
```

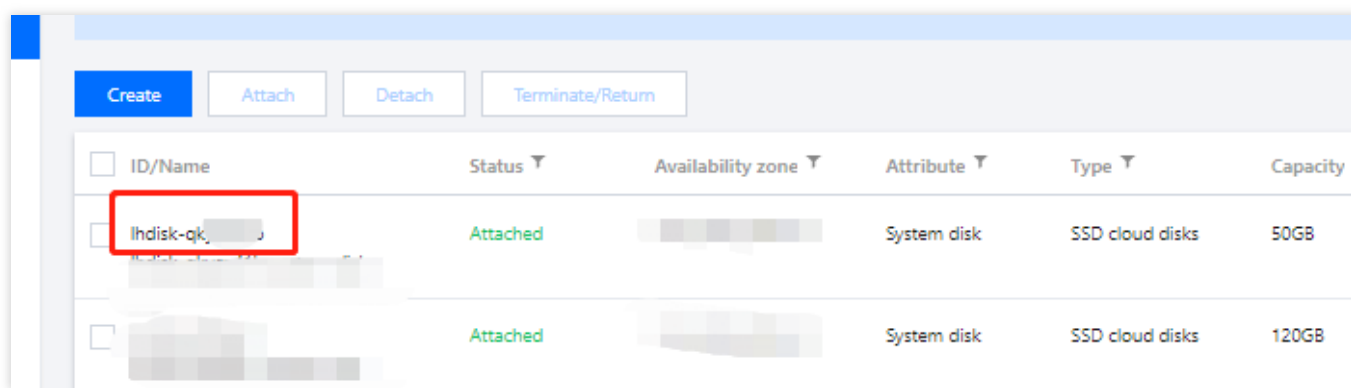
For mounting the partition, add the following content:



```
/dev/disk/by-id/virtio-disk-xxxxx-part1 /data/newpart ext4 defaults 0 2
```

**Note:**

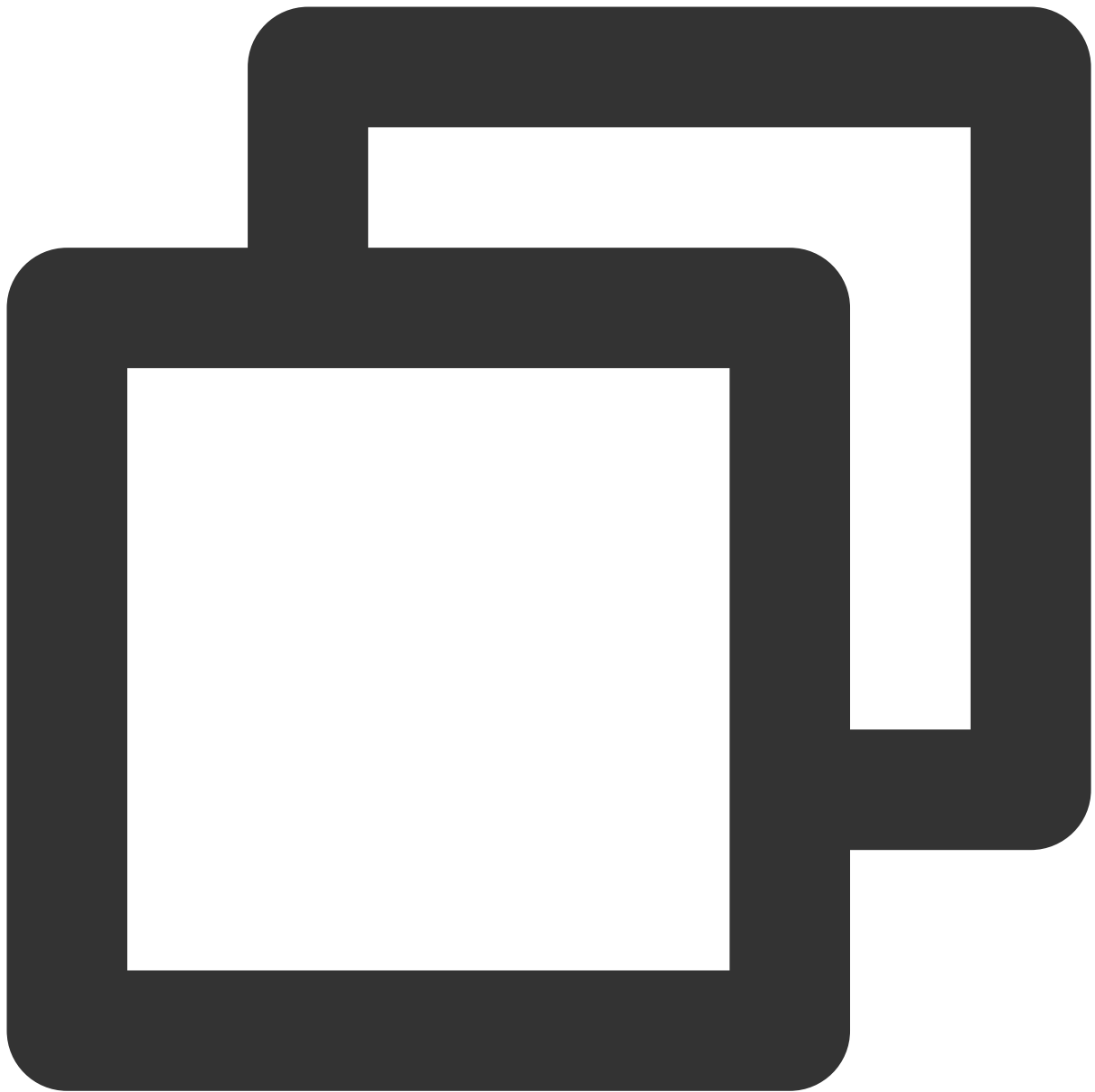
If you have multiple cloud disks, you can distinguish them by comparing the `xxxxx` in `virtio-disk-xxxxx` with the cloud disk ID `lhdisk-xxxxxx` in the console. The cloud disk ID in the console is shown below:



The screenshot shows the Tencent Cloud console interface for managing disks. At the top, there are four buttons: 'Create' (blue), 'Attach', 'Detach', and 'Terminate/Return'. Below these buttons is a table with the following columns: 'ID/Name', 'Status', 'Availability zone', 'Attribute', 'Type', and 'Capacity'. The table contains two rows of data. The first row is highlighted with a red box around the 'ID/Name' column, which contains the text 'lhdisk-qk...'. The 'Status' column for this row is 'Attached'. The 'Availability zone' column shows a blurred value. The 'Attribute' column is 'System disk', the 'Type' is 'SSD cloud disks', and the 'Capacity' is '50GB'. The second row is also highlighted with a red box around the 'ID/Name' column, which contains the text 'lhdisk-qk...'. The 'Status' column for this row is 'Attached'. The 'Availability zone' column shows a blurred value. The 'Attribute' column is 'System disk', the 'Type' is 'SSD cloud disks', and the 'Capacity' is '120GB'.

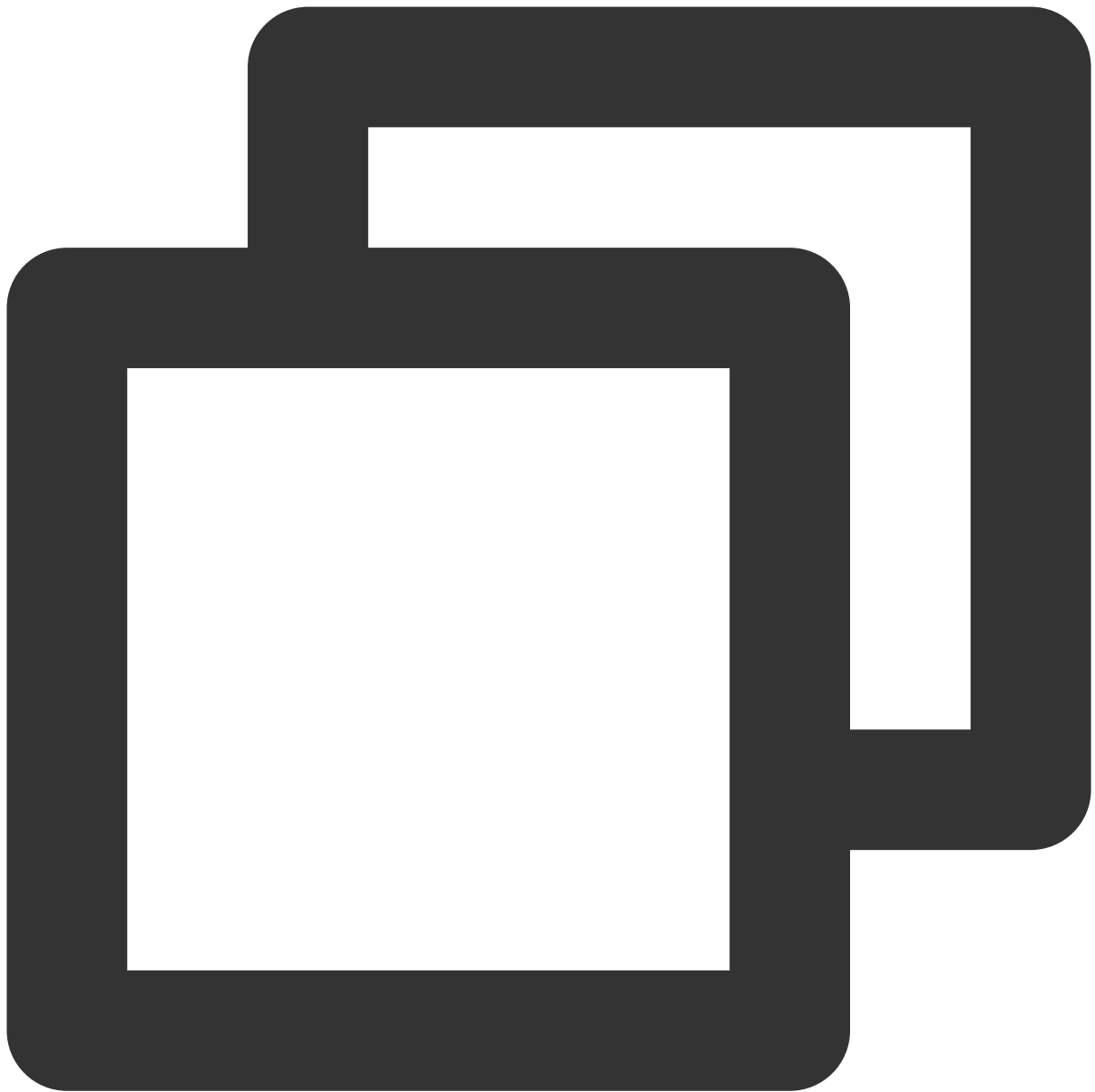
ID/Name	Status	Availability zone	Attribute	Type	Capacity
lhdisk-qk...	Attached		System disk	SSD cloud disks	50GB
lhdisk-qk...	Attached		System disk	SSD cloud disks	120GB

Take automatic mounting using the UUID of the disk partition as an example. Add the following content:



```
UUID=d489ca1c-5057-4536-81cb-ceb2847f9954 /data ext4 defaults 0 0
```

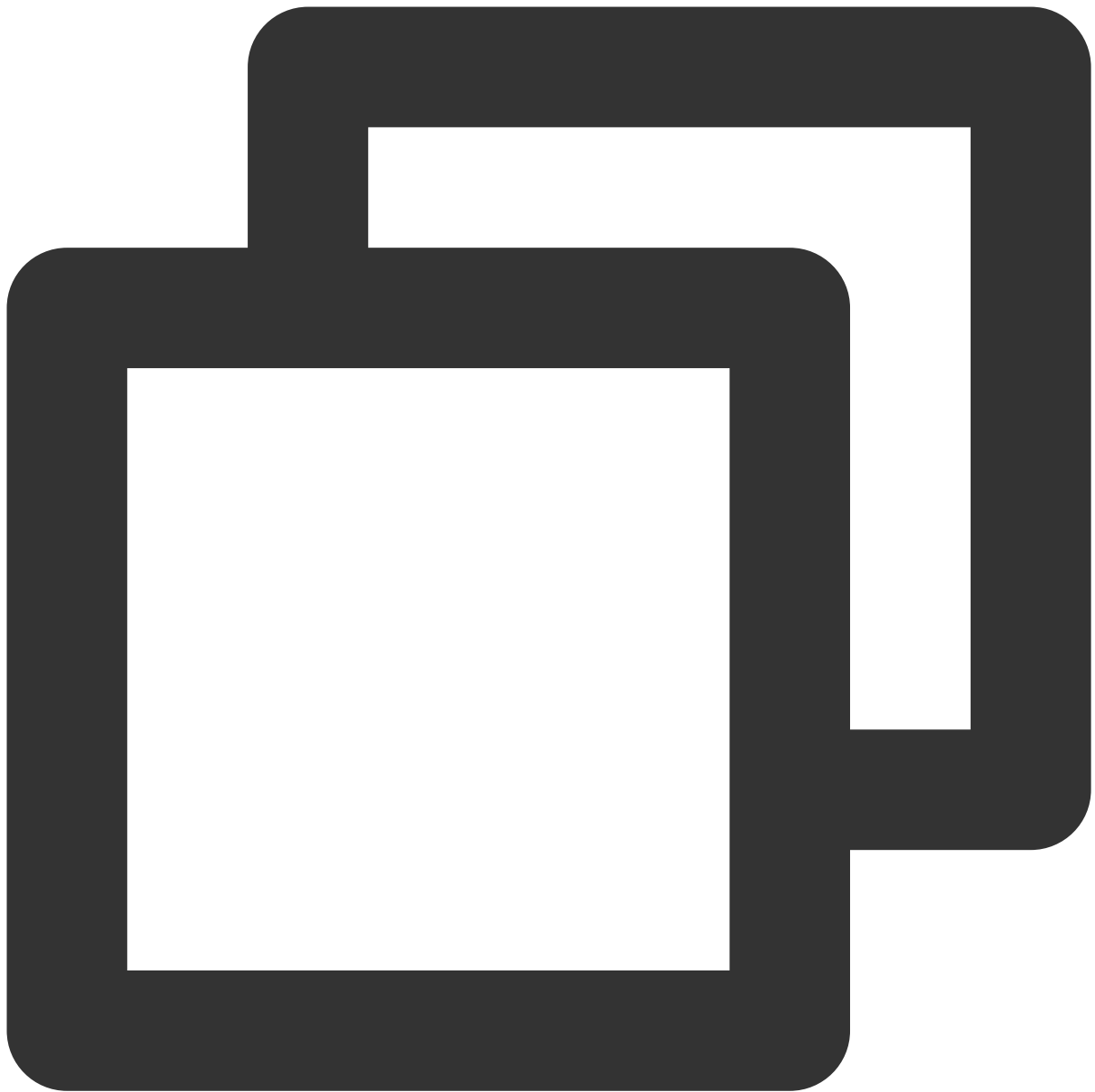
For mounting the partition, add the following content:



```
UUID=d489ca1c-5057-4536-81cb-ceb2847f9954 /data/newpart ext4 defaults 0 2
```

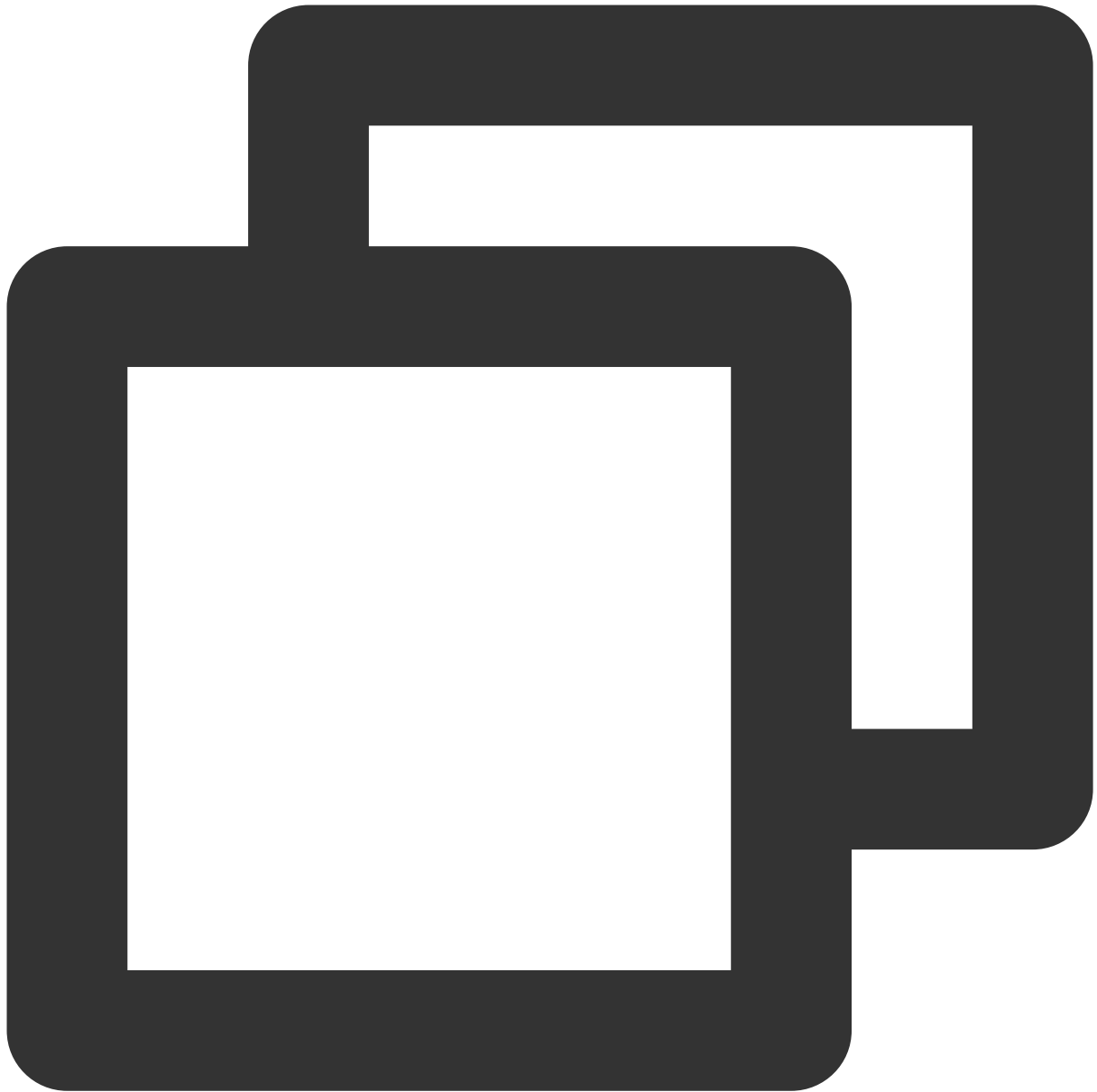
Take automatic mounting using the device name as an example. Add the following content:





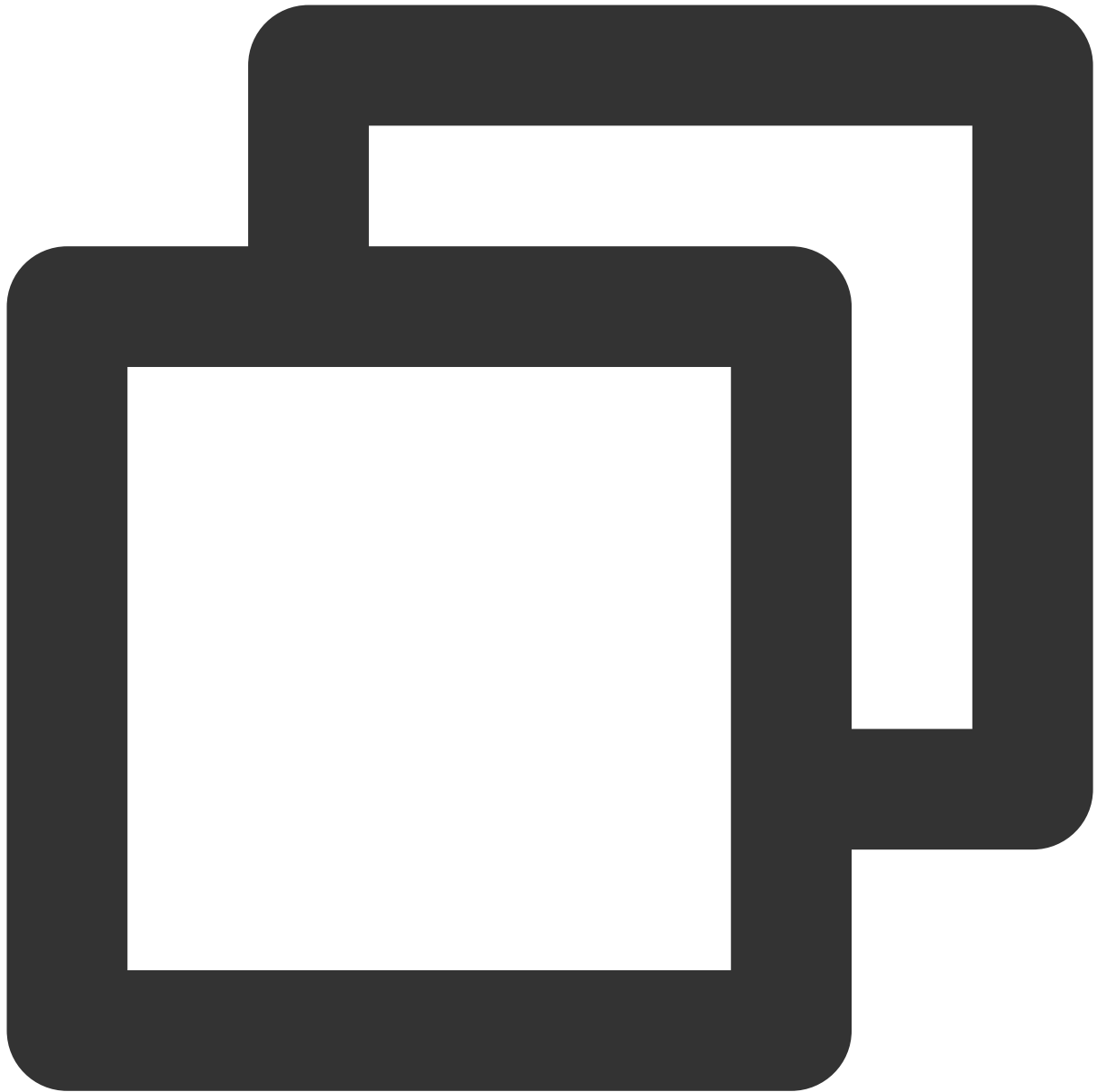
```
/dev/vdb /data ext4 defaults 0 0
```

For mounting the partition, add the following content:



```
/dev/vdb1 /data/newpart /data/newpart ext4 defaults 0 2
```

6. Press **Esc**, enter **:wq**, and press **Enter** to save the configuration and exit the editor.
7. Run the following command to check whether the **/etc/fstab** file has been written successfully.



```
sudo mount -a
```

If the command runs successfully, the file has been written. The newly created file system will automatically mount when the operating system starts up.

# Renewing Cloud Disks

Last updated : 2022-05-13 16:43:39

## Overview

This document describes how to manually renew cloud data disks or enable auto-renewal for them in the Lighthouse console.

## Directions

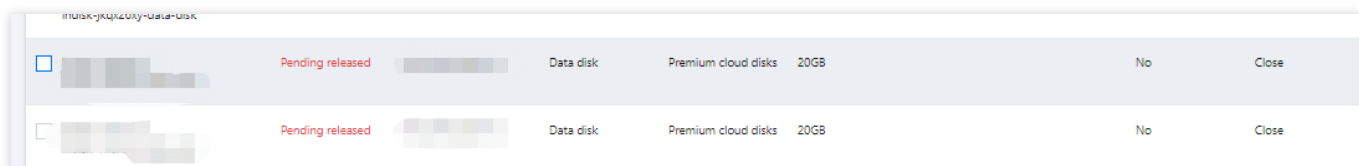
### Manual Renewal

You can choose the following renewal methods according to the cloud disk status:

Pending released instances

Unexpired cloud disks

1. Log in to the Lighthouse console and click **Cloud Disk** on the left sidebar.
2. Select a region at the top of the "Cloud disk" page, find the target cloud disk, and click **Renew** under the "Operation" column.



<input type="checkbox"/>	...	Pending released	...	Data disk	Premium cloud disks	20GB	No	Close
<input type="checkbox"/>	...	Pending released	...	Data disk	Premium cloud disks	20GB	No	Close

3. In the **Renew cloud disk** pop-up window, select the renewal period, click **OK**, and make the payment for the renewal order.

You can renew an unexpired cloud disk in the following methods:

### Renew on the cloud disk page

1. Log in to the Lighthouse console and click **Cloud Disk** on the left sidebar.
- . Select a region at the top of the **Cloud disk** page, find the target cloud disk, and click **Renew** under the **Operation** column.

<a href="#">Create</a> <a href="#">Attach</a> <a href="#">Detach</a> <a href="#">Terminate/Return</a>									
<input type="checkbox"/> ID/Name	Status	Availability zone	Attribute	Type	Capacity	Associated to	Released upon l...	Auto-renewal	Cr Ex
<input type="checkbox"/> [blurred]	Attached	[blurred]	System disk	SSD cloud disks	50GB	lhins-h8had2up SRS Video Server-8cAE	Yes	Close	Cr Ex
<input type="checkbox"/> [blurred]	Attached	[blurred]	System disk	SSD cloud disks	120GB	lhins-1zputg13 SRS Video Server-N70e	Yes	Close	Cr Ex
<input type="checkbox"/> [blurred]	Attached	[blurred]	System disk	SSD cloud disks	50GB	lhins-4x3dvfo7 SRS Video Server-K9o7	Yes	Close	Cr Ex
<input type="checkbox"/> [blurred]	Attached	[blurred]	System disk	SSD cloud disks	50GB	lhins-k41xbg9t CentOS-p01c	Yes	Close	Cr Ex
<input type="checkbox"/> [blurred]	To be attached	[blurred]	Data disk	Premium cloud disks	20GB		No	Close	Cr Ex
<input type="checkbox"/> [blurred]	To be attached	[blurred]	Data disk	Premium cloud disks	20GB		No	Close	Cr Ex

2. In the **Renew cloud disk** pop-up window, select the renewal period, click **OK**, and make the payment for the renewal order.

### Renew on the instance details page

1. Log in to the [Lighthouse console](#) and select the target instance and enter the details page.
2. Select the **Cloud disk** tab, find the target cloud disk, and click **Renew** under the **Operation** column.

<a href="#">Overview</a> <a href="#">Pre-installed application</a> <a href="#">Cloud disk</a> <a href="#">Firewall</a> <a href="#">SSH key pair</a> <a href="#">Snapshot</a> <a href="#">Monitoring</a>									
<a href="#">Attach cloud disk</a> <a href="#">Detach</a>									
<input type="checkbox"/> ID/Name	Status	Availability zone	Attribute	Type	Capacity	Released upon l...	Auto-renewal	Creation/Expiry time	Operatio
<input type="checkbox"/> [blurred]	Attached	[blurred]	System disk	SSD cloud disks	50GB	Yes	Close	Created at 2022-04-24 15:21:28 Expire at 2022-05-24 15:21:28	<a href="#">Renew</a>
<input type="checkbox"/> [blurred]	Attached	[blurred]	Data disk	Premium cloud disks	20GB	No	Enable	Created at 2022-04-21 14:36:02 Expire at 2022-07-21 14:36:02	<a href="#">Renew</a>
Total items: 2						20 / page			

3. In the **Renew cloud disk** pop-up window, select the renewal period, click **OK**, and make the payment for the renewal order.

### Auto-Renewal

It's recommended that you enable the auto-renewal to prevent the cloud disks from being returned or terminated due to overdue payment. The methods for enabling the auto-renewal are as follows:

#### Note:

When the auto-renewal is enabled, the cost of the next billing cycle will be deducted from your sufficient account balance upon the expiry date of the cloud disk.

Cloud disk page

Instance details page

1. Log in to the Lighthouse console and click [Cloud Disk](#) on the left sidebar.

2. Select a region at the top of the **Cloud disk** page, find the target cloud disk, and click **More > Enable auto-renewal** under the "Operation" column.

<input type="checkbox"/>		Attached		Data disk	Premium cloud disks	20GB	<a href="#">lhm-9wlc8d9</a> Cloudreve-GZRu-2	No	Enable	Created at 2022-04-21 09:39:32 Expire at 2022-08-21 09:39:32
<input type="checkbox"/>		To be attached		Data disk	SSD cloud disks	20GB		No	Close	Created at 2022-04-21 09:37:02 Expire at 2022-08-09 09:37:02
<input type="checkbox"/>		Attached		System disk	SSD cloud disks	50GB	<a href="#">lhm-9wlc8d9</a> Cloudreve-GZRu-2	Yes	Close	Created at 2022-04-14 16:52:37 Expire at 2022-05-14 16:52:37

3. Click **OK** in the pop-up window.

1. Log in to the [Lighthouse console](#) and select the target instance and enter the details page.
2. Select the **Cloud disk** tab, find the target cloud disk, and click **More > Enable auto-renewal** under the **Operation** column.

Overview

Pre-installed application

Cloud disk

Firewall

SSH key pair

Snapshot

Monitoring

Attach cloud disk

Detach

<input type="checkbox"/>	ID/Name	Status	Availability zone	Attribute	Type	Capacity	Released upon L...	Auto-renewal	Creation/Expiry time
<input type="checkbox"/>		Attached		System disk	SSD cloud disks	50GB	Yes	Close	Created at 2022-04-24 15:21:28 Expire at 2022-05-24 15:21:28
<input type="checkbox"/>		Attached		Data disk	Premium cloud disks	20GB	No	Enable	Created at 2022-04-21 14:36:02 Expire at 2022-07-21 14:36:02

Total items: 2

20 / page

H

A

3. Click **OK** in the pop-up window.

# Detaching Cloud Disks

Last updated : 2022-05-13 16:43:39

## Overview

You can detach a cloud disk used as a data disk from a Lighthouse instance and reattach it to another Lighthouse instance. This document describes how to detach a cloud disk in the Lighthouse console. Note that **detaching a cloud disk will not clear the disk data**.

## Considerations

Only cloud disks that are used as data disks can be detached, and the system disks cannot be detached.

It's recommended that you run the `umount` command (for Linux instances) or make the cloud disk offline (for Windows instances) before detaching the disk. Otherwise, the cloud disk may not be recognized when it's reattached to the Lighthouse instance.

## Directions

### Preparations

You need to run the `umount` command (for Linux instances) or make the cloud disk offline (for Windows instances) before detaching the disk.

Windows instances

Linux instances

To prevent data loss, we recommend that you suspend read and write operations on all file systems of the disk.

Otherwise, data that has not been read or written will be lost.

When detaching a cloud disk, you must first set the disk to offline status. Otherwise, you may not be able to reattach the cloud disk unless you restart the Lighthouse instance.

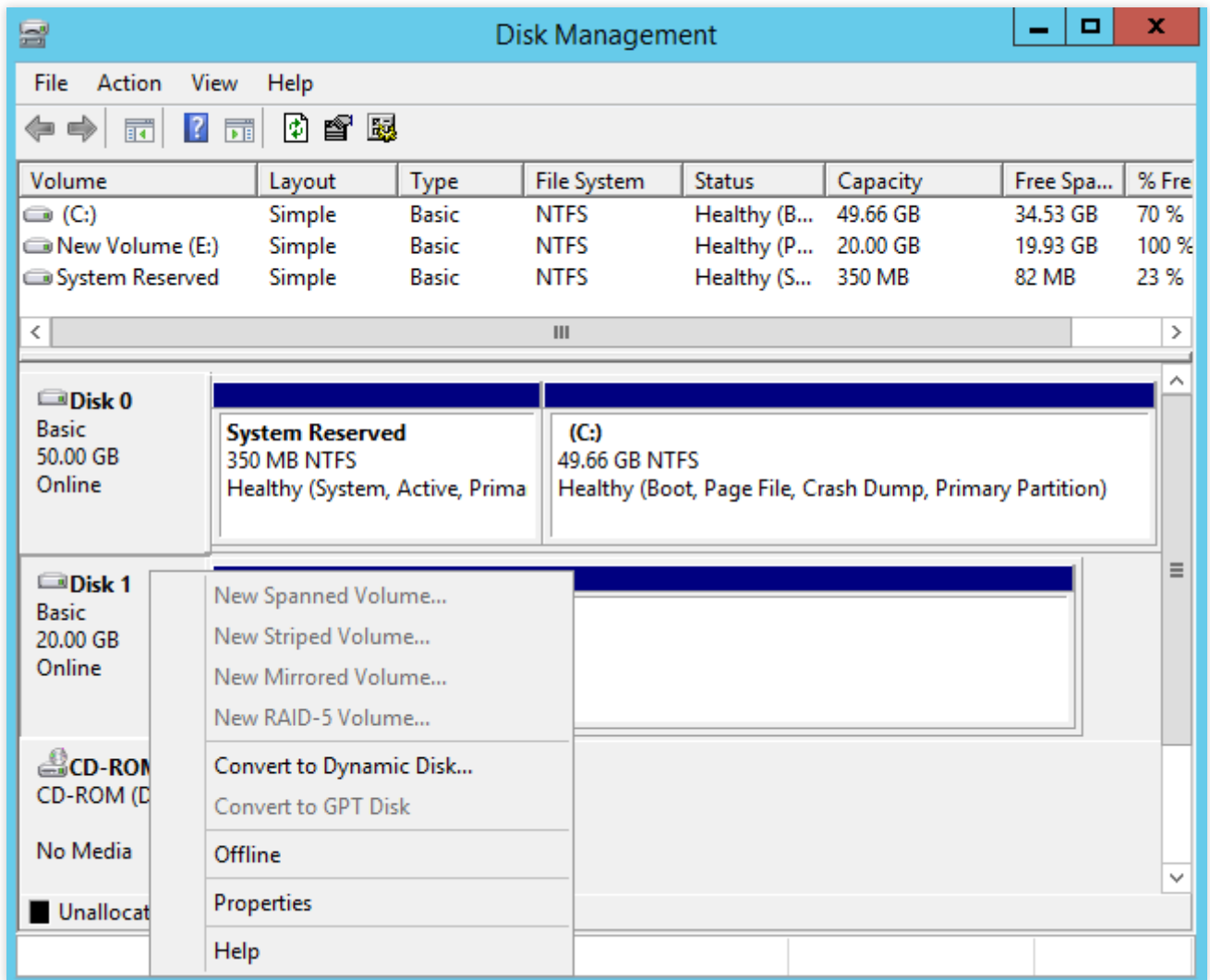
Perform the following operations:

1. Log in to the Lighthouse instance. For more information, see [Logging In to a Windows Instance via VNC](#).
2. Right-click



on the lower left corner of the desktop, and select **Disk management** in the pop-up menu.

3. In the **Disk management** window, right-click the Disk 1 area and select **Offline** from the menu list.



If you detach the disk directly from the console without running the `umount` , the problem shown below may occur upon the instance shutdown or start-up:



```
Checking filesystems
/dev/vda1: clean, 35630/524288 files, 335690/2096474 blocks
fsck.ext3: Unable to resolve 'UUID=dabe8ee8-221b-44c7-9074-4d3f8fc4ae44'
fsck.ext3: No such file or directory while trying to open /dev/disk/by-id/virtio-disk-ezy5q5l6-part5
/dev/disk/by-id/virtio-disk-ezy5q5l6-part5:
The superblock could not be read or does not describe a correct ext2
filesystem. If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]

*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

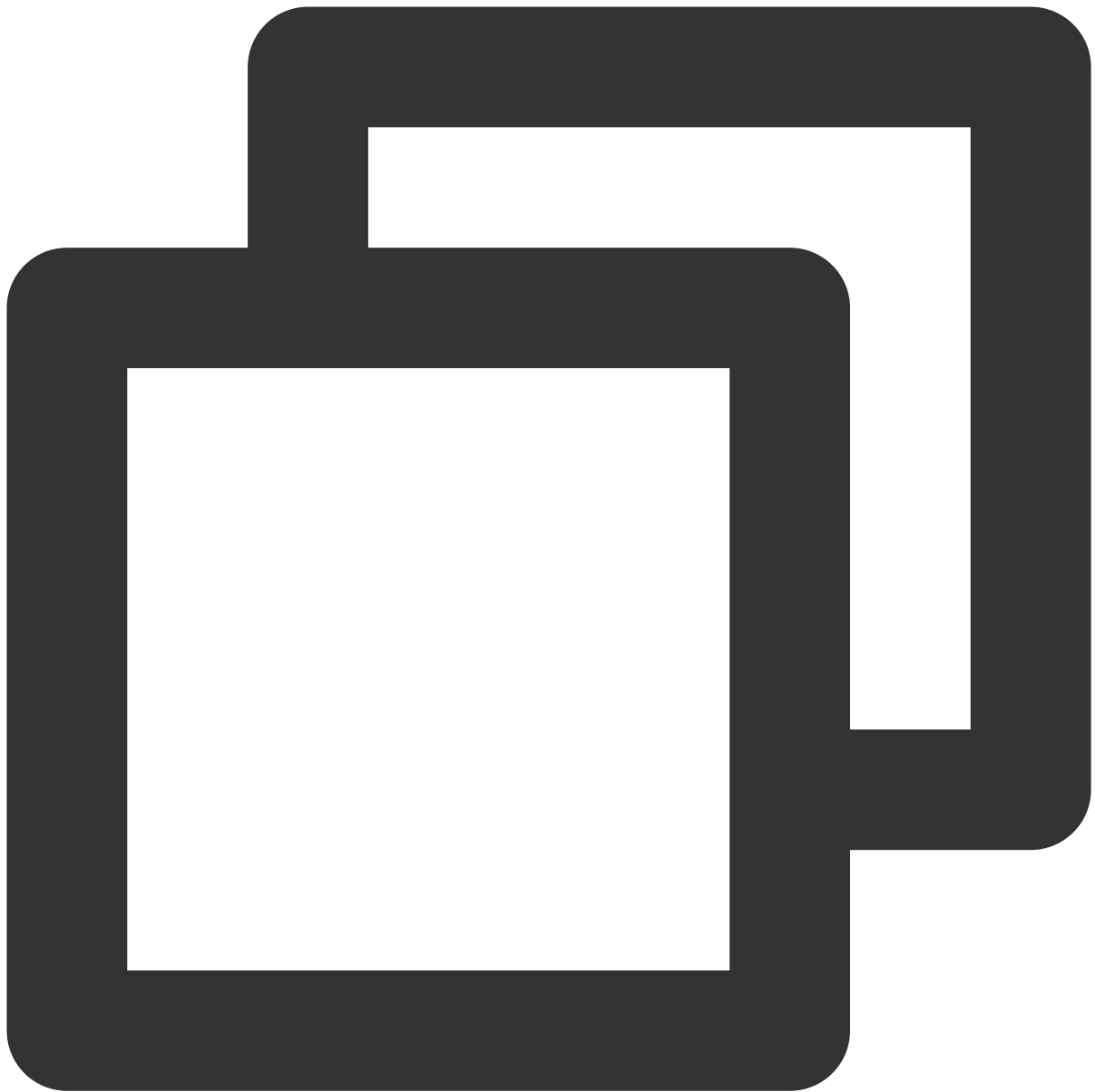
If you have enabled the auto-attaching, please modify the `/etc/fstab` file to prevent the disk from being attached automatically when the instance starts up again.

[Log in to the Lighthouse instance](#), and run the `sudo umount <mount point>` command to detach the cloud disk.

If you have created a Logical Volume Manager (LVM) in a Lighthouse instance, detaching the disk directly in the console without run the `umount` command may cause some device data to remain in memory. A system error occurs when an application inside the instance attempts to traverse or access the device.

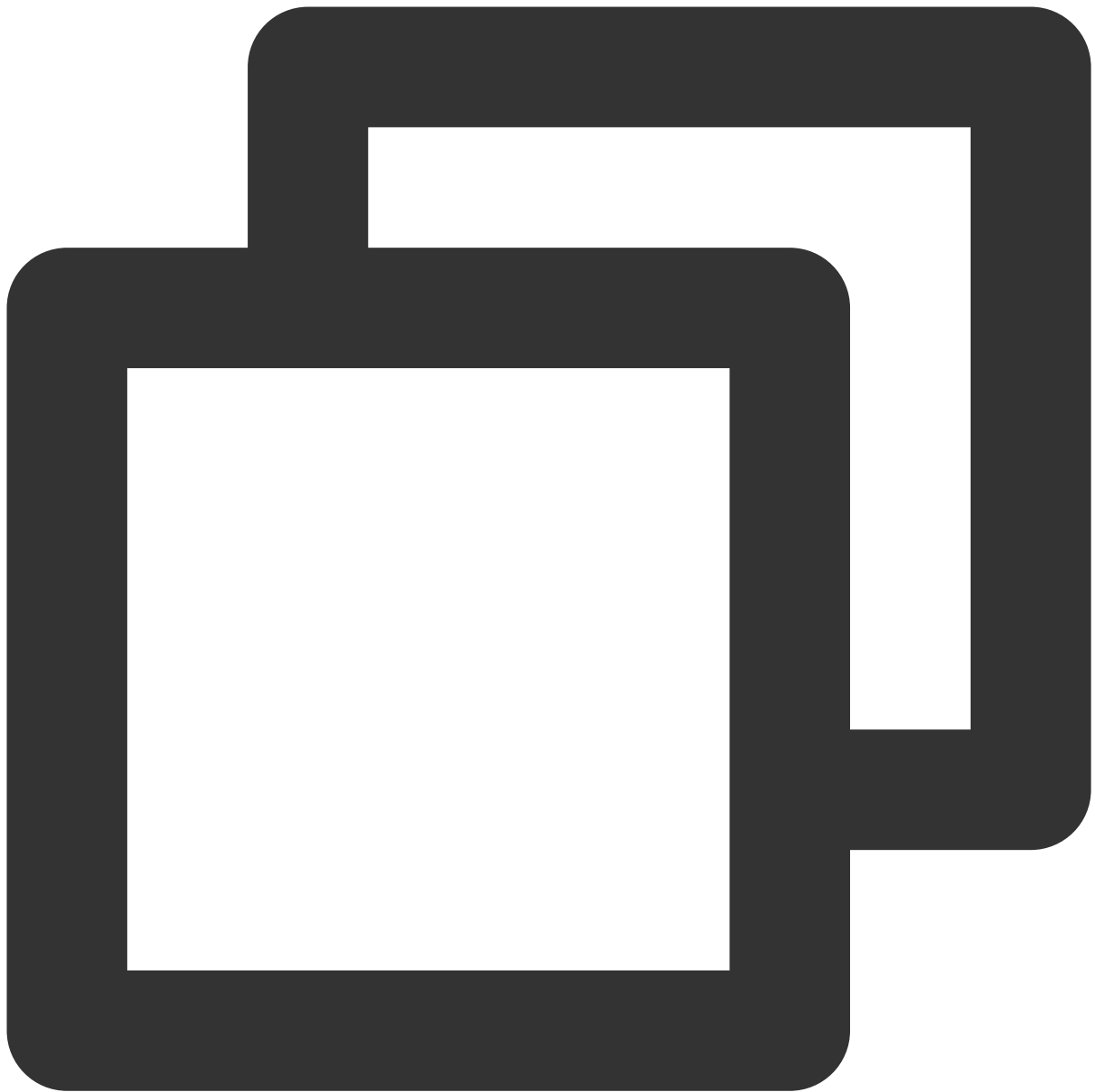
Assume that you have created a logical volume `/dev/test/lv1` based on `/dev/vdb1` and mounted it into the `/data` directory. Then, do the following:

1.1 Run the following command to unmount the disk mount point.



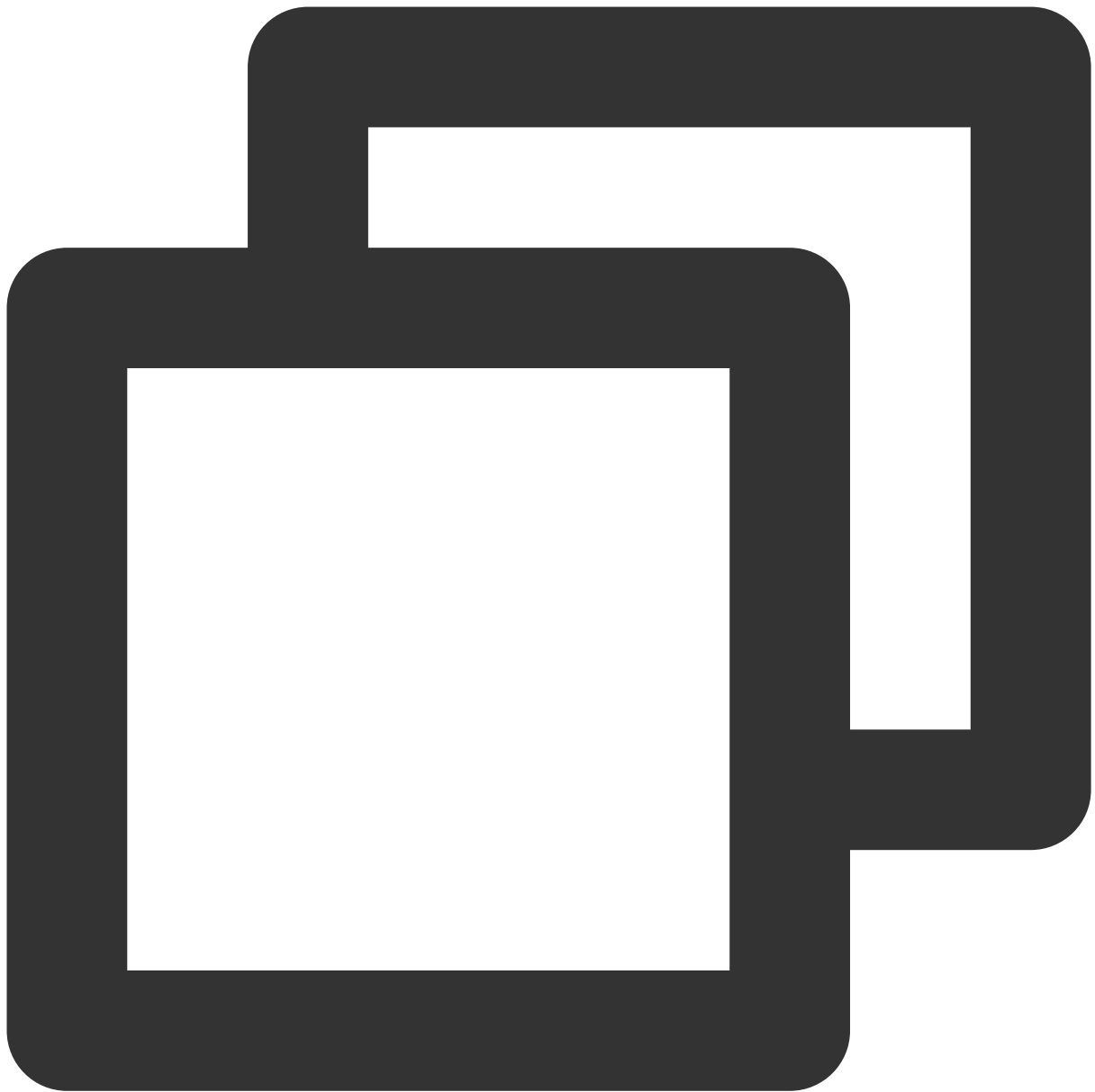
```
sudo umount /data
```

1.2 Run the following command to remove the Logical Volume (LV). If there are multiple LVs, remove all LVs in sequence.



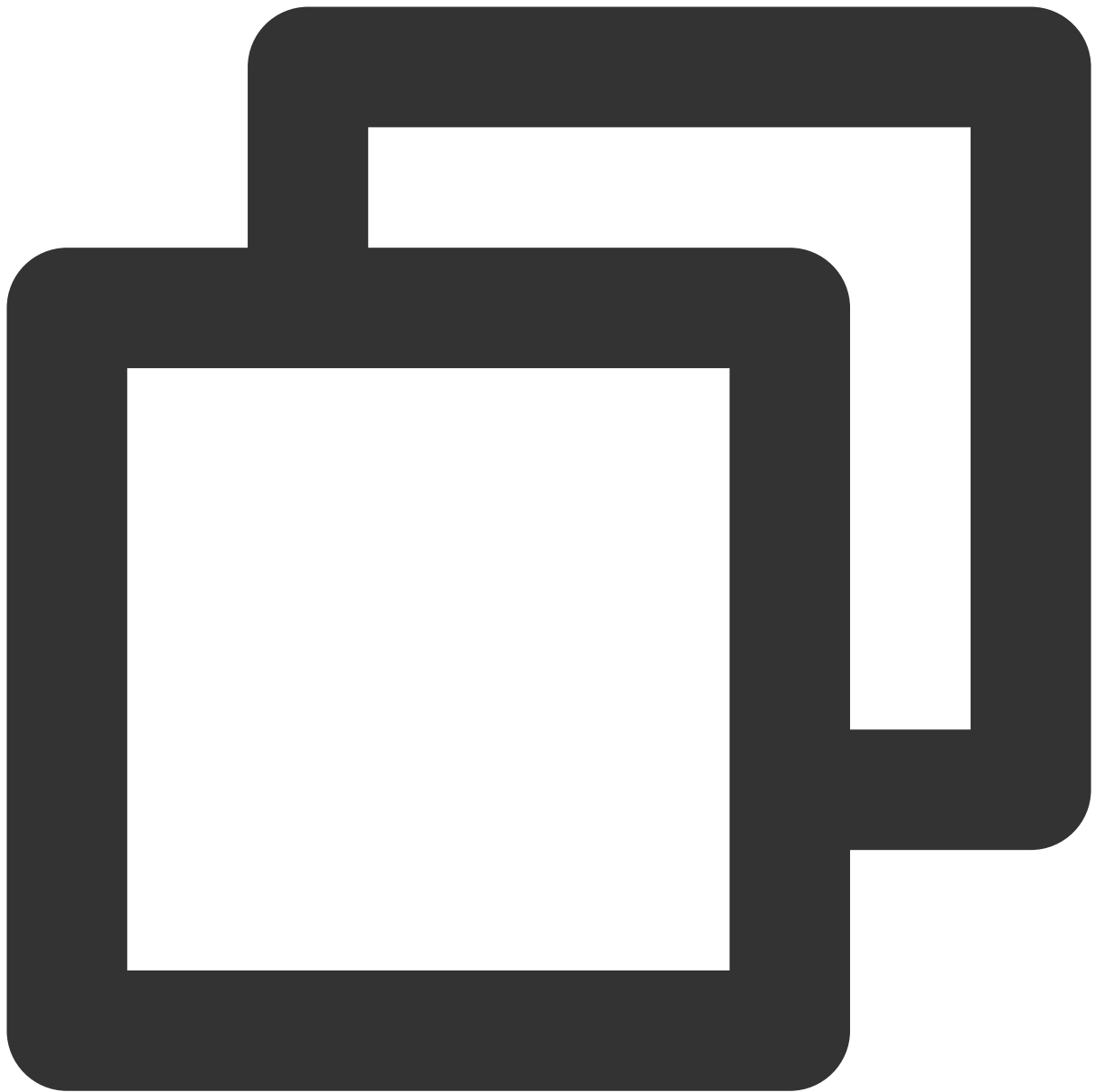
```
sudo lvremove /dev/test/lv1
```

1.3 Run the following command to remove the volume group.



```
sudo vgremove test
```

1.4 Run the following command to remove the physical volume.



```
sudo pvremove /dev/vdb1
```

## Detaching the cloud disks in the console

You can detach the cloud disks in the following ways:

Detach on the cloud disk page

Detach on the instance details page

1. Log in to the Lighthouse console and click **Cloud Disk** on the left sidebar.
2. Select a region at the top of the **Cloud disk** page, find the target cloud disk, and click **More > Detach**.

<input type="checkbox"/>		Attached		Data disk	Premium cloud disks	20GB	<a href="#">lhrs-9wlo9d9</a> Cloudreve-GZRU-2	No	Enable	Created at 20 Expire at 2021
<input type="checkbox"/>		To be attached		Data disk	SSD cloud disks	20GB		No	Close	Created at 20 Expire at 2021
<input type="checkbox"/>		Attached		System disk	SSD cloud disks	50GB	<a href="#">lhrs-9wlo9d9</a> Cloudreve-GZRU-2	Yes	Close	Created at 20 Expire at 2021

To detach multiple cloud disks at the same time, select the target cloud disks, and click **Detach** at the top of the page.

3. In the pop-up **Detach cloud disks** window, confirm the information and click **OK**.

Once detached, the cloud disks go to **To be attached** status.

1. Log in to the [Lighthouse console](#) and select the target instance and enter the details page.

2. Select the **Cloud disk** tab, find the target cloud disk, and click **More > Detach** under the "Operation" column.

Overview

Pre-installed application

Cloud disk

Firewall

SSH key pair

Snapshot

Monitoring

Attach cloud disk

Detach

<input type="checkbox"/>	ID/Name	Status	Availability zone	Attribute	Type	Capacity	Released upon i...	Auto-renewal	Creation/Expiry time	Ops
<input type="checkbox"/>		Attached		System disk	SSD cloud disks	50GB	Yes	Close	Created at 2022-04-24 15:21:28 Expire at 2022-05-24 15:21:28	Re
<input type="checkbox"/>		Attached		Data disk	Premium cloud disks	20GB	No	Enable	Created at 2022-04-21 14:36:02 Expire at 2022-07-21 14:36:02	Re

Total items: 2

20

/ page

H

◀

1

To detach multiple cloud disks at the same time, select the target cloud disks, and click **Detach** at the top of the page.

3. In the pop-up **Detach cloud disks** window, confirm the information and click **OK**.

After the detachment is successful, you cannot see the disk in the **Cloud disk** tab of the instance. You can view that the cloud disk status is "To be attached" on the [Cloud Disk](#) page.

# Terminating Cloud Disks

Last updated : 2022-05-13 16:43:39

## Overview

When a cloud disk is no longer in use and important data has been backed up, you can release the virtual resources by terminating the cloud disk. You will not be billed for the cloud disk after termination. **When the cloud disk is terminated, all data on the cloud disk will be deleted and cannot be restored. Please note that cloud disks that have been terminated cannot be recovered.** This document describes how to terminate the data disks in the Lighthouse console.

Cloud disks have different life cycles as system disks and data disks. They can be terminated in the following ways:

Data disk

System disk

The lifecycle of the cloud disk used as a data disk is independent of that of the Lighthouse instance, so the disk can be terminated independently. You can choose to terminate the cloud disk by yourself or enable auto-termination.

**Manual termination:** The cloud disks can be manually terminated before expiry. After being terminated, the cloud disks will be kept in the recycle bin for seven days, and they can be permanently terminated in the recycle bin.

Each entity can return one cloud disk within five days without reason. Each account can also do returns for 199 cloud disks. For more information on refunds, see [Refund](#). When you hit the return limit, you will not be able to manually terminate the cloud disks.

**Automatic termination** A cloud disk in the recycle bin will be automatically terminated if it is not recovered within 7 days. To continue the use, renew the disk within the specified time. For renewal, see [Renewing a Cloud Disk](#).

The lifecycle of a cloud disk used as a system disk is the same as the Lighthouse instance. It can only be terminated when the Lighthouse instance is terminated. For more information, see [Terminating an instance](#).

## Prerequisites

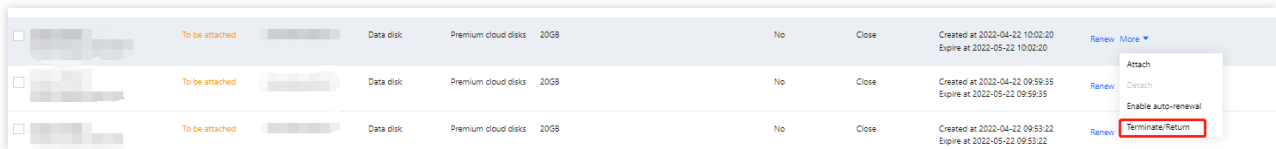
The cloud disks are in **To be attached** status. To terminate the "Attached" cloud disks, you need to detach them first. See [Detaching a Cloud Disk](#).

The important data has been backed up.

## Directions

### Terminate unexpired cloud disks manually

1. Log in to the Lighthouse console and click **Cloud Disk** on the left sidebar.
2. Select a region at the top of the **Cloud Disk** page, find the target cloud disk, and click **More > Terminate/Return**.



<input type="checkbox"/>	To be attached	Data disk	Premium cloud disks	20GB	No	Close	Created at 2022-04-22 10:02:20 Expire at 2022-05-22 10:02:20	Renew More ▾
<input type="checkbox"/>	To be attached	Data disk	Premium cloud disks	20GB	No	Close	Created at 2022-04-22 09:59:35 Expire at 2022-05-22 09:59:35	Renew Attach
<input type="checkbox"/>	To be attached	Data disk	Premium cloud disks	20GB	No	Close	Created at 2022-04-22 09:53:22 Expire at 2022-05-22 09:53:22	Renew Enable auto-renewal Terminate/Return

To terminate multiple cloud disks at the same time, select the target disks and click **Terminate/Return** at the top of the page.

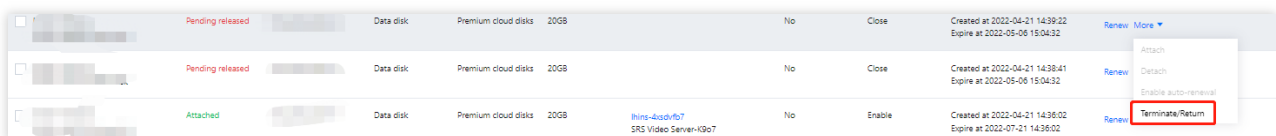
3. In the **Terminate/Return Cloud Disks** pop-up window, check **I have read and agree to Refund Policy**, and click **OK**.
4. On the refund information page, confirm the refund information and click **Confirm Refund**.

**Note:**

After termination, the cloud disk is in **Pending released** status and will be kept for seven days. At this time, the cloud disk is no longer available. If you don't need to retain the disk data, you can completely terminate the disk.

**Terminate cloud disks completely**

1. On the "Cloud Disk" page, select the cloud disk in "Pending released" status, click **More > Terminate/Return** under the operation column.



<input type="checkbox"/>	Pending released	Data disk	Premium cloud disks	20GB	No	Close	Created at 2022-04-21 14:39:22 Expire at 2022-05-06 15:04:32	Renew More ▾
<input type="checkbox"/>	Pending released	Data disk	Premium cloud disks	20GB	No	Close	Created at 2022-04-21 14:38:41 Expire at 2022-05-06 15:04:32	Renew Detach
<input type="checkbox"/>	Attached	Data disk	Premium cloud disks	20GB	No	Enable	Created at 2022-04-21 14:36:02 Expire at 2022-07-21 14:36:02	Renew Enable auto-renewal Terminate/Return

To terminate multiple cloud disks at the same time, select the target disks and click **Terminate/Return** at the top of the page.

2. In the **Terminate/Return Cloud Disks** pop-up window, click **OK** to completely terminate the cloud disk.

**Note:**

When a cloud disk is completely terminated, all data on the disk will be deleted and cannot be recovered. Cloud disks that have been terminated cannot be restored.



# Managing Keys

Last updated : 2022-04-06 14:31:47

## Overview

Currently, Lighthouse provides two types of user credentials for remote instance login: password and SSH key pair. The latter is a more secure and convenient for login authentication. It is a pair of public and private keys generated by an encryption algorithm and can be bound to a created instance. Then, you can use the private key to log in to the instance.

### Note:

The SSH key pair login method is applicable to Linux instances only.

## Strengths

An SSH key pair has the following strengths compared with a username and password:

**Security:** compared with general password login, an SSH key pair has a higher security and cannot be cracked with brute force. It is generated by using an asymmetric encryption algorithm and encrypted with a public key. Then, it can be decrypted only with the corresponding private key stored by yourself without being sent over the network.

**Convenience:** you can quickly log in to a Linux instance remotely by using an SSH key pair without entering the password each time. In addition, you can also maintain and manage multiple Linux instances more easily in a unified manner in this way.

## Use Limits

Up to **ten** SSH key pairs can be created in each region under one account.

## Directions

### Creating SSH key

1. Log in to the Lighthouse console and click **Key** on the left sidebar.
2. On the key list page, click **New**.
3. In the **Create an SSH key** pop-up window, set the key region, select the key creation method, and click **OK**.

### Note:

The private key will be automatically downloaded after the creation is completed. Tencent Cloud will not save your private key information. Download and get the private key within 10 minutes after key creation. You can download the key only once. Keep it confidential.

**Create an SSH key**

Region: Hong Kong, China Singapore Tokyo  
Silicon Valley Frankfurt Mumbai

Creation Method: ☒ Create a key pair ☐ Use an existing public key

Key Name:   
Enter 1-25 English letters, numbers and underlines

**i** Once created, the private key will be automatically downloaded and can only be downloaded once. You need to keep it safe. Tencent Cloud will not keep your private key.

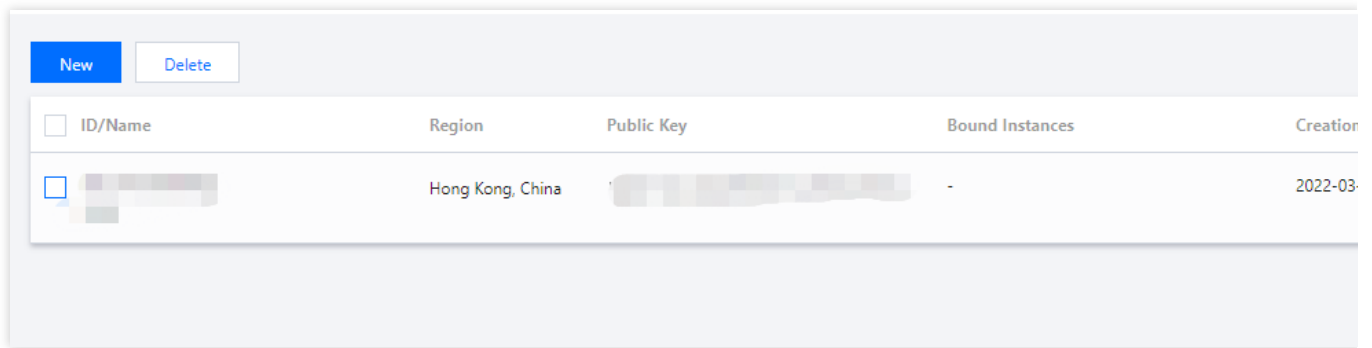
OK Close

If you select **Create a key pair** as the creation method, enter the key name.

If you select **Use an existing public key** as the creation method, enter the key name and existing public key information.

## Binding/Unbinding key to/from instance

1. Log in to the [Lighthouse console](#).
2. Click **Key List** on the left sidebar.
3. On the key list page, select the target SSH key and click **Bind/Unbind Instances**.



<input type="button" value="New"/>		<input type="button" value="Delete"/>		
<input type="checkbox"/> ID/Name	Region	Public Key	Bound Instances	Creation Time
<input checked="" type="checkbox"/> [redacted]	Hong Kong, China	[redacted]	-	2022-03-

4. In the **Bind/Unbind Instances** pop-up window, select the target Linux instance and click **OK**.

#### Note:

When you bind/unbind an instance, if the selected instance is running, pay attention to the following:

During the binding/unbinding process, the instance will shut down first and then start up, and the business will be interrupted momentarily. We recommend you do so during off-peak hours.

If the instance fails to shut down normally, it will be forced to shut down. Forced shutdown may cause data losses or file system corruption. Therefore, perform forced shutdown with caution.

Forced shutdown may take a while. Please be patient.

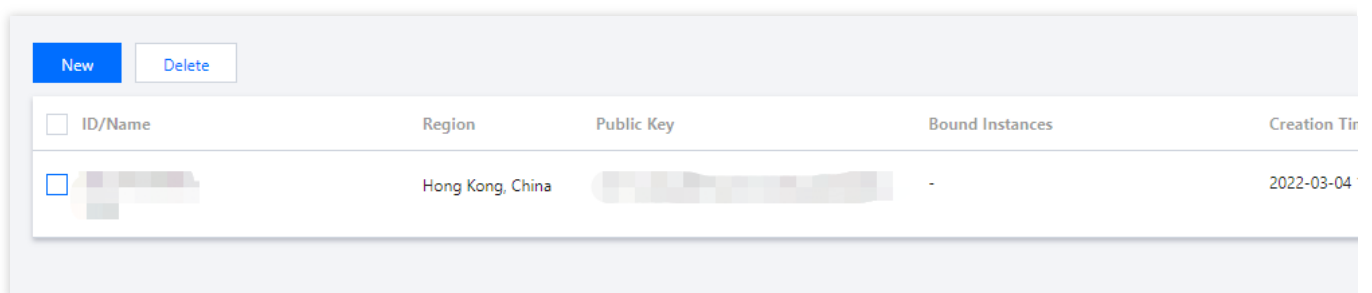
To improve the Lighthouse instance security, after a Linux instance is bound to a key, login to the `root` account with a password will be forbidden by default. If you want to keep the password login method, modify the configuration as instructed in [Modifying SSH configuration](#).

## Deleting SSH key

#### Note:

If an SSH key is bound to a Linux instance, it cannot be deleted.

1. Log in to the [Lighthouse console](#).
2. Click **Key List** on the left sidebar.
3. On the key list page, select the target SSH key and click **Delete**.



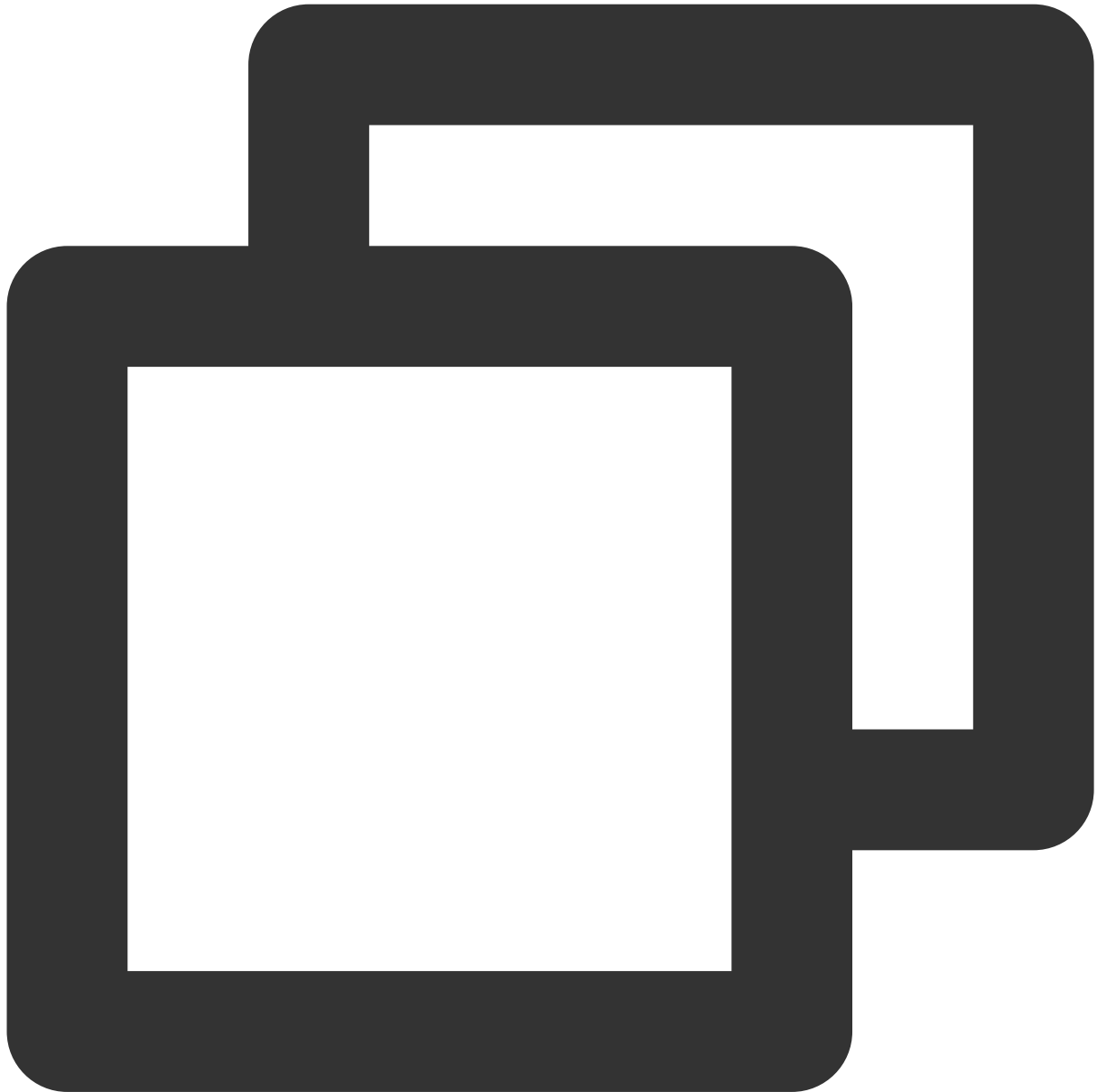
<input type="button" value="New"/>		<input type="button" value="Delete"/>		
<input type="checkbox"/> ID/Name	Region	Public Key	Bound Instances	Creation Time
<input checked="" type="checkbox"/> [redacted]	Hong Kong, China	[redacted]	-	2022-03-04

4. In the key deletion pop-up window, click **OK**.

## Relevant Operations

## Modifying SSH configuration

1. Log in to the target Linux instance via WebShell. You can also use other login methods as needed.
2. Run the following command to open the `sshd_config` configuration file:



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

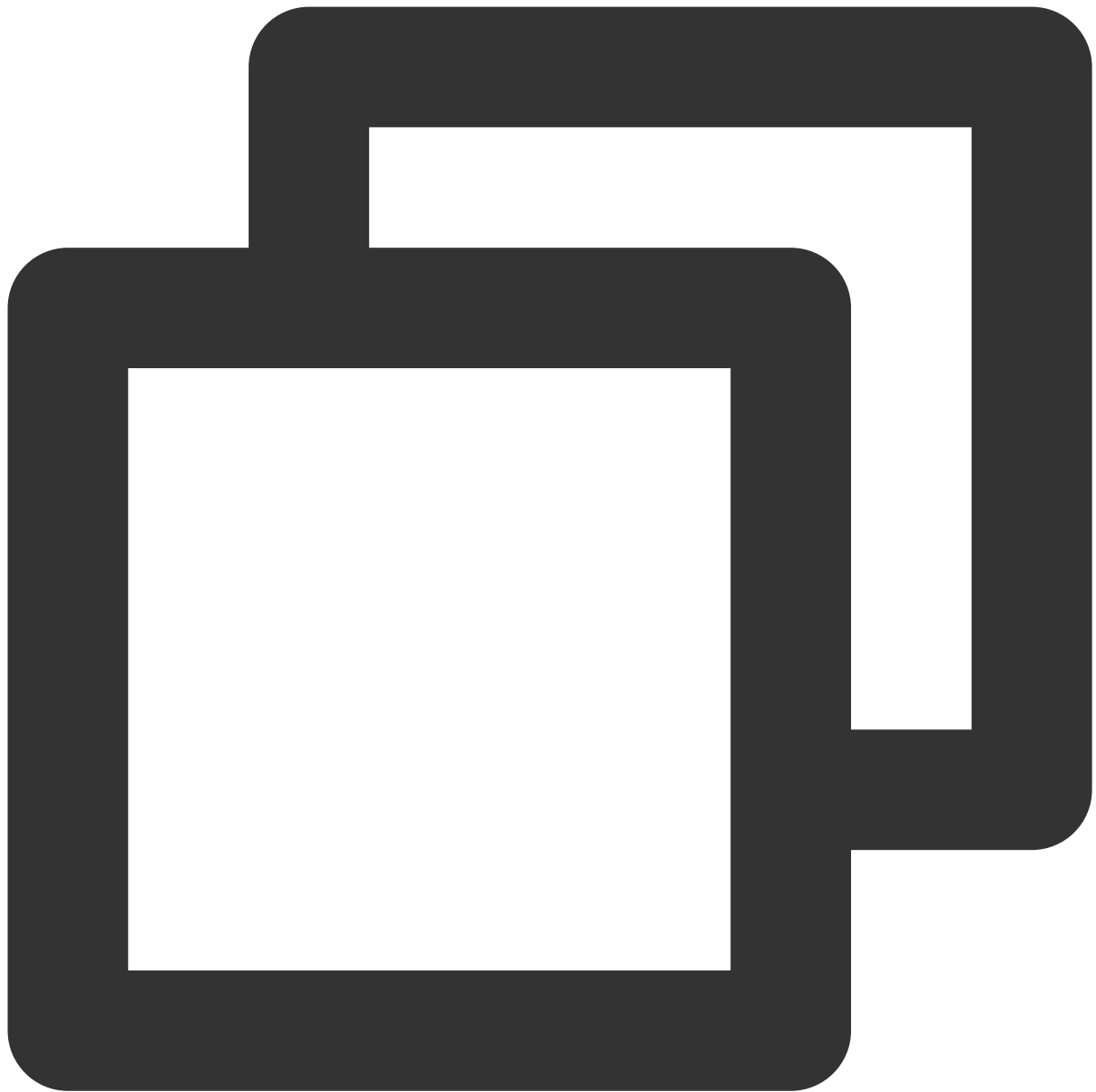
3. Press **i** to switch to the edit mode, find `#Authentication` , and change the value of the `PasswordAuthentication` parameter to `yes` as shown below:

**Note:**

If the `sshd_config` configuration file doesn't contain this configuration item, add `PasswordAuthentication` `yes` .

```
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin yes
PasswordAuthentication yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

4. Run the following command to restart the SSH service. This document uses CentOS 7 as an example. Run the applicable command based on your actual operating system.



```
sudo systemctl restart sshd
```

After the restart, you can try logging in with a password.

# Managing Firewall

## Manage instance firewall

Last updated : 2023-12-06 11:38:46

### Overview

A firewall is an important method to protect the Lighthouse instance's network security. Its security protection features are equivalent to security groups in CVM. You can configure firewall rules to allow or reject access to Lighthouse instances over the private or public network.

#### Note:

The firewall can control only the traffic flowing to the instance. All traffic going out from the instance is allowed by default.

### Concepts

**Outbound traffic:** Traffic generated when data is transmitted from within the instance to outside the instance through the public or private network.

**Inbound traffic:** Traffic generated when data is transmitted from outside the instance to within the instance through the public or private network.

### Firewall Rule

#### Quota limits

Up to **100** firewall rules can be created for each Lighthouse instance.

#### Parameters

A Lighthouse instance firewall can have multiple firewall rules, each of which contains the following parameters:

Parameter	Description
Type	Custom: Specify the protocol and port as needed. Common templates, such as Windows login (3389) and Linux login (22), are provided. If you choose a template, the corresponding protocol and port are entered automatically and cannot be modified.
Source	Specified IPv4 address or range.

Protocol	Protocol type. You can select TCP, UDP, or ICMP.
Port	Port number. You can specify one or multiple ports.
Policy	Allow: Allow traffic to this port Reject: Discard all data packets going to this port without any response.
Notes	A short description of the rule

## Rule priorities

Firewall rules have priorities.

The rule at the top of the list has the highest priority and will take effect first, while the rule at the bottom has the lowest priority and will take effect last.

If there is a rule conflict, the rule with the higher priority will prevail by default.

When traffic goes into an instance associated with the firewall, the firewall rules are calculated from top to bottom. If a rule is hit and takes effect, the subsequent rules do not take effect.

You can adjust the priority of existing firewall rules as instructed in [Modifying firewall rule priority](#).

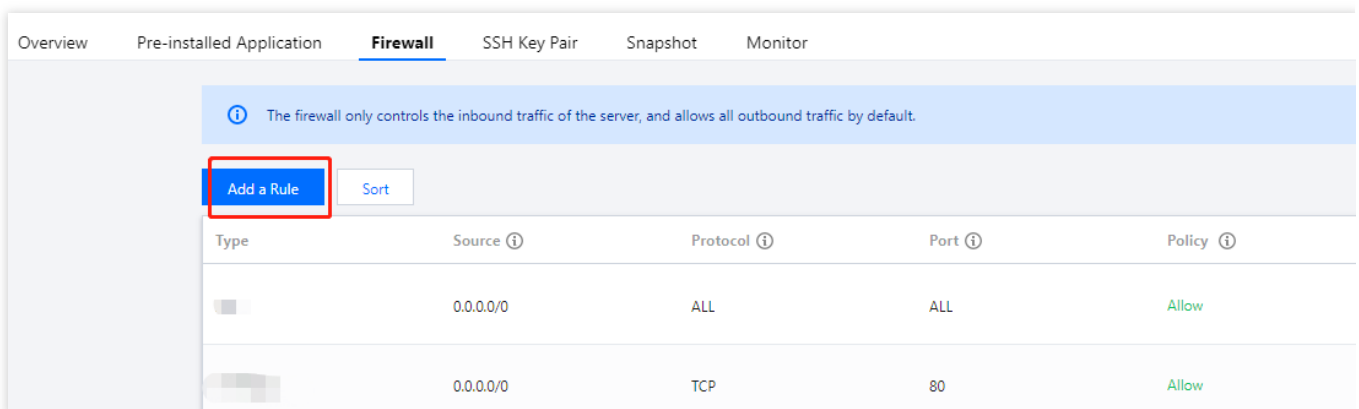
## Directions

### Note:

You can add or delete firewall rules as follows, and the modification will take effect immediately.

### Adding a firewall rule

1. Log in to the [Lighthouse console](#), select the target instance and enter the details page.
2. On the instance details page, select the **Firewall** tab, and click **Add a rule**.



### Note:



After a Lighthouse instance is created, the ICMP protocol will be allowed and ports 80 (HTTP service), 443 (HTTPS service), 22 (Linux SSH service), and 3389 (Windows RDP service) will be opened by default.

You can modify the policies of these ports to **Reject**, or delete the firewall rules as needed on the instance details page. If the firewall rules are deleted, the port will be disabled by default.

3. In the **Create a rule** pop-up window, add a rule by referring to the following:

This document takes adding a rule of allowing traffic whose source IP is `192.168.1.1`, protocol type is `TCP`, and ports are `3306-20000` as an example. Add rules based on your actual conditions. For more information on rule parameters, see [Parameters](#).

### Create a Rule

*i* Controls the inbound traffic of the Lighthouse instance.

Type

Custom

Specified Source *i*

☒ Enable

Source IP *i* \*

192.168.1.1

✓

Protocol

TCP

Port *i* \*

3306-20000

✓

Policy

Allow

Notes

You can enter 60 more characters

OK

Close

**Type:** To set the protocol type and port, select **Custom**.

**Specified source:** To restrict the source IPs, select **Enable**.

If **Enable** is not selected, the rule takes effect for all IPv4 source addresses.

**Source IP:** The firewall rule only takes effect on the specified source IPs. You can enter IP addresses in the following formats:

**Single IP:** Such as `192.168.1.1` .

**CIDR block:** Such as `192.168.1.0/24` .

**All IPv4 addresses:** `0.0.0.0/0` .

**Protocol:** You can select TCP, UDP, or ICMP. This document takes **TCP** as an example.

**Port:** You can select one or multiple ports ranging from 1 to 65535 and use commas to separate them. You can enter ports in the following formats:

**Single port:** Such as `80` .

**Multiple discrete ports:** Such as `80,443` .

**Continuous ports:** Such as `3306-20000` .

**All ports:** `ALL` .

**Policy:** **Allow** or **Refuse**. **Allow** is selected by default.

**Allow:** Traffic to this port is allowed.

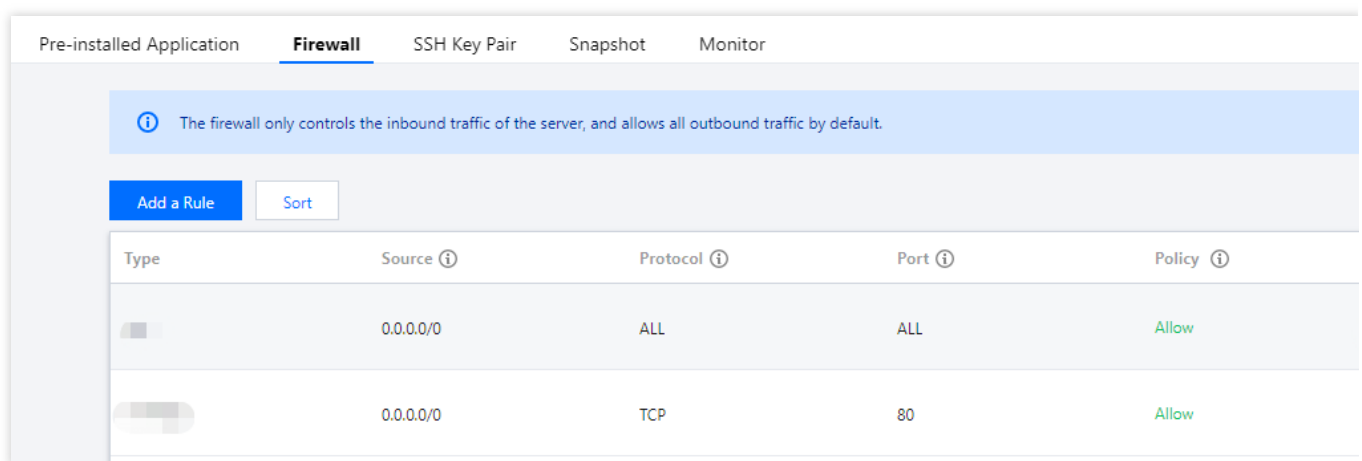
**Reject:** Data packets will be discarded without any response.

**Notes:** A short description of the rule for easier management.

4. Click **OK**.

## Deleting a firewall rule

1. Log in to the [Lighthouse console](#), select the target instance and enter the details page.
2. On the instance details page, select the **Firewall** tab.
3. On the **Firewall** tab, select **Delete** on the right of the target firewall rule.

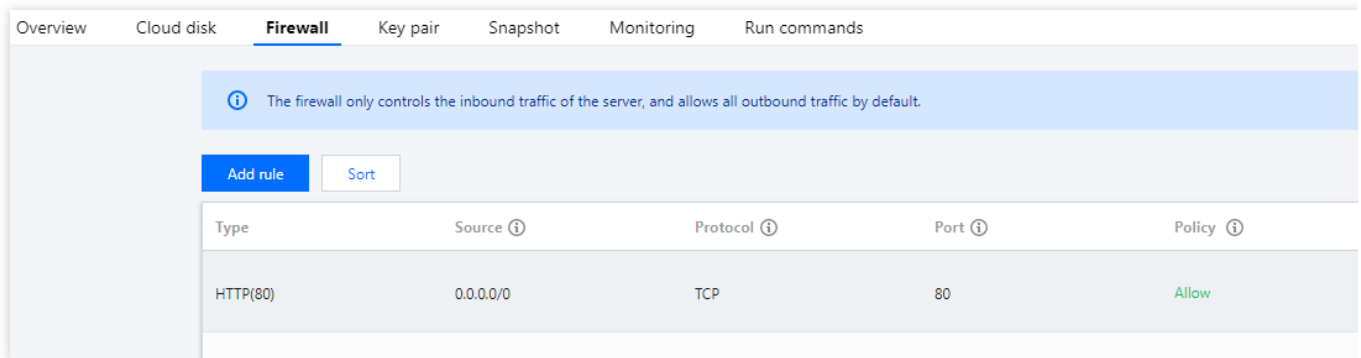


4. In the pop-up prompt box, click **OK**.

## Modifying a firewall rule

1. Log in to the [Lighthouse console](#), select the target instance and enter the details page.

2. On the instance details page, select the **Firewall** tab.
3. On the **Firewall** tab, select **Edit** on the right of target firewall rule.



4. In the pop-up window, modify the configurations with reference to [Parameters](#). Click **OK**.

**Note:**

If the **Type** is not **Custom**, the protocols and ports cannot be modified. If you want to modify them, please change the application type to **Custom**.

You do not need to restart the Lighthouse instance after the modification.




## Related Operations

### Modifying firewall rule priority

1. Log in to the [Lighthouse console](#), select the target instance and enter the details page.
2. On the instance details page, select the **Firewall** tab, and click **Sort**.
3. Select



before the target rule, drag the rule to the desired position, and drop it as shown below:

<div>Add a RuleSort</div>			
Type	Source ⓘ	Protocol ⓘ	Port ⓘ
	0.0.0.0/0	ALL	ALL
	0.0.0.0/0	TCP	80
	0.0.0.0/0	ICMP	ALL

4. Click **Save** below the list.

# Managing Snapshot

Last updated : 2023-07-19 14:54:12

## Overview

You can create a snapshot manually to replicate a Lighthouse instance's system disk at a certain time point. Snapshot is a convenient and efficient data protection service. When a system failure or maloperation occurs in an instance for which a snapshot has been created, you can use the snapshot to roll back the application version of the instance.

Lighthouse instance snapshots have the following use cases:

### Daily data backup

You can use snapshots to regularly back up important business data to avoid data loss caused by incorrect operations, attacks, and viruses.

### Quick data recovery

You can create snapshots before performing major operations, such as changing operating systems, upgrading applications, or migrating business data. If any problem occurs, you can use snapshots to restore the business data.

## Notes

**Snapshot use limits:** Snapshots cannot be created for instances on the storage-optimized package.

**Snapshot quota limits:** The maximum number of free snapshots in each region is the number of created instances (excluding instances to be repossessed and instances on the storage package) multiplied by 2 and cannot exceed 10. When a Lighthouse instance is terminated, all its created snapshots will also be deleted.

## Directions

### Creating snapshot

1. Log in to the [Lighthouse console](#).
2. On the instance list page, select the target instance to enter its details page.
3. On the instance details page, select the **Snapshot** tab.

On this tab, you can click **Create Snapshot** to create a snapshot or view the list of snapshots created for this instance.


4. In the **Create Snapshot** pop-up window, you can customize the snapshot name and click **OK** to create the snapshot as shown below:

### Note:

Generally, it takes less than five minutes to create a snapshot. Please wait patiently. During the creation, the instance doesn't need to be shut down.

During snapshot creation, application data saved in the memory may not be persistently stored. As such, snapshots may not capture the latest and most complete cloud disk data. Refer to [Notes](#) to ensure snapshot data consistency.

**Create a snapshot**×

 **Notes**


1. The free snapshot quota for each region is up to 10 and equals to the number of instances created (excluding instances pending released and instances on storage-optimized bundles) multiplied by 2.
2. Instances on storage-optimized bundles do not support snapshot creation.
3. Snapshots usually can be created within 5 minutes. You do not need to shut down the instance during the creation.

Instance name/ID

aaPanel-fxGA (lhins-9fsu35mz)

Lighthouse bundles

CPU: 2 core; Memory: 2 GB  
System disk: SSD Cloud Disk 30 GB  
Transfer: GB/month (Bandwidth30Mbps)

Snapshot quota 

Quota for current region: 8 (Used: 0)

Snapshot name

Snapshot-20230719114420

✓

Enter 1-60 characters

OK

Cancel

## Using snapshot to roll back instance system disk

### Note:

Rolling back the instance system disk with a snapshot is irreversible. It will clear the system disk data generated after the snapshot creation time. To avoid maloperations, we recommend you create an instance snapshot right before

rollback to back up the latest data.

1. Log in to the [Lighthouse console](#).
2. On the server list page, select the target instance to enter its details page.
3. On the instance details page, select the **Snapshot** tab.

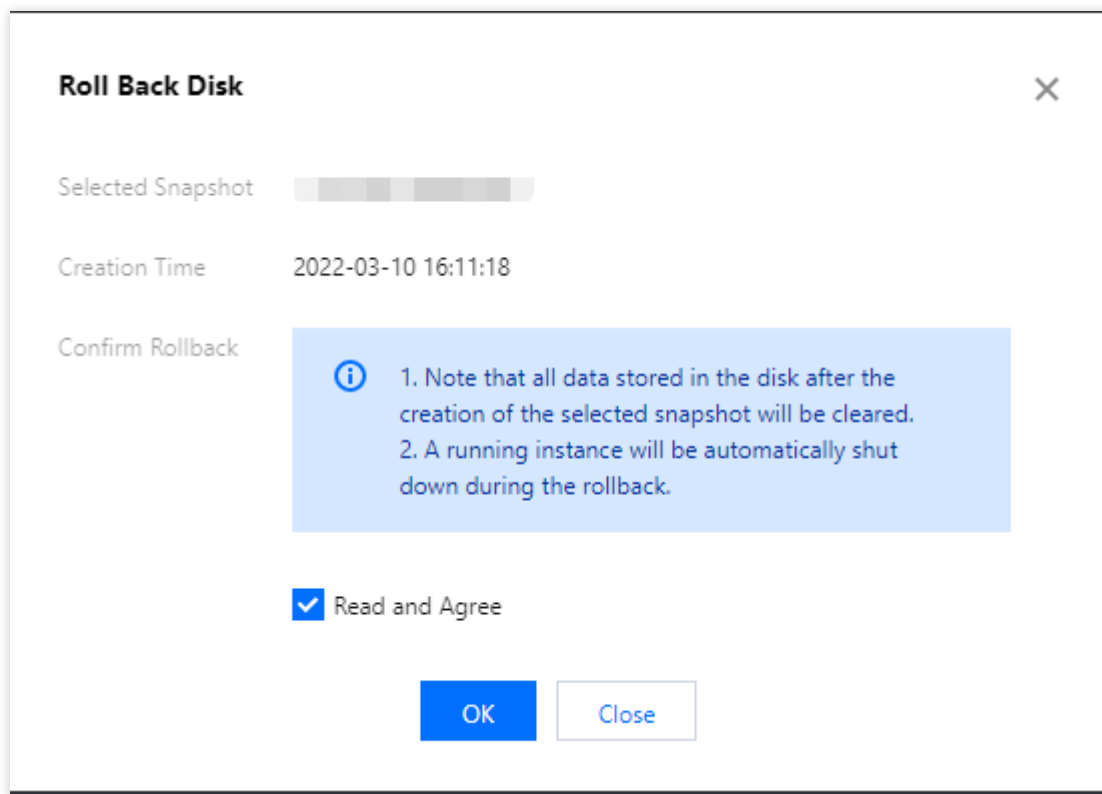
You can also view the list of snapshots created for this instance on this tab.

4. Select **Roll back** on the right of the row of the target snapshot. In the **Roll Back Disk** pop-up window, select **Read and agree** and click **OK** as shown below:

**Note:**

After rollback, the entire instance system disk, rather than a partition or directory, will be restored to the status at the snapshot creation time point.

If the instance is running, it will be shut down automatically during rollback.

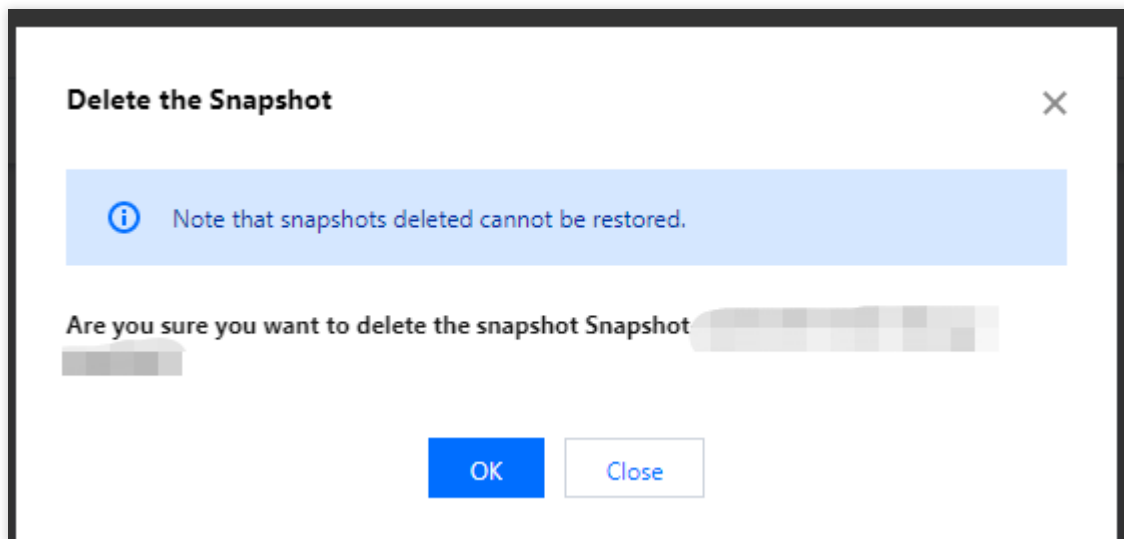


## Deleting snapshot

1. Log in to the [Lighthouse console](#).
2. On the server list page, select the target instance to enter its details page.
3. On the instance details page, select the **Snapshot** tab.
4. Select **Delete** on the right of the row of the target instance. In the **Delete snapshot** pop-up window, click **OK** as shown below:

**Note:**

Deleting a snapshot will also delete all data in the snapshot, and the data cannot be retrieved. Deleted snapshots cannot be restored, so please delete snapshots with caution.





# Managing Image

## Working with Custom Images

Last updated : 2022-09-26 11:28:02

### Overview

You can create a custom image in addition to using Lighthouse application images and system images. The custom image can be used to quickly create Lighthouse instances with the same configurations as the image in the Lighthouse console.

### Notes

Up to 20 custom images can be created in each region. To increase the quota limit, [submit a ticket](#) for application. A free tier of five custom images is provided in each region, and excessive images will incur fees. For more information, see [Billing Overview](#).

If your account has overdue payments:

The custom image feature will be disabled, and you cannot create more custom images.

All custom images (including those within the free tier) under your account will be isolated in the **To be repossessed** status and become unavailable. **The images that exceed the free tier will continue to be billed** until they are deleted. If you don't top up your account within seven days, the custom images will be deleted automatically.

The creation process takes ten minutes or more, which depends on the data size of the instance. Prepare in advance to avoid business impacts.


Currently, cross-region replication of custom images is not supported. You can regularly check out the [Tencent Cloud Lighthouse](#) page to get the latest information.

### Directions

#### Creating a custom image

1. Log in to the [Lighthouse console](#).
2. On the instance list page, select the target instance to enter the instance details page.
3. In **Application information** on the instance details page, select **Create image**.

### Image Details

Image Name	 TencentOS Server <a href="#">Reset Application</a> <a href="#">Create Image</a>
Image Type	System Image
Operating System	TencentOS Server 3.1 (TK4)

4. In the **Enter image information** step in the **Create custom image** pop-up window, enter the **Image name** and **Description**, and click **Next: Shut down the instance**.

### Create custom image ✕

1 Enter image information

>

2 Shutdown Instance

1. Custom image quota and billing:

- Each region supports creating up to 20 custom images.
- Five free custom images are available to each region where instances (excluding those pending repossessed) exists. The number of images exceeding five will be billed hourly.
- To create an image, ensure your account balance is sufficient.

2. The image can be created only when the instance is shut down. It takes about 10 minutes to create an image.

Image Name \*

Supports letters, numbers and "-". 60 more characters allowed

Description

You can enter 60 more characters

Free quota for custom images in this region: 5; created custom images: 0

Next: Shut Down Instance

Close

5. In the **Shutdown instance** step, select "Agree to a forced shutdown" and click **Create image**. After the custom image is created, you can go to the [custom image](#) list page to view it.

## Deleting a custom image

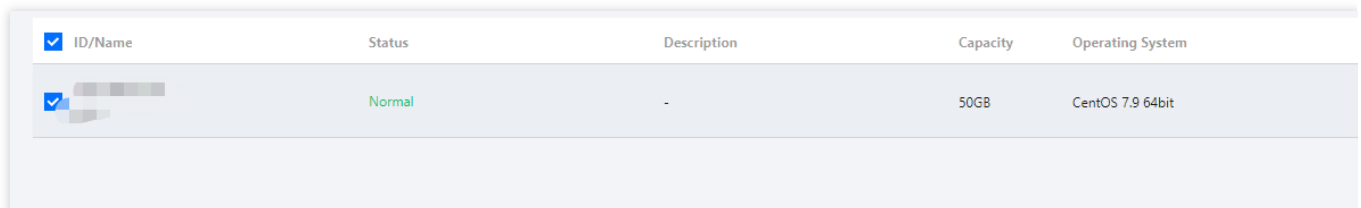
1. Log in to the Lighthouse console and select **Custom image** on the left sidebar.
2. At the top of the **Custom image** page, select the region of the target image.
3. Select **More > Delete** on the right of the target image in the list.
4. In the **Delete image** pop-up window, click **OK** to delete the image.

## Related Operations

### Using a custom image to create an instance

You can use a custom image to quickly create a Lightweight instance in the following steps:

1. Log in to the Lighthouse console and select **Custom image** on the left sidebar.
2. At the top of the **Custom image** page, select the region of the target image.
3. Select **Create instance** on the right of the target image in the list to enter the Lighthouse instance purchase page.



<input checked="" type="checkbox"/> ID/Name	Status	Description	Capacity	Operating System
<input checked="" type="checkbox"/> [blurred]	Normal	-	50GB	CentOS 7.9 64bit

4. On the Lightweight instance purchase page, select other configuration items of the instance as instructed in [Purchase Methods](#).

#### Note:

As custom images don't have a unified template and are created based on your own data, the instances created by using them don't have the **Pre-installed Application** tab.

### Viewing the information of the custom images in the current region

You can view the information of existing custom images in a specific region in the following steps:

1. Log in to the Lighthouse console and select **Custom image** on the left sidebar.
2. At the top of the **Custom image** page, select the region of the target image.
3. Then, you can view the total number of custom images, free tier, and estimated price information in the current region on the page.

#### Note:

A free tier of five custom images is provided in each region.

Once your account has overdue payments, all custom images (including those within the free tier) under your account will be isolated in the **To be repossessed** status and become unavailable. If you don't top up your account within seven days, the custom images will be deleted automatically.

Hong Kong, Macau and Taiwan (China)				Southeast Asia		US West		Europe		Northeast Asia		South Asia	
Hong Kong, China				Singapore		Silicon Valley		Frankfurt		Tokyo		Mumbai	

Region	Total	Free Quota ⓘ	Estimated
Hong Kong, China	1	5	

# References

[Overview](#)

[Billing Overview](#)

# Replicating Custom Images Across Regions

Last updated : 2023-08-29 14:14:55

## Feature

With Cross-Region Replication, you can replicate a custom image to multiple destination regions, and create Lighthouse instances in the destination regions with the replicated image.

## Precautions

An image cannot be replicated between the Chinese mainland and other countries/regions.

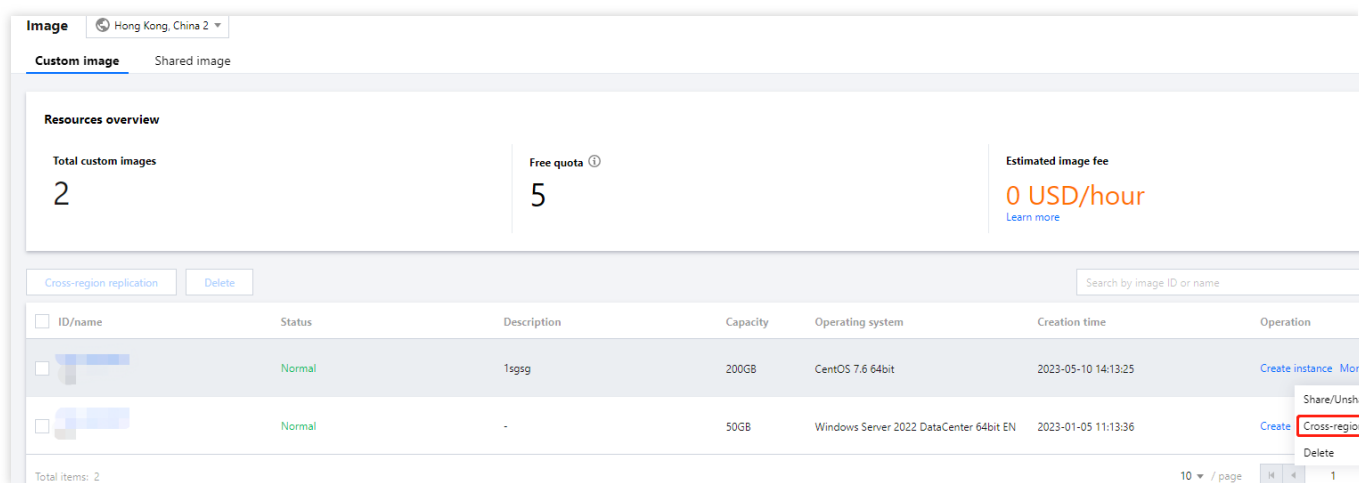
When an image is replicated to a destination region, it consumes the custom image quota in this region and be charged as a custom image. For more information, see [Custom Image Pricing](#).

It usually takes 15 to 40 minutes to replicate an image.

You can replicate an image to up to 10 destination regions at one time.

## Directions

1. Log in to the Lighthouse console and select **Image** on the left sidebar.
2. Select the region at the top of the **Image** page and click the **Custom image** tab.
3. Select **More > Cross-region replication** on the right of the target image in the list.



4. In the **Cross-region replication** window that pops up, read the precautions, and click **OK**.

After the replication is completed:

You can find an image with the same name but a different ID in the list.

You can use the image to create an instance in the destination region. For detailed steps, see [Working with Custom Images](#).

# Share Custom Images

Last updated : 2023-07-19 17:08:04

## Overview

Tencent Cloud allows you to share custom images between Lighthouse and CVM. You can customize image sharing as needed to implement offline migration between them. You can also use a shared image to quickly create instances and then get the needed components from them or add custom content to them.

**Note:**

Shared images do not take up the quota of custom Lighthouse instance images.

A shared custom Lighthouse instance can be deleted only after sharing is canceled.

## Usage Limits

Custom images can be shared only between Lighthouse and CVM instances in the same region under the same account.

You cannot share the following custom images from CVM to Lighthouse:

- Imported custom CVM instance images.

- Custom images already shared from CVM to Lighthouse.

- Custom images of entire CVM instances.

- Custom images whose underlying operating system and version are not listed in [Supported Operating Systems](#).

- Custom images without Cloud-init installed.

## Supported Operating Systems

Images on the following underlying operating systems and versions can be shared:

- CentOS 6.8 or later

- Ubuntu 16.04 or later

- Debian 8.2 or later

- Windows Server 2012 or later

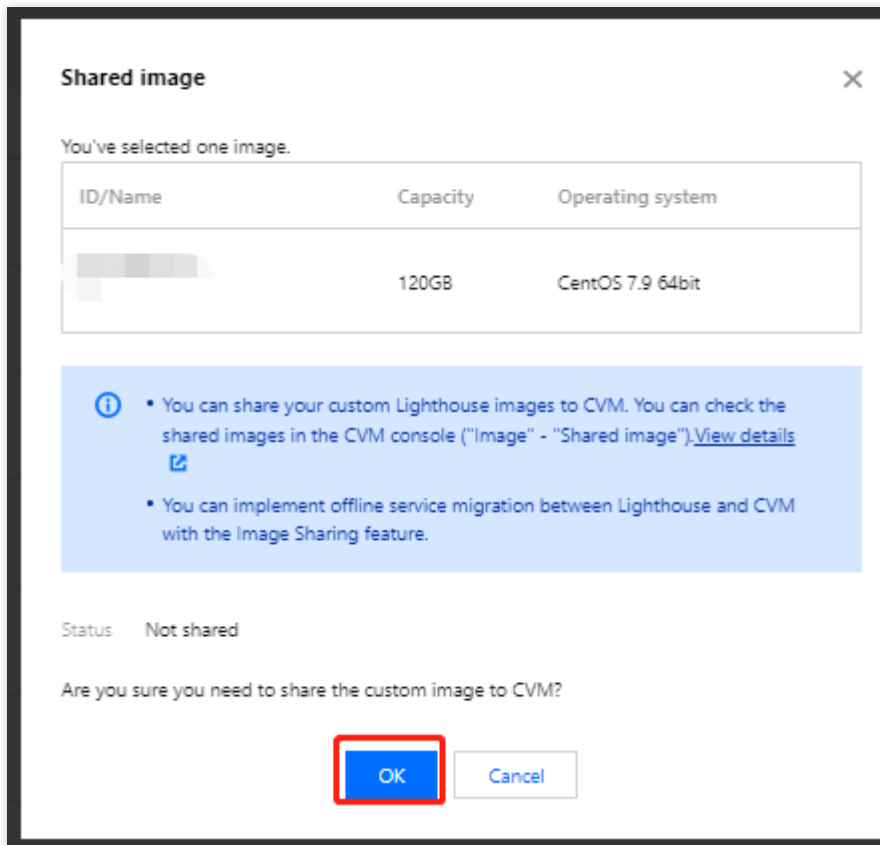
- TencentOS Server 2.4 or later

## Directions



## Sharing image to CVM

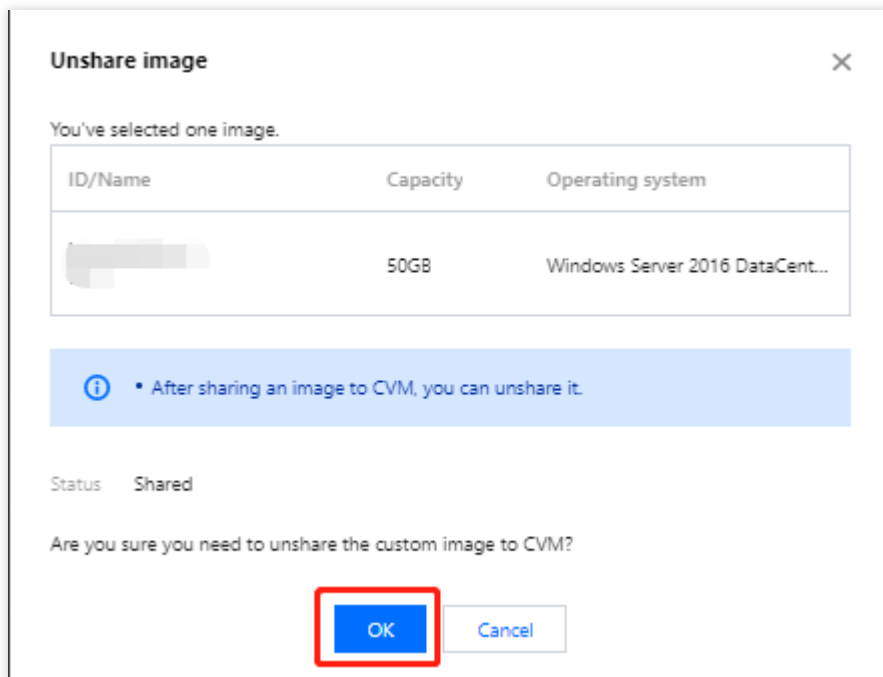
1. Log in to the Lighthouse console and select **Images** on the left sidebar.
2. Select the region at the top of the **Image** page and click the **Custom image** tab.
3. On the right of the row of the target image, select **More > Share/Unshare**.
4. In the **Share Image** pop-up window, click **OK** as shown below:



After sharing the image, you can view it on the [shared image](#) list page in the CVM console.

## Unsharing image to CVM

1. On the **Custom image** tab, select **More > Share/Unshare** on the right of the row of the target image.
2. In the **Unshare Image** pop-up window, click **OK** as shown below:



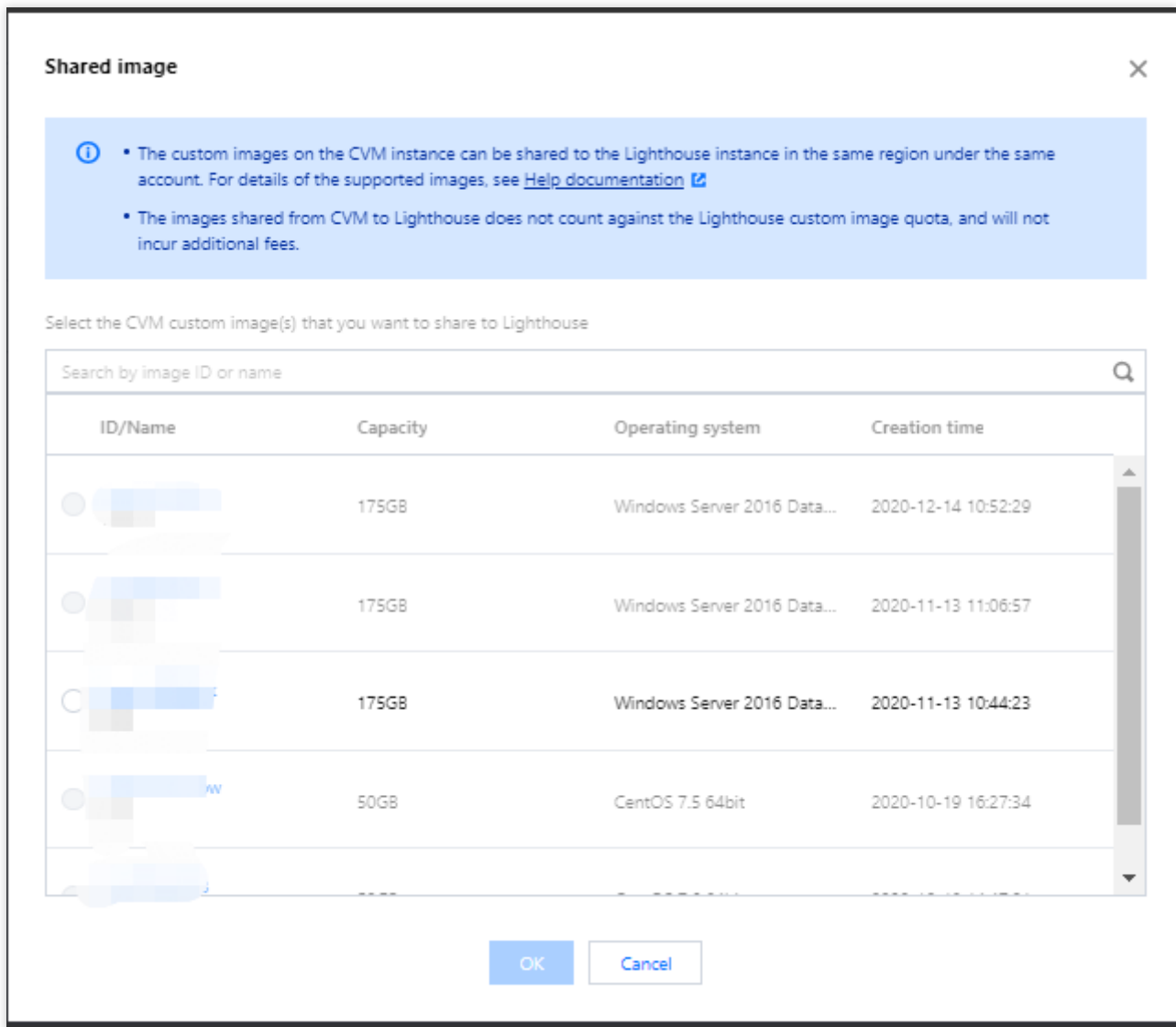
## Sharing image to Lighthouse

You can share a custom CVM instance image to Lighthouse in the following consoles:

Lighthouse console

CVM console

1. Log in to the Lighthouse console and select **Images** on the left sidebar.
2. Select the region at the top of the **Image** page and click the **Shared image** tab.
3. Click **Share CVM image**. In the **Share Image** pop-up window, select the target image as shown below:



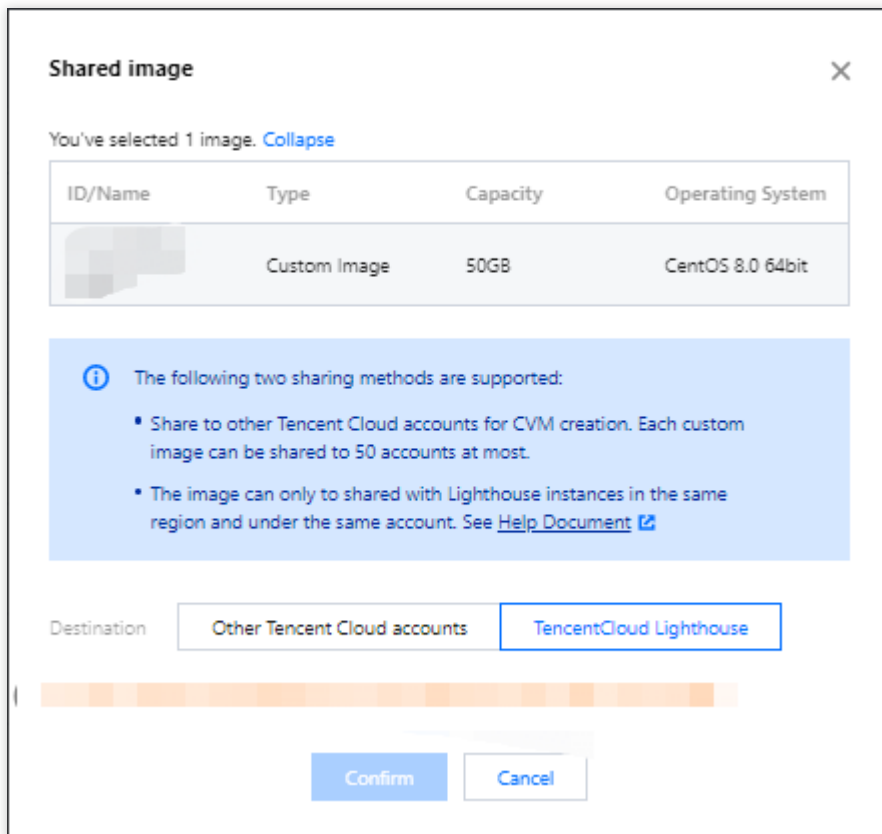
4. Click **OK**.

1. Log in to the CVM console and click **Images** on the left sidebar.

2. Select the region at the top of the **Image** page and click the **Custom image** tab.

3. On the right of the row of the target image, select **Share**.

4. In the **Share Image** pop-up window, select **Lighthouse** as the destination as shown below:



5. Click **OK**.

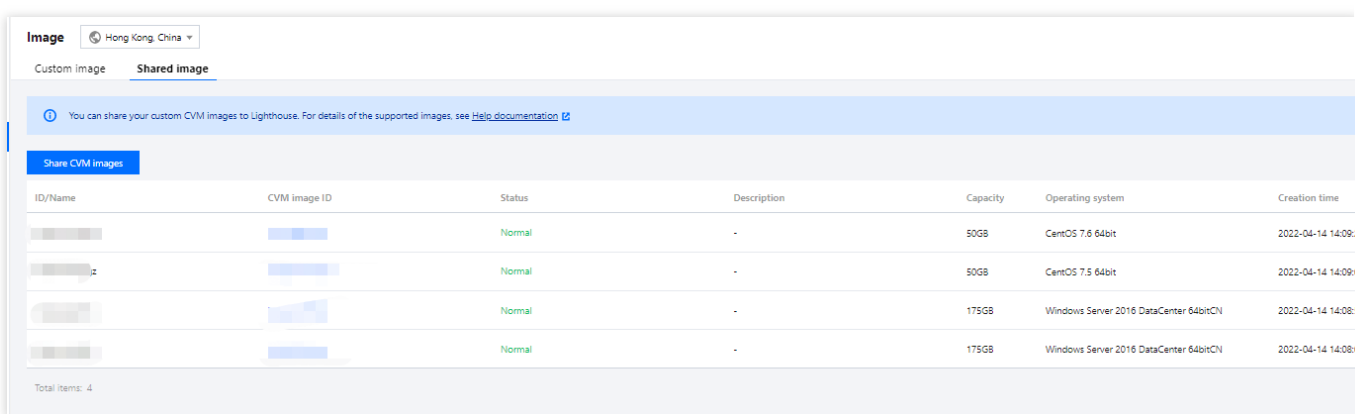
## Unsharing image to Lighthouse

You can unshare a custom CVM instance image to Lighthouse in the following consoles:

Lighthouse console

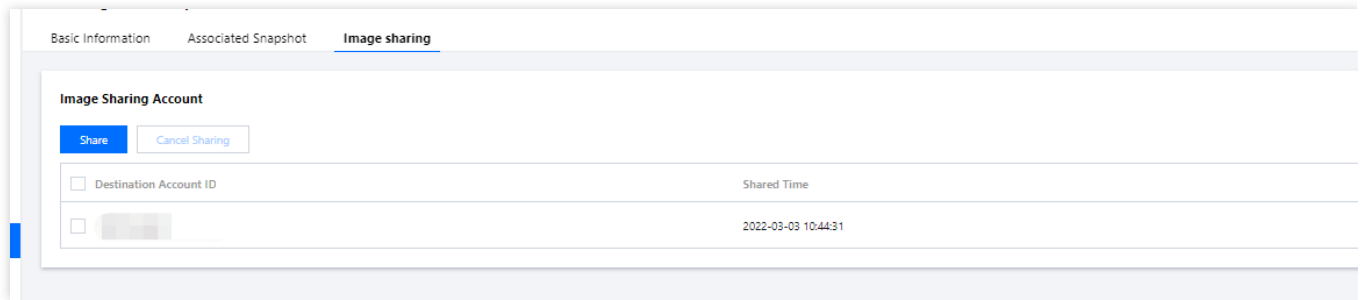
CVM console

1. Log in to the Lighthouse console and select **Images** on the left sidebar.
2. Select the region at the top of the **Image** page and click the **Shared image** tab.
3. On the right of the row of the target image, click **Unshare** as shown below:



4. In the **Unshare Image** pop-up window, click **OK**.

1. Log in to the CVM console and click **Images** on the left sidebar.
2. Select the region at the top of the **Image** page and click the **Custom image** tab.
3. On the right of the row of the target image, select **More > Unshare**.
4. On the **Shared image** tab on the image details page, select **Unshare** on the right of the row of the target image sharing record as shown below:



5. In the **Unshare** pop-up window, click **OK**.

## Related Operations

### Viewing image sharing status

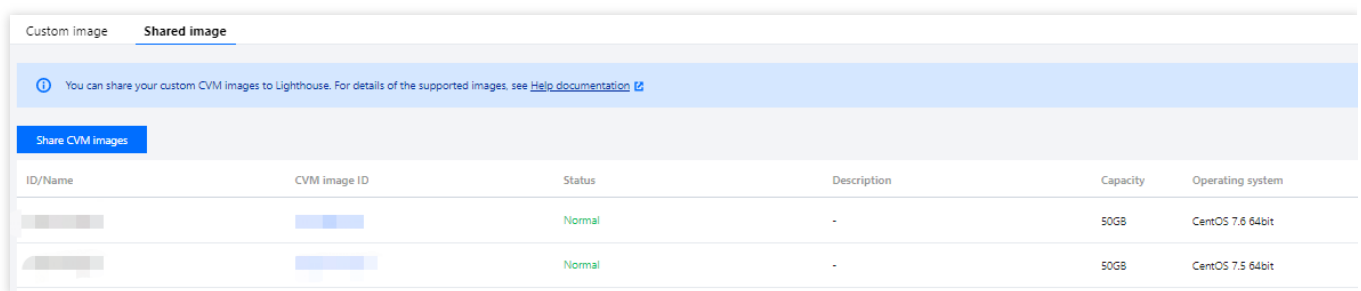
You can view image information and sharing status on the custom image details page in the Lighthouse console:

1. Log in to the Lighthouse console and select **Images** on the left sidebar.
2. Select the region at the top of the **Image** page and click the **Custom image** tab.
3. Click the ID of the target image to enter its details page to view its information and sharing status.

### Using shared image to create instance

You can use an image shared to Lighthouse to create an instance quickly.

1. Log in to the Lighthouse console and select **Images** on the left sidebar.
2. Select the region at the top of the **Image** page and click the **Shared image** tab.
3. On the right of the row of the target image, click **Create instance** as shown below:



4. On the Lighthouse instance purchase page, select the configuration as need and create the instance.

Here, the shared instance is selected for **Image**, and you need to set other configuration items as instructed in [Purchase Methods](#).

# Tencent Cloud Support for Lighthouse Images

Last updated : 2022-05-30 16:08:00

Tencent Cloud Lighthouse provides rich application images for efficient application deployment. Besides the underlying operating systems (CentOS and Windows Server), these images also encapsulate third-party applications (such as LAMP, WordPress, ASP.NET, and Node.js), the runtime environments, and relevant initialization configuration files. Tencent Cloud provides support for the images deployed in the Lighthouse instances, including the operating system and Tencent Cloud software and ensures the proper running of the server. The user needs to take care of the rest part of the server, such as applications installed by themselves.

## Note:

Tencent does not provide any technical support for any Third Party Software. Please visit the relevant open source communities for technical support.

Tencent Cloud provides the following support on the listed application images. You can also seek help on the official websites of the third-party software and other community websites.

Application Image Name	Tencent Cloud Support	Third-party Tutorial	Notes		
WordPress	For a Lighthouse instance created using the application image, Tencent Cloud will guarantee that: The instance can be started up normally and enter the "running" status. The operating system can be booted and run normally. The pre-installed third-party application software in the application image and the operating environment that the application depends on can be started and run normally, and the preset initialization configuration file can be loaded normally.	Third-party tutorials are for learning and reference only.	-		
Typecho			-		
Cloudfire			-		
Matomo			-		
LAMP			-		
Node.js			-		
ASP.NET			-		
Theia IDE			-		
Docker CE			-		
K3s			-		





# Private Network Interconnection

Last updated : 2022-08-15 18:03:47

## Overview

Lighthouse uses the [Virtual Private Cloud](#) automatically assigned by Tencent Cloud for network isolation. By default, Lighthouse instances cannot interconnect with other Tencent Cloud resources in VPCs such as CVM and TencentDB over the private network, and their interconnection needs to be implemented by associating a CCN instance. The interconnection feature is applicable to the following businesses:

Lighthouse access to CVM.

Lighthouse access to TencentDB.

### **Note:**

Lighthouse instances in the same region under the same account are interconnected over the private network by default. For more information, see [Region and Interconnection](#).

Lighthouse and COS in the same region are interconnected over the private network by default with no need to be interconnected over CCN.

Other Tencent Cloud resources need to use VPC to interconnect with Lighthouse.

This document describes how to associate/disassociate an instance with/from CCN in the Lighthouse console. For more information on CCN, see [Overview](#).

## Must-knows

The interconnection feature of Lighthouse is free of charge. You only need to pay attention to CCN billing information. For more information, see [Pricing](#).

CCN cross-MLC-border connections are not available for Lighthouse instances.

Under the same account:

All Lighthouse instances in the same region are in the same VPC. A VPC can be associated with only one CCN instance.

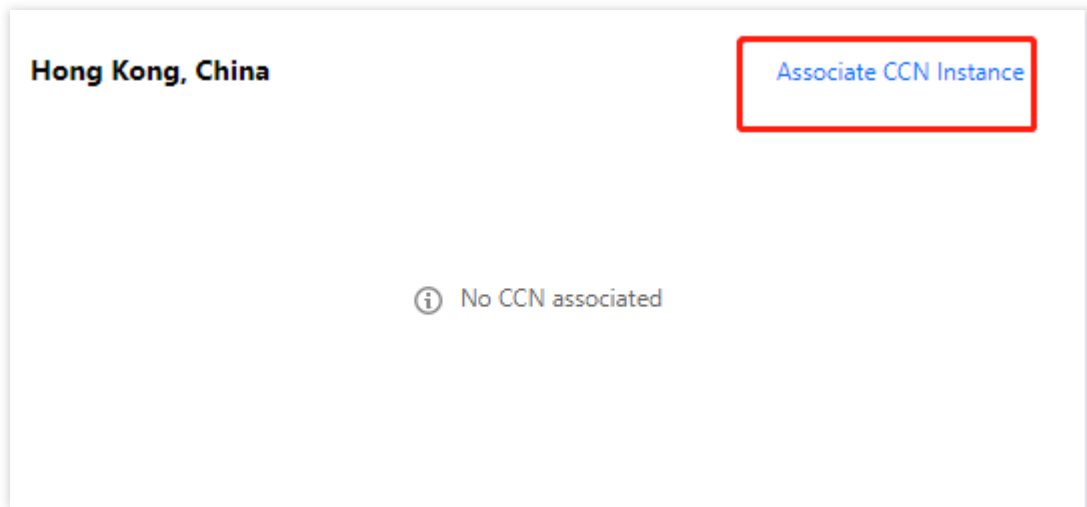
Lighthouse instances in different regions are in different VPCs, which need to be associated with CCN instances separately.

If there are no Lighthouse instances in a region, you cannot associate a CCN instance in that region.

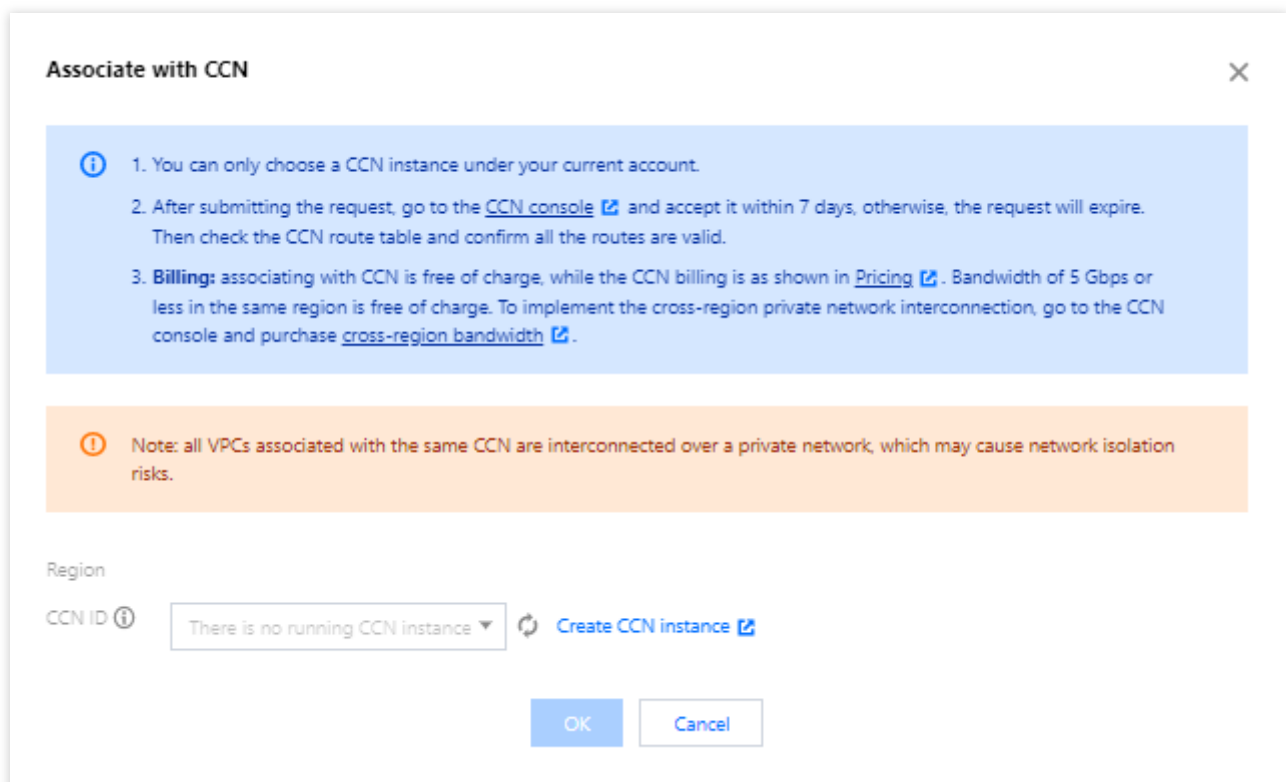
## Directions

### Applying for Associating with a CCN

1. Log in to the Lighthouse console and select **Interconnection** on the left sidebar.
2. Select **Associate CCN Instance** in the target region.



3. In the **Associate with CCN** pop-up window, select the target CCN instance and click **OK** to submit the association application.

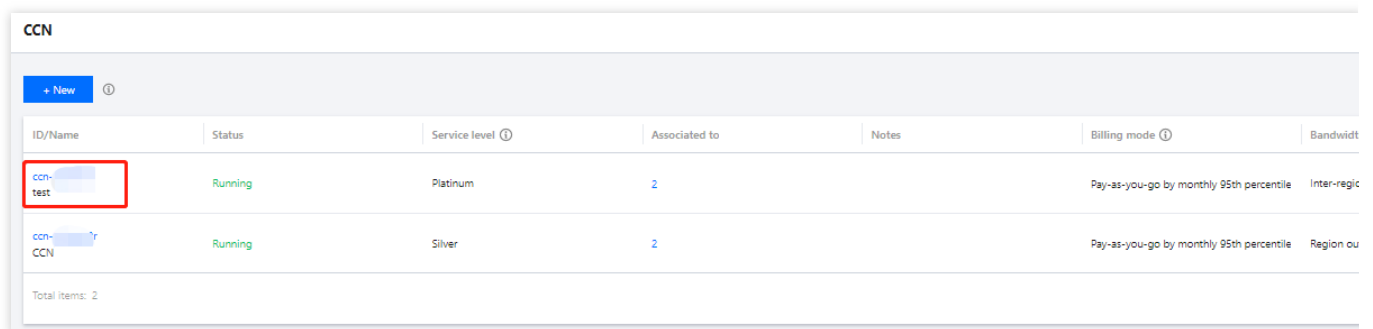
**Note:**

If no CCN instances are available, create one as instructed in [Creating a CCN Instance](#).

Only CCN instances under the same account can be associated with.

After submitting the association application, log in to the [CCN console](#) in seven days to approve the application; otherwise, the application will expire, and you need to apply for association again.

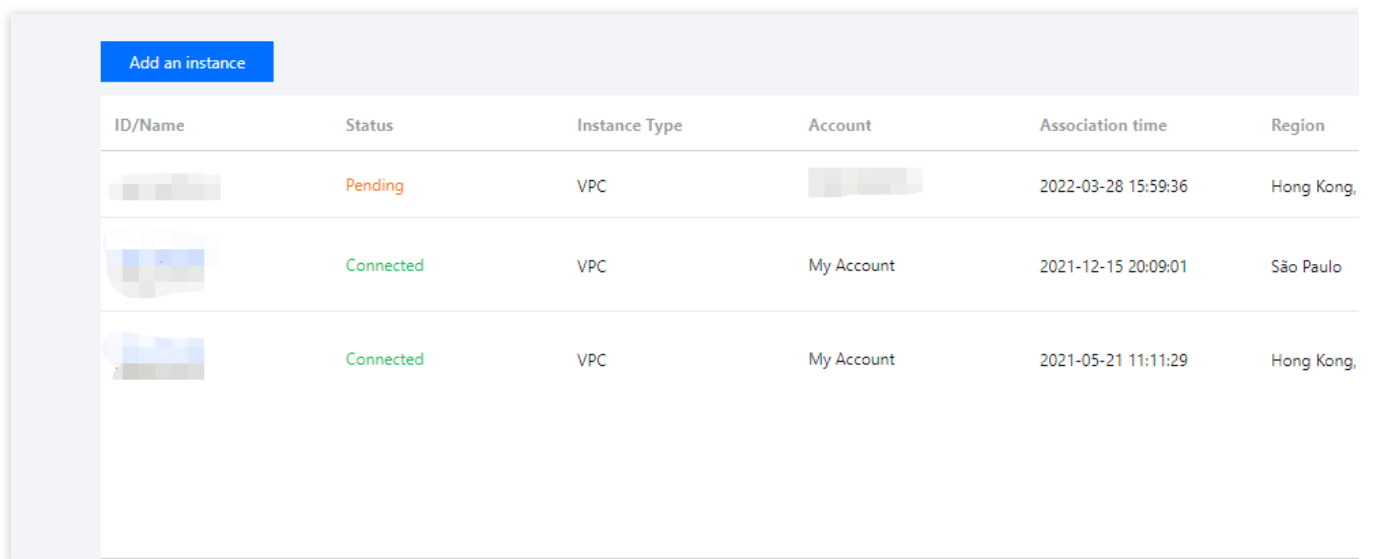
4. Log in to the [CCN console](#), and click the ID/Name of the target CCN instance to open its details page.



<a href="#">+ New</a> ⓘ						
ID/Name	Status	Service level ⓘ	Associated to	Notes	Billing mode ⓘ	Bandwidth
ccn-test	Running	Platinum	2		Pay-as-you-go by monthly 95th percentile	Inter-regio
ccn-CCN	Running	Silver	2		Pay-as-you-go by monthly 95th percentile	Region ou
Total items: 2						

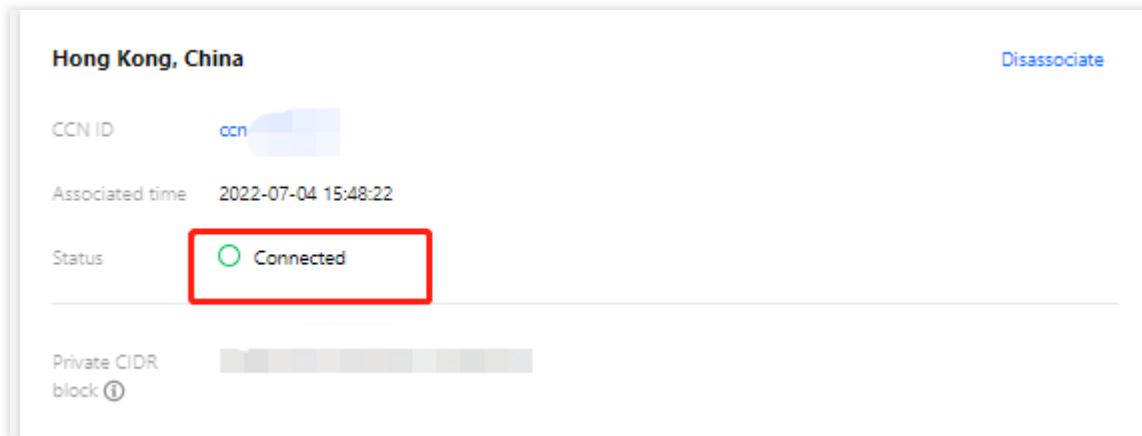
5. On the CCN instance details page, select **Approve** on the right of the target association application.

Remarks "Lighthouse VPC" will be added to the VPC instance of Lighthouse by default. Select the correct instance as shown below:



ID/Name	Status	Instance Type	Account	Association time	Region
	Pending	VPC		2022-03-28 15:59:36	Hong Kong,
	Connected	VPC	My Account	2021-12-15 20:09:01	São Paulo
	Connected	VPC	My Account	2021-05-21 11:11:29	Hong Kong,

6. In the pop-up window, click **OK** to complete association. On the interconnection page, the region status will become **Connected**.



7. After the association is complete, check that the route is valid by following these steps:

- On the **Interconnection** page, click **CCN ID** under the region to go to the CCN details page.
- On the CCN details page, select **Route Table** tab.
- Confirm that the new routes are "valid". If there is a CIDR block conflict, the route may be invalid.

**Note:**

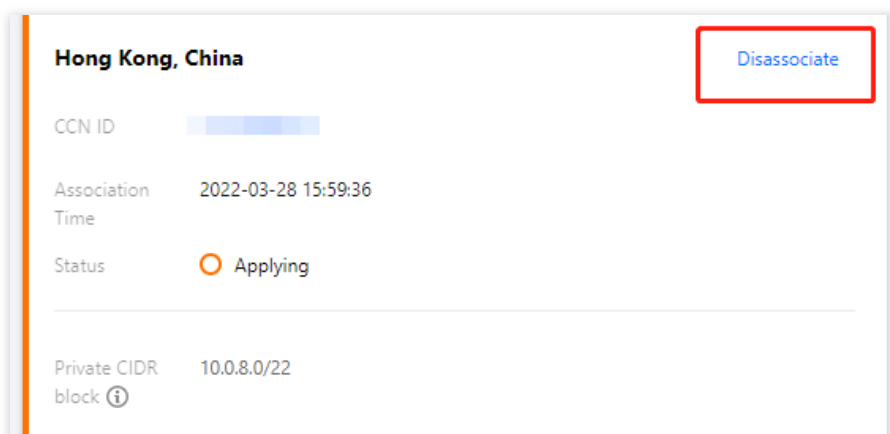
To use invalid routes, see [Disabling Route](#) and [Enabling route](https://intl.cloud.tencent.com/document/product/1003/30069). For conflict rules and restrictions, see [Use Limits](#).

8. After associating the Lighthouse instance with CCN, you can associate Tencent Cloud resources such as CVM and TencentDB instances to CCN to implement interconnection. For more information, see [Associating Network Instances](#).

## Disassociating from a CCN

You can disassociate a CCN instance when the CCN association application status is **Applying**, **Expired**, or **Connected**. If the status is **Connected**, disassociation will interrupt the connections of all instances in the current region to other VPCs in CCN. Perform the following operations after confirming that they will not affect your business:

- Log in to the Lighthouse console and select **Interconnection** on the left sidebar.
- Select **Disassociate** in the target region.



3. In the **Disassociate from CCN** pop-up window, click **OK**.

## Examples of Interconnection Between Lighthouse with Cloud Resources

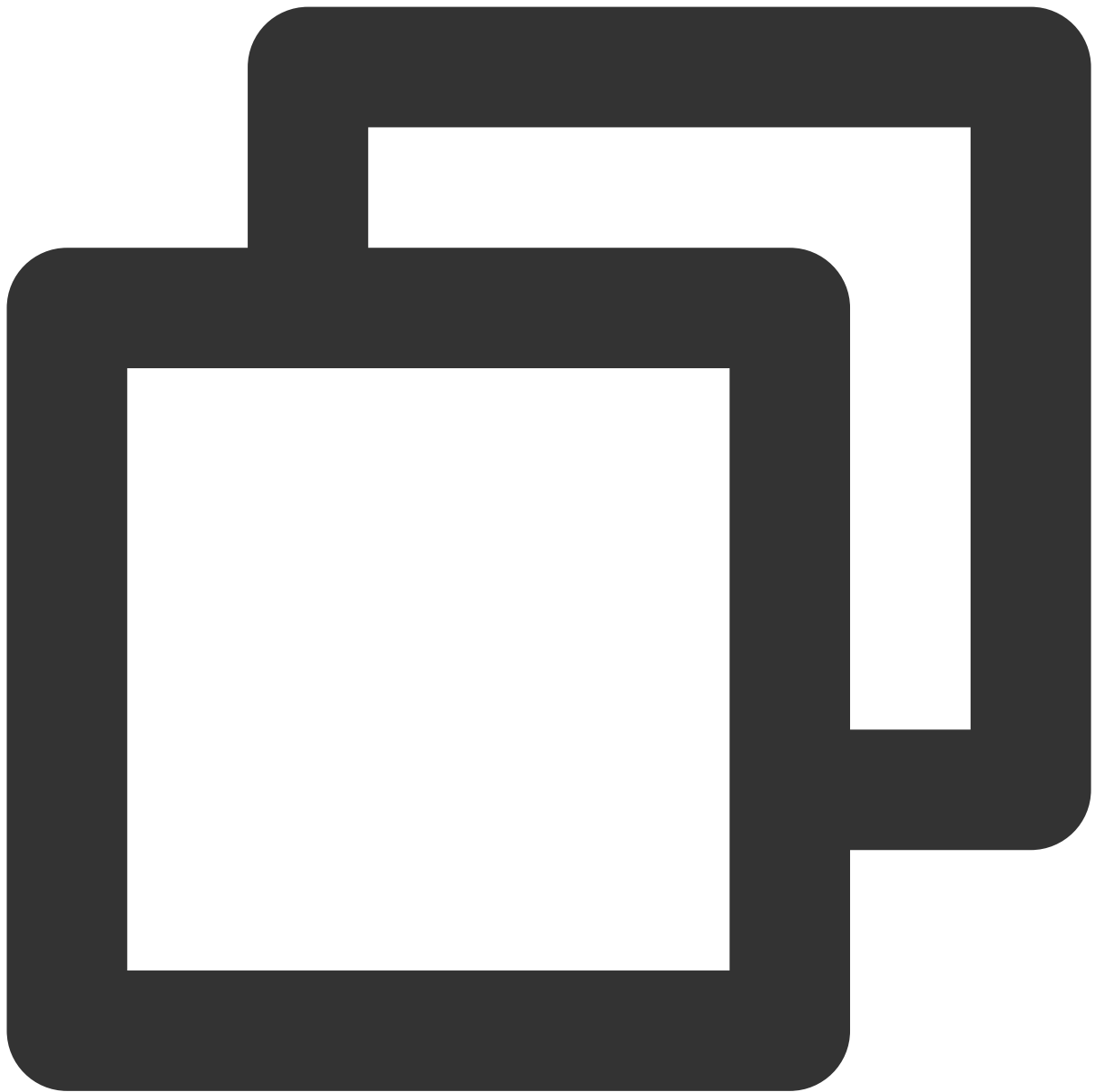
Example 1: Interconnection Between Lighthouse and CVM

### Scenario

The Lighthouse and CVM instances in the Guangzhou region are not interconnected by default and need to be associated with CCN for interconnection.

### Steps

1. Log in to the Lighthouse instance and run the following command:



```
ping CVM instance's private IP
```

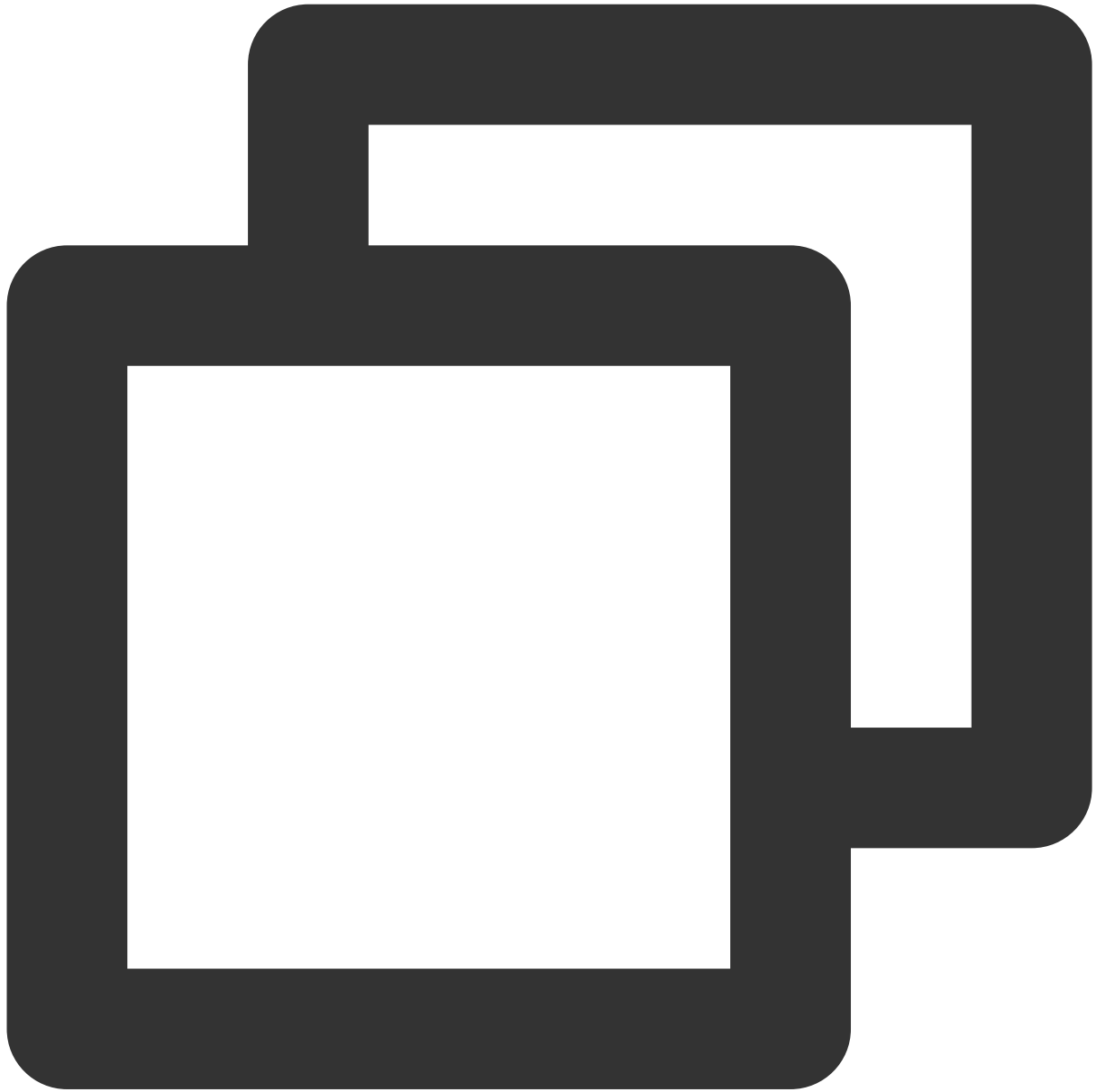
If the following information is returned, the IP cannot be pinged:

```
[lighthouse@VM-12-13-centos ~]$ ping 10.18.8.74
PING 10.18.8.74 (10.18.8.74) 56(84) bytes of data.
^C
--- 10.18.8.74 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 7999ms
```

2. Associate with a CCN as instructed in [Applying for associating with a CCN](#).

Associate the VPC of CVM with the CCN instance as instructed in [Associating Network Instances](#).

3. Log in to the Lighthouse instance and run the following command:



```
ping CVM instance's private IP
```

If the following information is returned, the IP can be pinged and the interconnection succeeds.

```
[lighthouse@VM-12-13-centos ~]$ ping 10.18.1.74
PING 10.18.1.74 (10.18.1.74) 56(84) bytes of data.
64 bytes from 10.18.1.74: icmp_seq=1 ttl=64 time=0.658 ms
64 bytes from 10.18.1.74: icmp_seq=2 ttl=64 time=0.684 ms
64 bytes from 10.18.1.74: icmp_seq=3 ttl=64 time=0.662 ms
64 bytes from 10.18.1.74: icmp_seq=4 ttl=64 time=0.652 ms
^C
--- 10.18.1.74 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.652/0.664/0.684/0.012 ms
```

## Example 2: Interconnection Between Lighthouse and TencentDB for MySQL

### Scenario

In Guangzhou region, the Lighthouse and TencentDB for MySQL instructed in [Overview](#) are not interconnected by default. You need to associate MySQL with CCN to implement the interconnection.

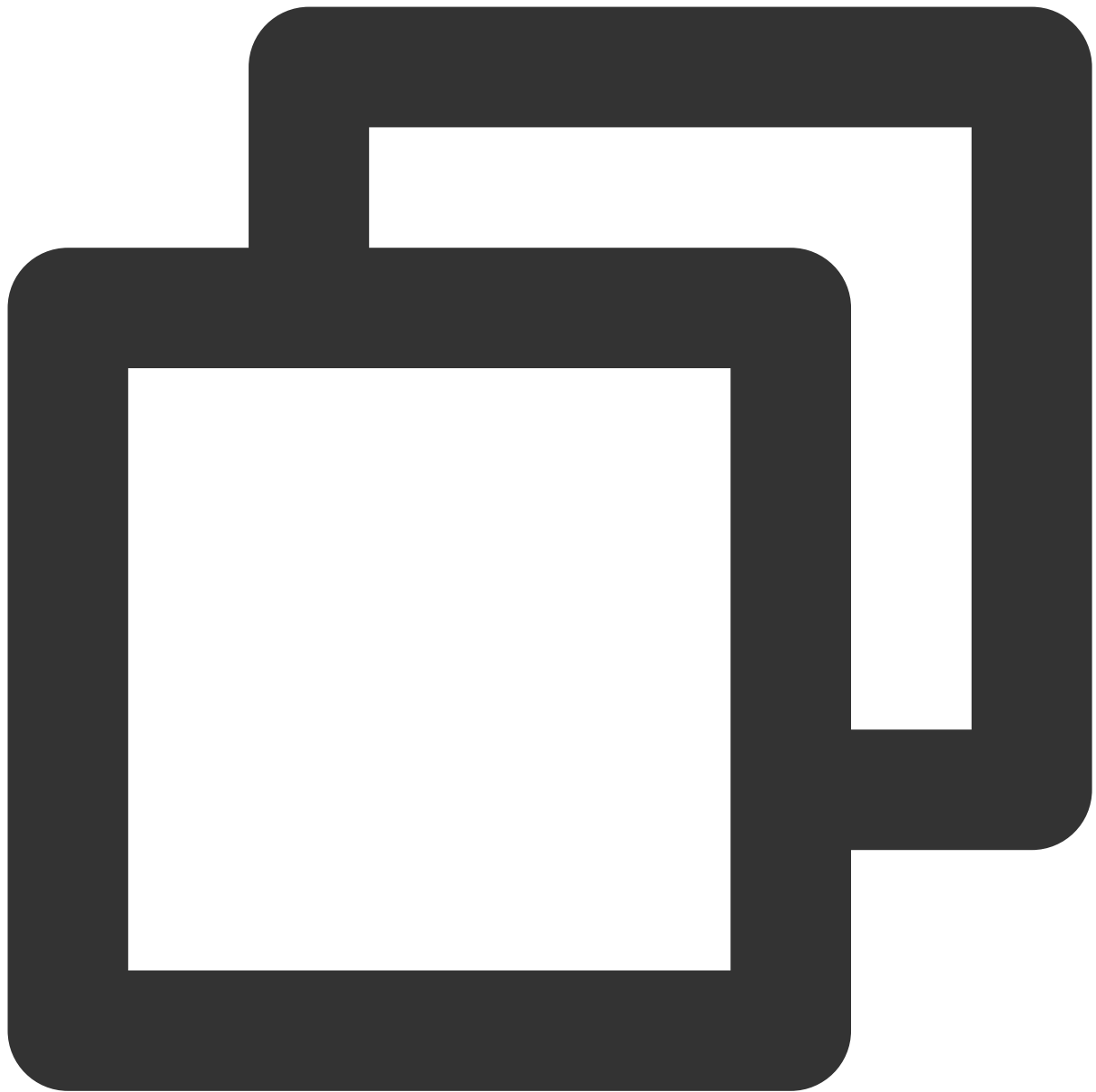
### Prerequisites

TencentDB for MySQL uses private network port `3306` by default. Allow this port in the inbound rules of the security group associated with the MySQL instance. For details, see [TencentDB Security Group Management](#).

### Steps

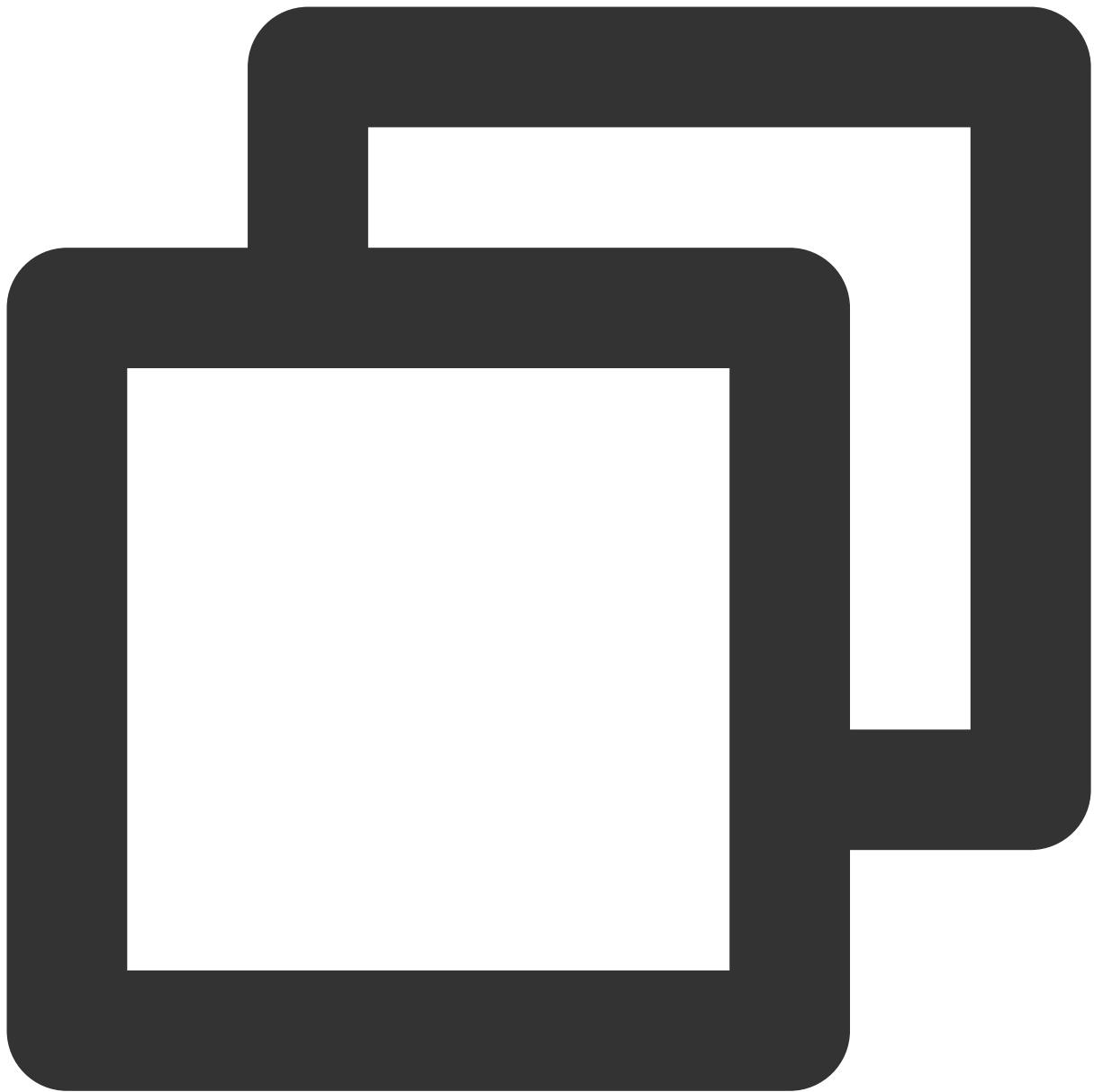
1. Log in to the Lighthouse instance and run the following command to install `telnet` :





```
sudo yum install telnet -y
```

2. Run the following command to test whether the interconnection is successful or not.



```
telnet TencentDB for MySQL instance's private IP 3306
```

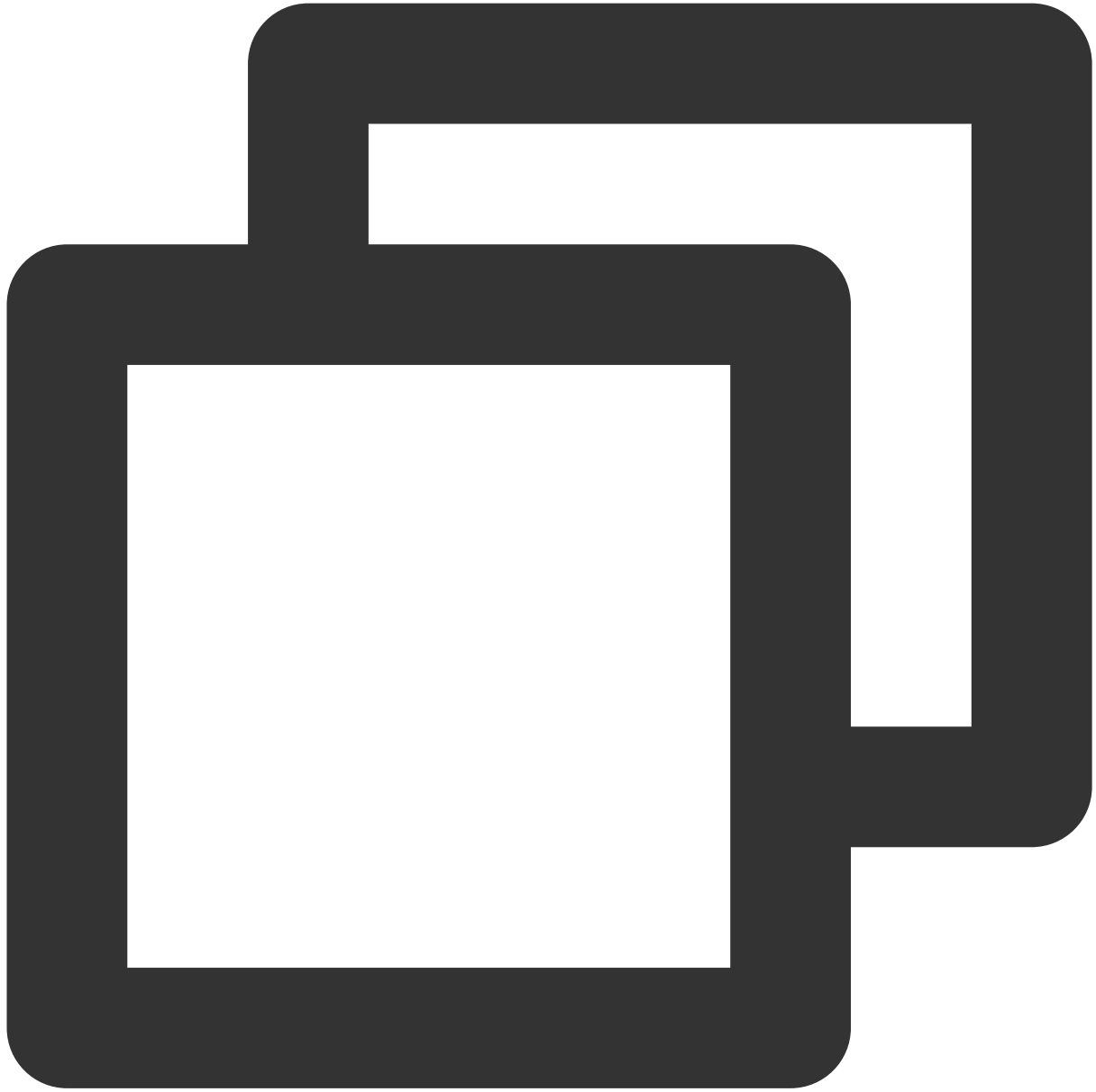
If the following information is returned, the interconnection fails.

```
[lighthouse@VM-12-13-centos ~]$ telnet 10.8.9.11 3306
Trying 10.8.9.11...
telnet: connect to address 10.8.9.11: Connection timed out
```

3. Associate with a CCN as instructed in [Applying for associating with a CCN](#).

Associate the VPC of TencentDB for MySQL with the CCN instance as instructed in [Associating Network Instances](#).

4. Log in to the Lighthouse instance and run the following command:



```
telnet TencentDB for MySQL instance's private IP 3306
```

If the following information is returned, the interconnection succeeds.

```
[lighthouse@VM-12-13-centos ~]$ telnet 10.0.16.12 3306
Trying 10.0.16.12...
Connected to 10.0.16.12.
Escape character is '^]'.
P
PJJu[~z#&TqV&mysql_native_password^[a
```

5. Connect the Lighthouse instance to a MySQL instance as instructed in [Connecting to MySQL Instance](#).

Example 3: Interconnection Between Lighthouse and TencentDB for Redis

### Scenario

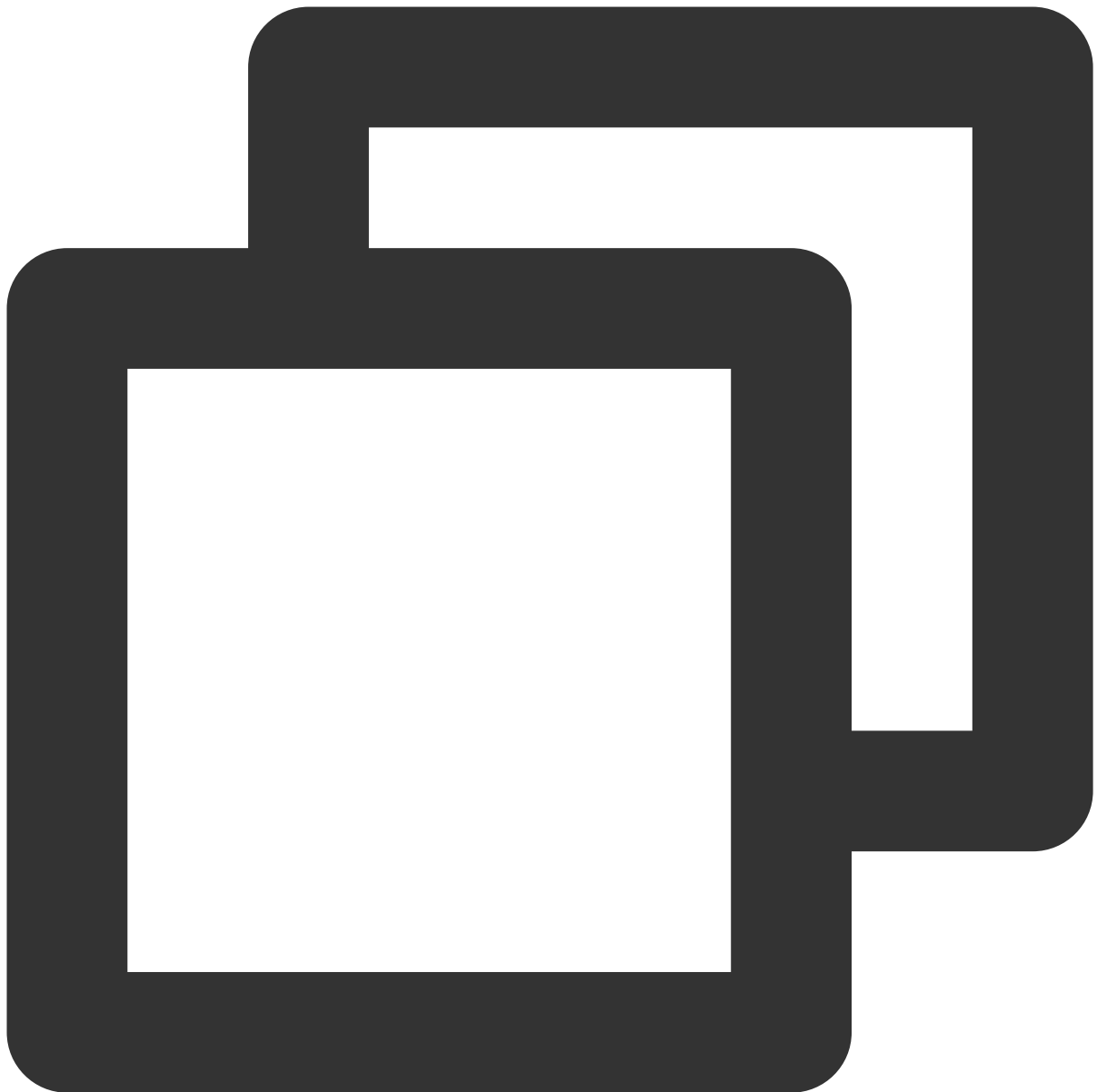
In Guangzhou region, the Lighthouse and TencentDB for Redis instructed in [Overview](#) are not interconnected by default. You need to associate Redis with CCN to implement the interconnection.

### Prerequisites

TencentDB for Redis uses private network port `6397` by default. Allow this port in the inbound rules of the security group associated with the Redis instance. For details, see [Configuring Security Group](#).

### Steps

1. Log in to the Lighthouse instance and run the following command:

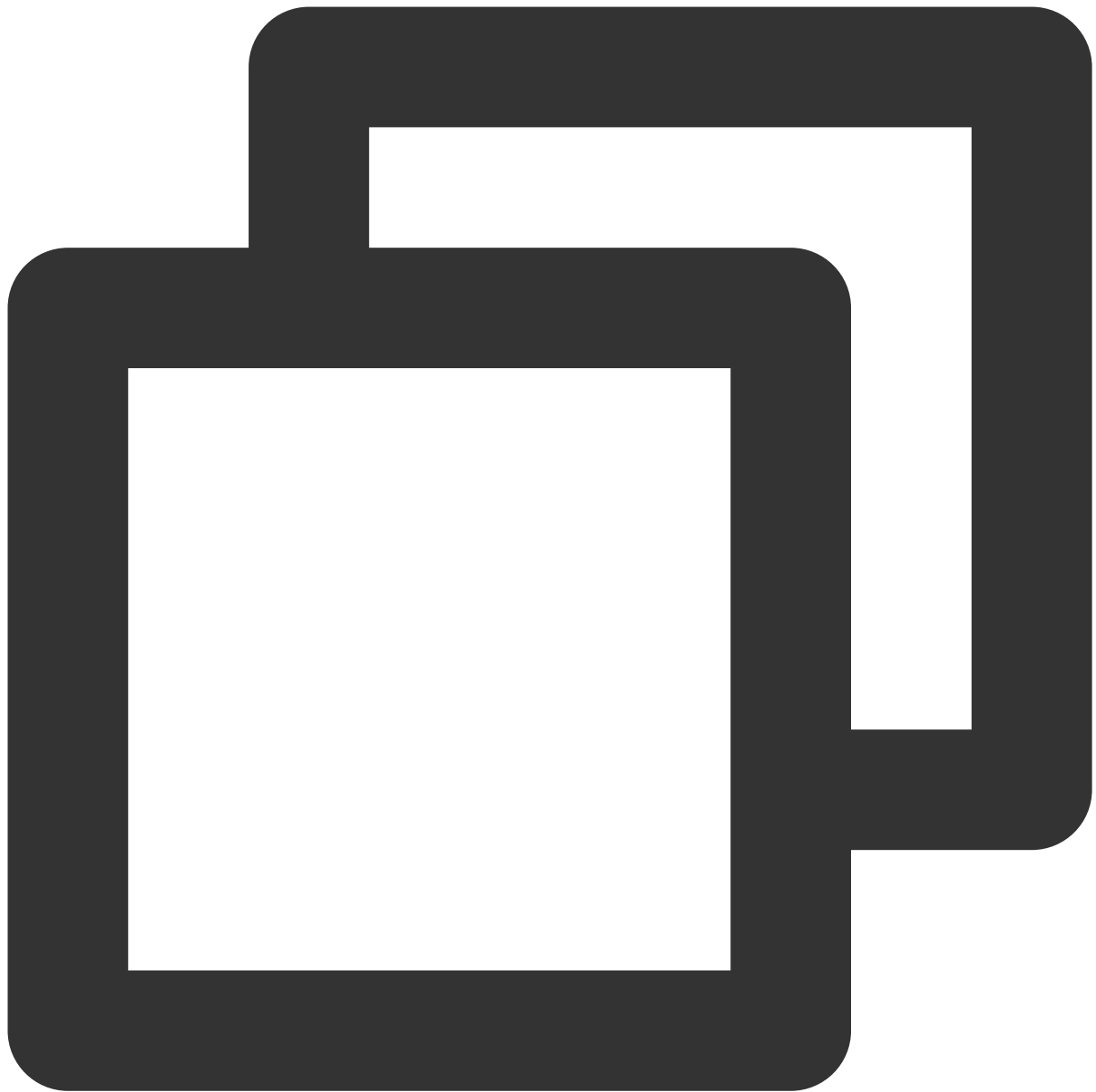


```
ping the Redis instance's private IP
```

If the following information is returned, the IP cannot be pinged:

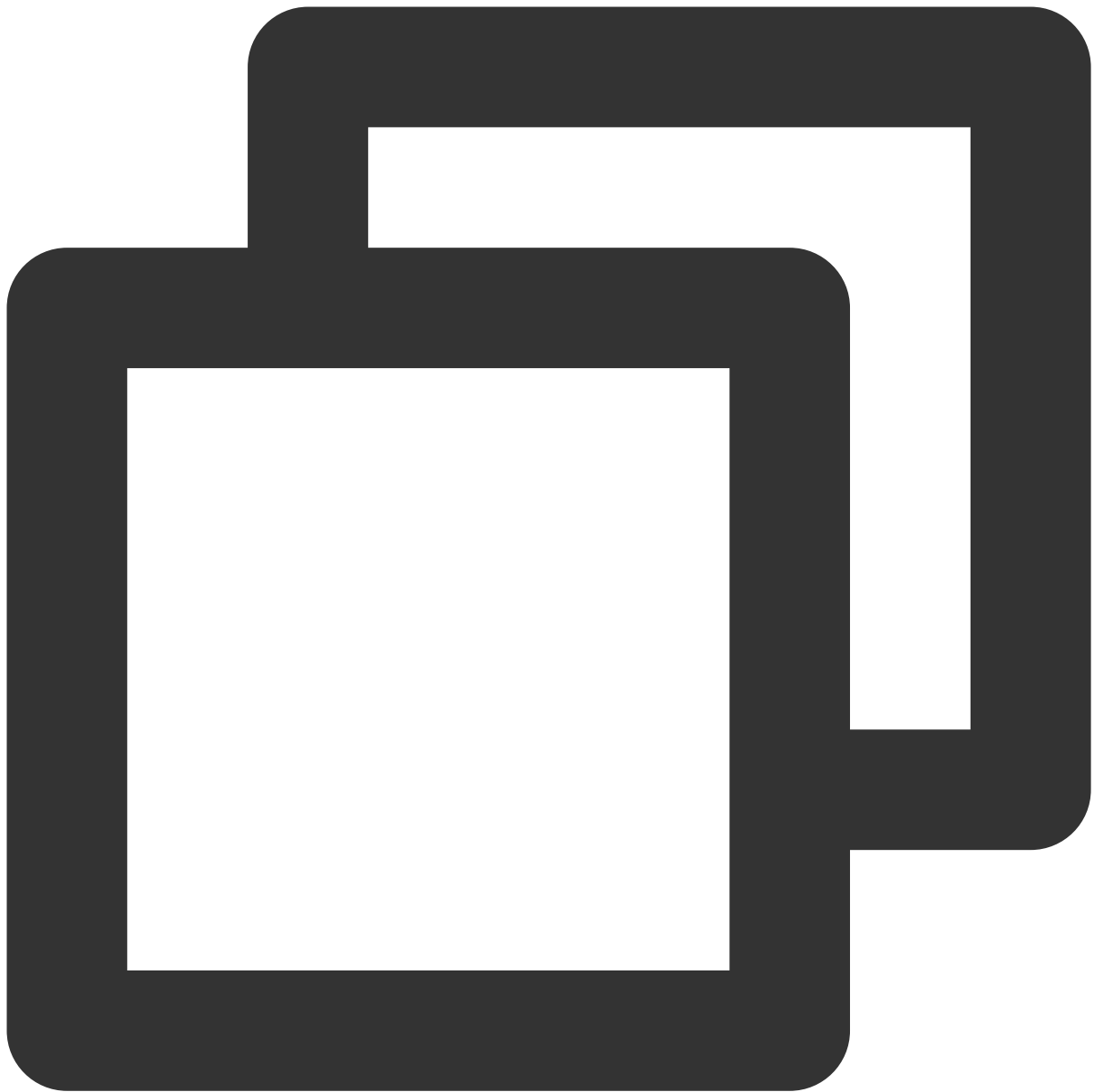
```
[lighthouse@VM-21-22-centos ~]$ ping 10.18.12.13
PING 10.18.12.13 (10.18.12.13) 56(84) bytes of data.
^C
--- 10.18.12.13 ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 13290ms
```

2. Run the following command to install `telnet` . Take a Lighthouse instance using CentOS as an example.



```
sudo yum install telnet -y
```

3. Run the following command to test whether the interconnection is successful or not.



```
telnet the Redis instance's private IP 6379
```

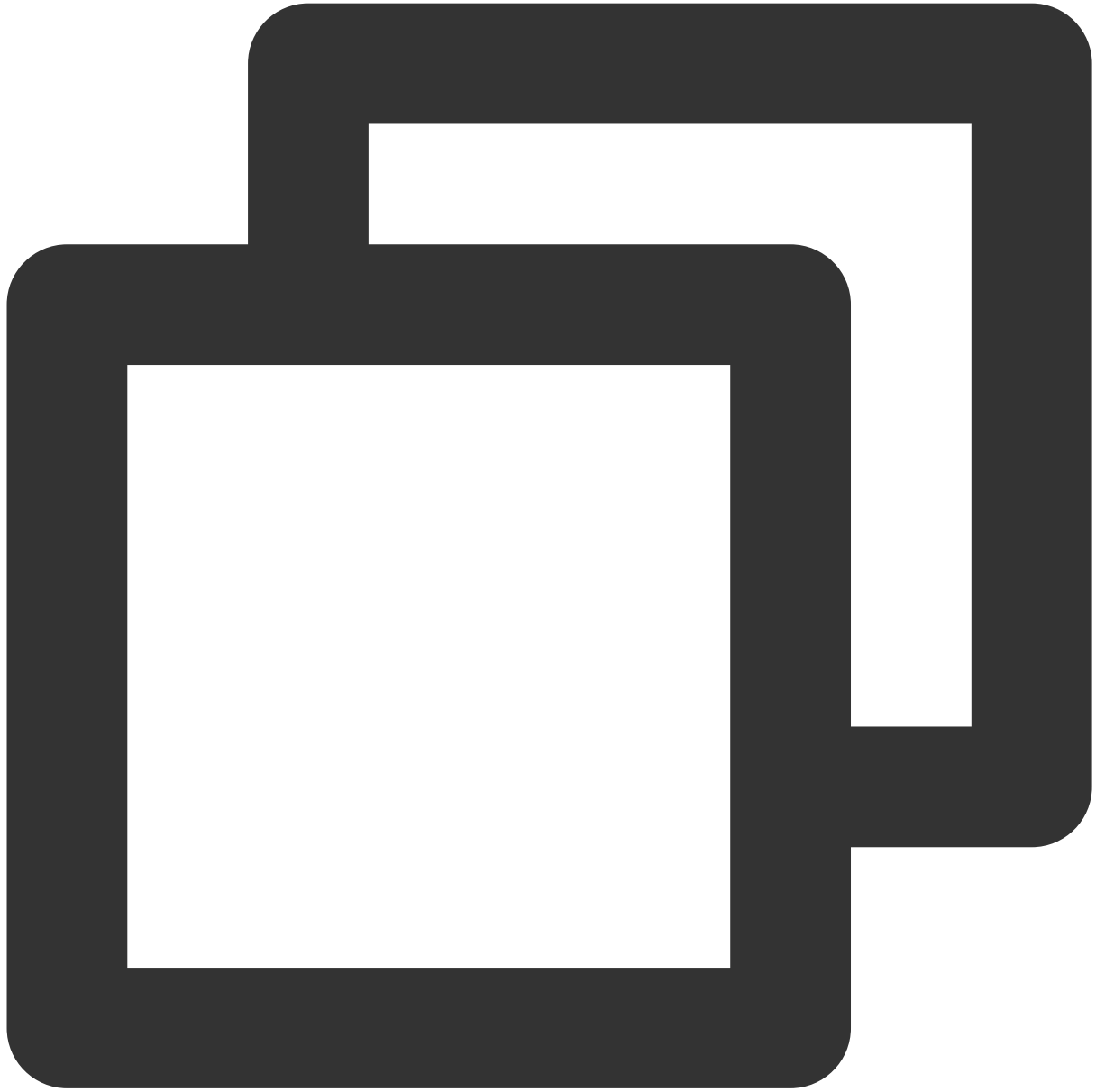
If the following information is returned, the interconnection fails.

```
[lighthouse@VM-21-22-centos ~]$ telnet 10.10.12.13 6379
Trying 10.10.12.13...
telnet: connect to address 10.10.12.13: Connection timed out
```

4. Associate with a CCN as instructed in [Applying for associating with a CCN](#).

Associate the VPC of TencentDB for Redis with the CCN instance as instructed in [Associating Network Instances](#).

5. Log in to the Lighthouse instance and run the following command:



```
telnet the Redis instance's private IP 6379
```

If the following information is returned, the interconnection succeeds.

```
[lighthouse@VM-21-22-centos ~]$ telnet 10.10.10.10 6379
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.
```



---

6. Connect the Lighthouse instance to a Redis instance as instructed in [Connecting to TencentDB for Redis Instance](#).

# OPS and Monitoring

## Instance Monitoring

Last updated : 2022-06-17 11:50:08

### Overview

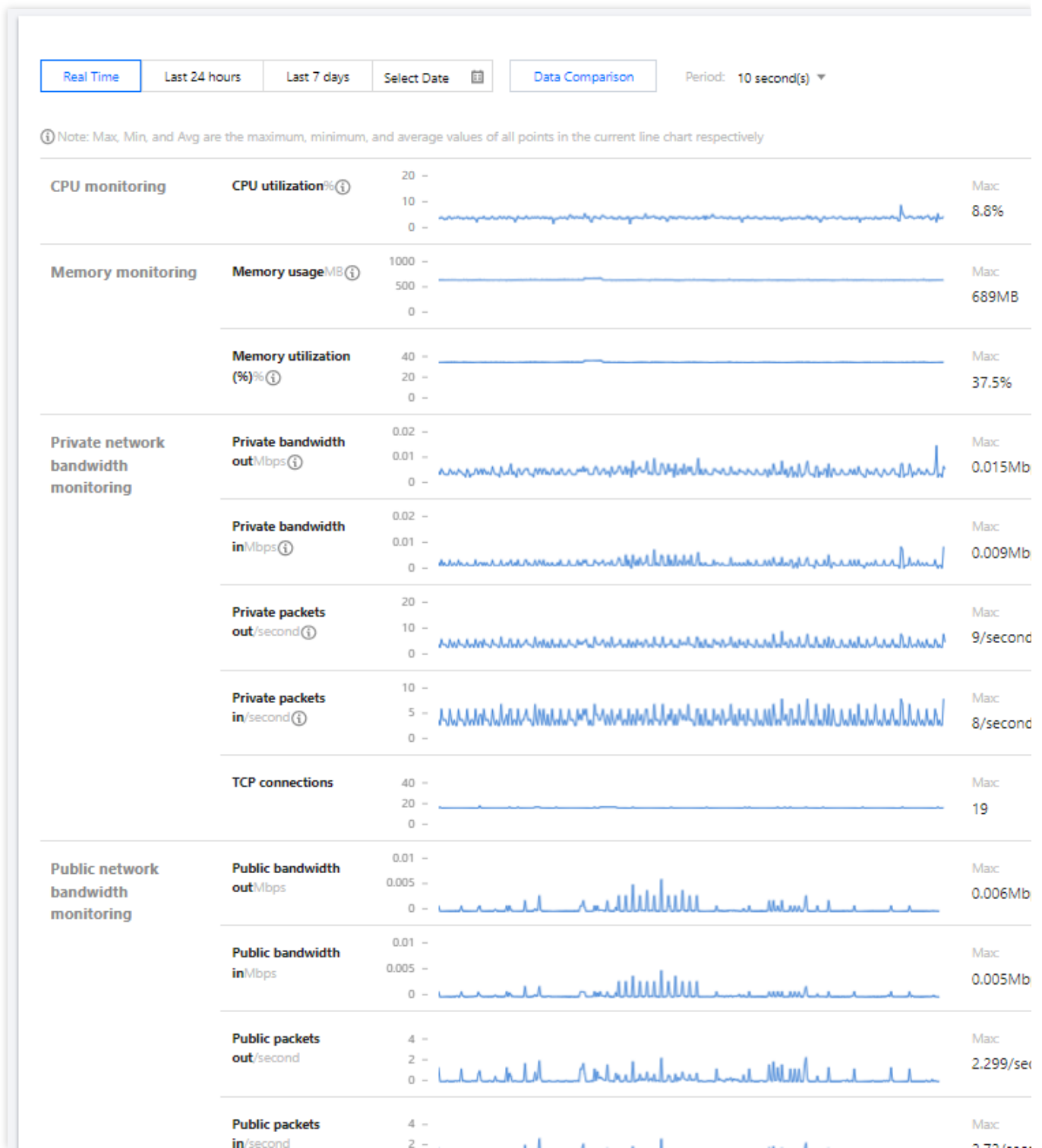
You can log in to the Lighthouse console and enter the instance details page to view the monitoring data of an instance.

### Directions

1. Log in to the [Lighthouse console](#).
2. Find the target instance in the instance list and enter its details page.
3. Select the **Monitoring** tab to enter the monitoring data page, where you can view the instance's monitoring data such as CPU, memory, private network bandwidth, public network bandwidth, and disk (system disk and data disk) usage as shown below:

**Note:**

If you want to set threshold alarms for the performance metrics of Lighthouse resources supported by [Cloud Monitor](#), so that when an exception occurs, you can promptly receive a notification by WeChat, email, SMS, or phone call and take corresponding actions, you need to click **Set alarm** to create an alarm policy. For more information, see [Creating Alarm Policy](#).



## Related Operations

### Getting CloudAudit operation records

Lighthouse supports [CloudAudit](#). You can get operation records in the CloudAudit console in the following steps. For more information on CloudAudit operation records, see [Viewing Event Details in Operation Record](#).

1. Log in to the CloudAudit console and select **Operation Record** on the left sidebar.
2. Select **LIGHTHOUSE** for **Resource Event Name** and click **Query** to view the logs as shown below:

Last 30 minutesLast hourLast dayLast 7 daysSpecify

Operation TypeWrite-only

Resource Event NameLIGHTHOUSE

Username

Sensitive OperationAll

Query

Reset

Unfold

	Event Time	Modified by	Event Name	Resource Type
<input type="checkbox"/> +	2022-03-29 15:59:48	root	ResetInstance	lighthouse
<input type="checkbox"/> +	2022-03-29 15:57:24	root	CreateBlueprint	lighthouse
<input type="checkbox"/> +	2022-03-29 15:50:46	root	CreateInstanceSnapshot	lighthouse
<input type="checkbox"/> +	2022-03-29 15:00:32	root	StartInstances	lighthouse
<input type="checkbox"/> +	2022-03-29 14:50:45	root	StopInstances	lighthouse

# Access Management

## CAM Overview

Last updated : 2022-05-12 12:24:12

If you have multiple users managing different Tencent Cloud services such as Lighthouse, VPC, and TencentDB, and they all share your Tencent Cloud account access key, you may face the following problems:

The risk of your key being compromised is high since multiple users are sharing it.

Your users might introduce security risks from maloperations due to the lack of user access control.

You can use [Cloud Access Management \(CAM\)](#) to allow different users to manage different services through sub-accounts so as to avoid the above problems. By default, a sub-account doesn't have the permission to use Lighthouse or its relevant resources. Therefore, you need to create a policy to grant the required permission to the sub-account. You can skip this section if you don't need to manage permissions to Lighthouse resources for sub-accounts, which will not affect your understanding and use of the other sections of the document.

## Features

CAM is a web-based Tencent Cloud service that helps you securely manage and control the access permissions of resources under your Tencent Cloud account. With CAM, you can create, manage, and terminate users or user groups and use identities and policies to control user access to Tencent Cloud resources. When using CAM, you can associate a policy with a user or user group to allow or forbid them to use specified resources to complete specified tasks.

Lighthouse has been connected to CAM, so you can use CAM to control the permissions of the Lighthouse resources.

## Concepts

### CAM users

A CAM user is an entity you create in Tencent Cloud. Each CAM user is associated with one Tencent Cloud account. The identity of your registered Tencent Cloud account is the **root account**, and you can create **sub-accounts** with different permissions for collaboration through [user management](#). The types of sub-accounts include [sub-user](#), [collaborator](#), and [message recipient](#).

### Policies

A [policy](#) is the syntax rule used to define and describe one or more permissions. CAM supports two types of policies: preset policy and custom policy.

Preset policies: Policies created and managed by Tencent Cloud. These are some common permission sets that are frequently used by users, such as full read and write permissions for resources. Preset policies have a wide range of operation objects, coarse operation granularity, and are preset by the system. They cannot be edited by users.

Custom policies: Policies created by users. These permit fine-grained division of permissions. For example, a usage policy is associated with a sub-account that gives the sub-account management permissions for the scaling groups of Auto Scaling, but no management permissions for TencentDB instances.

## Resources

[Resource](#) is an element of policies that describes one or multiple operation objects. For example, the launch configuration and scaling groups of Auto Scaling.

# Authorizable Resource Types

Last updated : 2022-05-12 12:24:12

With Cloud Access Management (CAM), you can grant resource-level permissions for users.

In CAM, the types of Lighthouse resources that can be authorized are as follows:

Resource Type	Resource Description Method in Authorization Policy
Instance	qcs::lighthouse:\$region:\$account:instance/*
Image	qcs::lighthouse:\$region:\$account:blueprint/*
Snapshot	qcs::lighthouse:\$region:\$account:snapshot/*
Key	qcs::lighthouse:\$region:\$account:keypair/*

The table below lists the API operations of Lighthouse that currently support resource-level permissions, as well as their resources and condition keys. When setting the resource path, you need to replace the variable parameters such as `$region` and `$account` with your actual parameter values. You can also use the `*` wildcard in the path. For relevant concepts such as `region`, `action`, `account`, and `resource` in CAM policies, see [Resource Description Method](#).

## Note:

Lighthouse API operations not listed here do not support resource-level permissions. You can still authorize a user to perform such an API operation, but you must specify `*` as the resource element of the policy statement.

## Instance

API	Resource
ModifyInstancesBundle	qcs::lighthouse:\$region:\$account:instance/\$instanceId
RenewInstances	qcs::lighthouse:\$region:\$account:instance/\$instanceId
IsolateInstances	qcs::lighthouse:\$region:\$account:instance/\$instanceId
ModifyInstancesAttribute	qcs::lighthouse:\$region:\$account:instance/\$instanceId
ModifyInstancesRenewFlag	qcs::lighthouse:\$region:\$account:instance/\$instanceId
RebootInstances	qcs::lighthouse:\$region:\$account:instance/\$instanceId
ResetInstance	qcs::lighthouse:\$region:\$account:instance/\$instanceId

ResetInstancesPassword	qcs::lighthouse:\$region:\$account:instance/\$instanceId
StartInstances	qcs::lighthouse:\$region:\$account:instance/\$instanceId
StopInstances	qcs::lighthouse:\$region:\$account:instance/\$instanceId
TerminateInstances	qcs::lighthouse:\$region:\$account:instance/\$instanceId
DescribeInstancesDeniedActions	qcs::lighthouse:\$region:\$account:instance/\$instanceId
DescribeInstancesReturnable	qcs::lighthouse:\$region:\$account:instance/\$instanceId
DescribeInstancesTrafficPackages	qcs::lighthouse:\$region:\$account:instance/\$instanceId
DescribeInstanceVncUrl	qcs::lighthouse:\$region:\$account:instance/\$instanceId
DescribeResetInstanceBlueprints	qcs::lighthouse:\$region:\$account:instance/\$instanceId

## Snapshot

API	Resource
CreateInstanceSnapshot	qcs::lighthouse:\$region:\$account:instance/\$instanceIdqcs::lighthouse:\$region
DeleteSnapshots	qcs::lighthouse:\$region:\$account:snapshot/\$snapshotId
ApplyInstanceSnapshot	qcs::lighthouse:\$region:\$account:instance/\$instanceIdqcs::lighthouse:\$region
DescribeSnapshotsDeniedActions	qcs::lighthouse:\$region:\$account:snapshot/\$snapshotId
ModifySnapshotAttribute	qcs::lighthouse:\$region:\$account:snapshot/\$snapshotId

## Firewall

API	Resource
CreateFirewallRules	qcs::lighthouse:\$region:\$account:instance/\$instanceId
DeleteFirewallRules	qcs::lighthouse:\$region:\$account:instance/\$instanceId
DescribeFirewallRules	qcs::lighthouse:\$region:\$account:instance/\$instanceId
ModifyFirewallRules	qcs::lighthouse:\$region:\$account:instance/\$instanceId



ModifyFirewallRuleDescription	qcs::lighthouse:\$region:\$account:instance/\$instanceId
-------------------------------	--

## Key

API	Resource
DeleteKeyPairs	qcs::lighthouse:\$region:\$account:keypair/\$keypairId
AssociateInstancesKeyPairs	qcs::lighthouse:\$region:\$account:instance/\$instanceIdqcs::lighthouse:\$
DescribeInstanceLoginKeyPairAttribute	qcs::lighthouse:\$region:\$account:instance/\$instanceId
DisassociateInstancesKeyPairs	qcs::lighthouse:\$region:\$account:instance/\$instanceIdqcs::lighthouse:\$
ModifyInstancesLoginKeyPairAttribute	qcs::lighthouse:\$region:\$account:instance/\$instanceId

## Image

API	Resource
CreateBlueprint	qcs::lighthouse:\$region:\$account:instance/\$instanceIdqcs::lighthouse:\$region:\$acc
DeleteBlueprints	qcs::lighthouse:\$region:\$account:blueprint/\$blueprintId
DescribeBlueprintInstances	qcs::lighthouse:\$region:\$account:instance/\$instanceId
ModifyBlueprintAttribute	qcs::lighthouse:\$region:\$account:blueprint/\$blueprintId

## Bundle

API	Resource
DescribeModifyInstanceBundles	qcs::lighthouse:\$region:\$account:instance/\$instanceId

## Billing

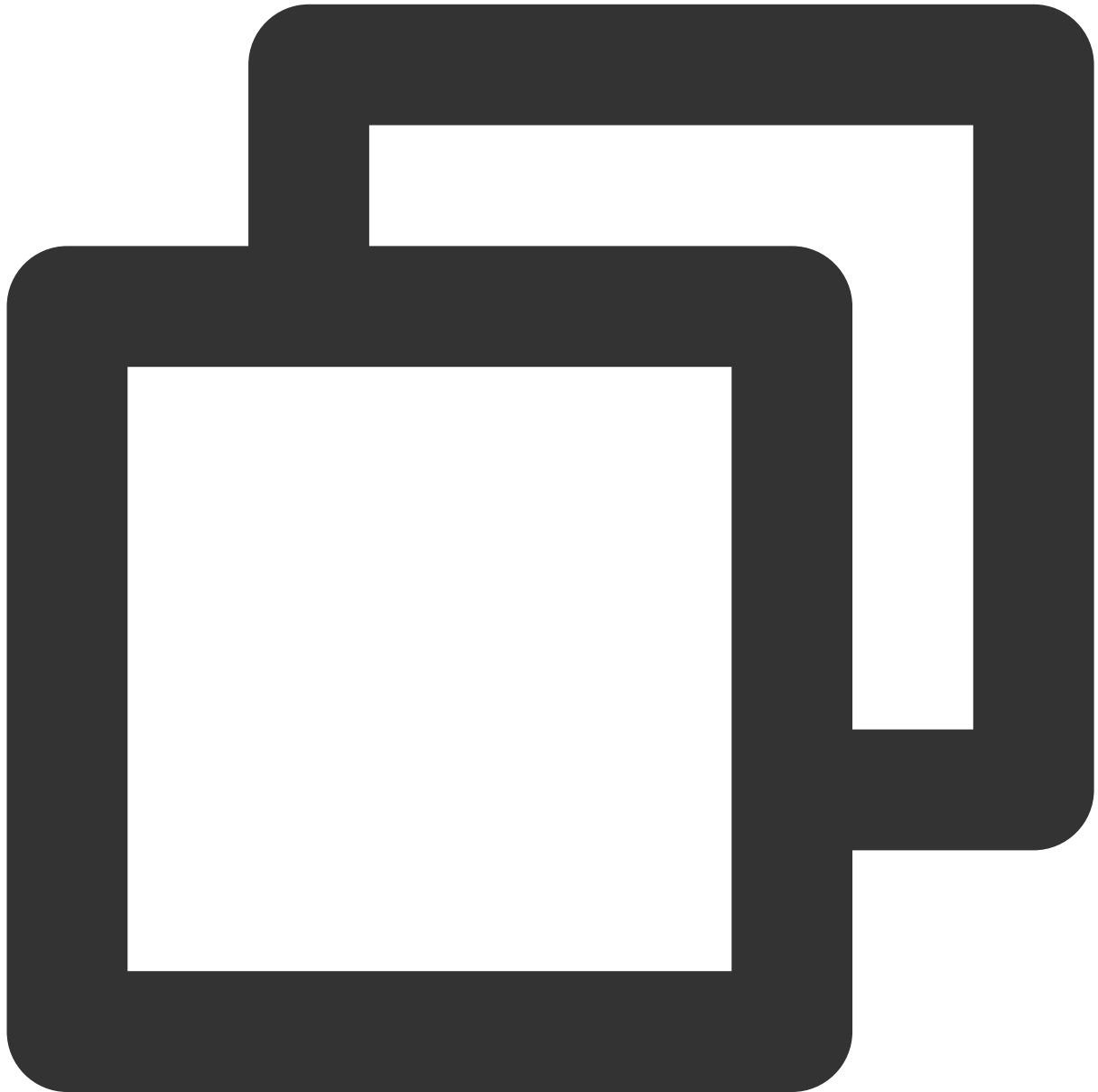
API	Resource
-----	----------

InquirePriceRenewInstances	qcs::lighthouse:\$region:\$account:instance/\$instanceId
----------------------------	--

# Authorization Policy Syntax

Last updated : 2022-05-12 12:24:12

## Policy syntax



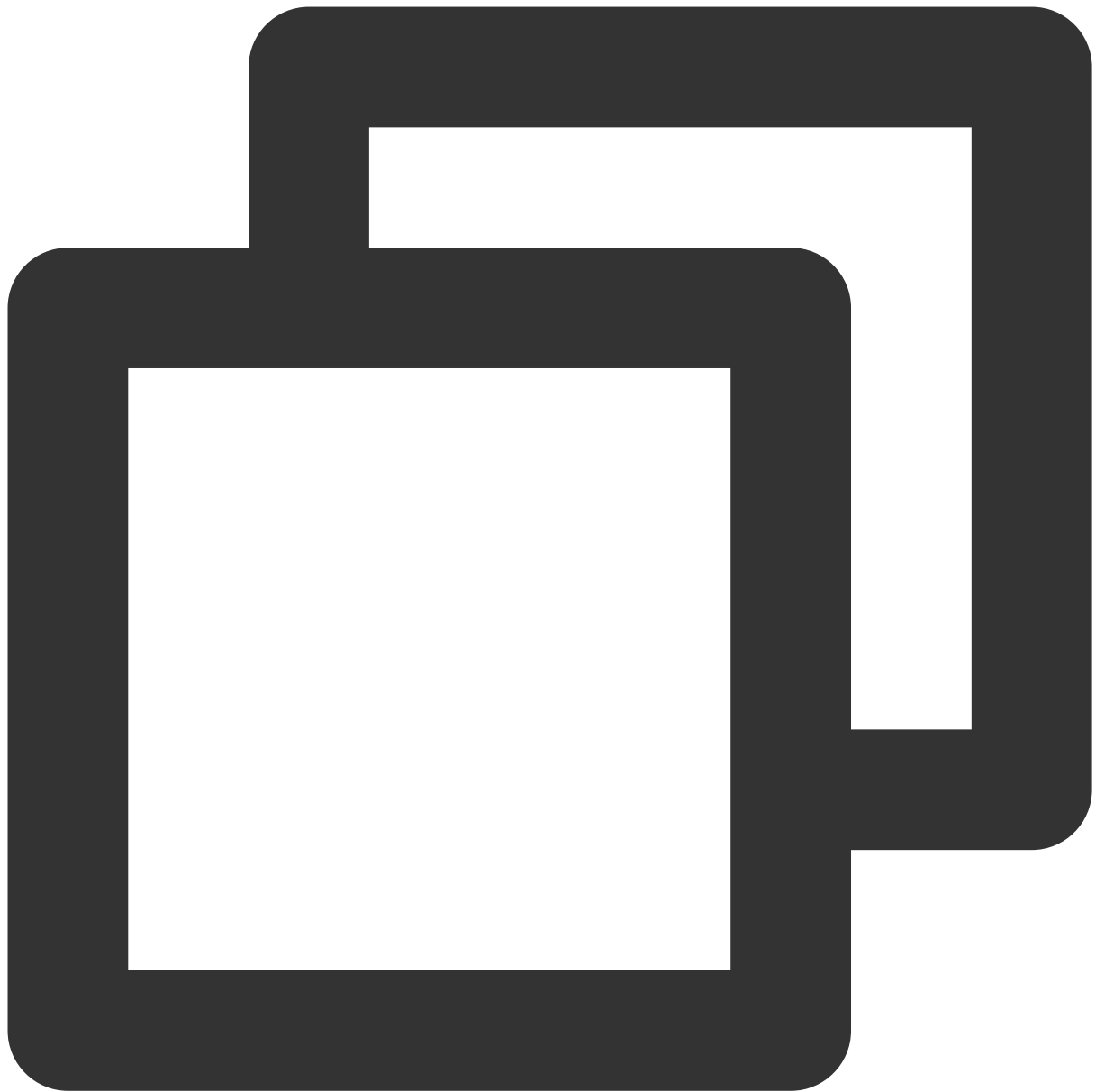
```
{  
  "version": "2.0",  
  "statement":  
  [  
    {  
      "action": "tencentcloud:iam:CreatePolicy",  
      "resource": "tencentcloud:iam:policy/*",  
      "effect": "allow",  
      "principal": "tencentcloud:iam:role/*",  
      "condition": {}  
    }  
  ]  
}
```

```
{
  "effect": "effect",
  "action": ["action"],
  "resource": ["resource"],
  "condition": { "key": { "value": "" } }
}
```

Element	Description
version	It is required. Currently, only the value "2.0" is allowed.
statement	It describes the details of one or more permissions. It contains a permission or permission set of multiple other elements such as `effect`, `action`, `resource`, and `condition`. One policy has only one `statement`.
effect	It is required and describes whether the statement result is an "allow" or an explicit "deny".
action	It is required and describes the allowed or denied action (operation). An operation can be an API (prefixed with "name") or a feature set (a set of specific APIs prefixed with "permid").
resource	It is required and describes the details of authorization. A resource is described in a six-segment format. Detailed resource definitions vary by product. For more information on how to specify a resource, see the product documentation corresponding to the resource statement you are writing.
condition	It is optional and describes the condition for the policy to take effect. A condition consists of an operator, action key, and action value. A condition value may contain information such as time and IP address. Some services allow you to specify additional values in a condition.

## Sample CAM Policy for Lighthouse

The following policy grants the permission to view the list of Lighthouse instances and prohibits the user `xxxxxxx` from viewing the details of the instance `lhins-e31oxxxx`.

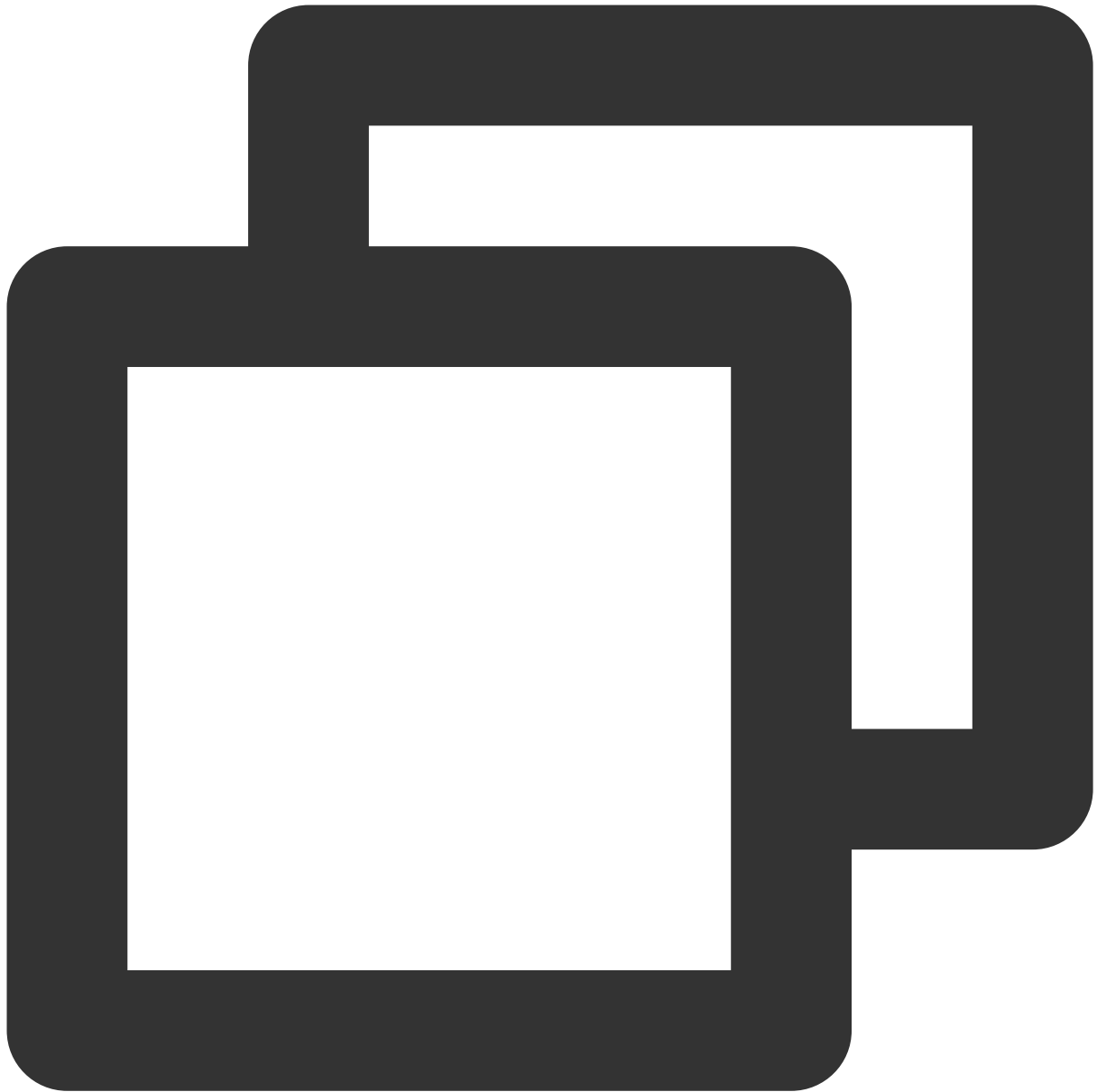


```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "lighthouse:DescribeInstances"
      ],
      "resource": [
        "*"
      ]
    }
  ]
}
```

```
    },  
    {  
      "effect": "deny",  
      "action": [  
        "lighthouse:DescribeInstances"  
      ],  
      "resource": [  
        "qcs::lighthouse::uin/xxxxxx:instance/lhins-e31oxxxx"  
      ]  
    }  
  ]  
}
```

## Lighthouse Resource Path

Each Lighthouse policy statement has its own applicable resources generally in the following format:



```
qcs:project_id:service_type:region:account:resource
```

**project\_id:** Describes the project information, which is only used to enable compatibility with legacy CAM logic and can be left empty.

**service\_type:** Describes the product abbreviation such as `lighthouse` .

**region:** Describes the region information, such as `ap-guangzhou` .

**account:** Describes the root account of the resource owner, such as `uin/xxxxxx` .

**resource:** Detailed resource information of each product, for example, `instance/instance_id1` or `instance/*`.

# Transferring File

## Uploading Local Files to Lighthouse

Last updated : 2022-09-26 11:28:02

This document describes how to upload local files to a Lighthouse instance or download the files on it to your local file system.

## Transfer Method

### Using TencentCloud Automation Tools to transfer files

You can use TencentCloud Automation Tools to upload a local file to a Lighthouse instance or download a file on it to your local file system through the browser.

Operation	Use Limits
Uploading a file to a Lighthouse instance	Only a text file of up to 36 KB in size can be uploaded. Only the uploaded files can be downloaded.
<a href="#">Log in to a Lighthouse instance with WebShell for file upload/download</a>	Only Lighthouse instances on Linux are supported. Files can be uploaded only to the `home > lighthouse` directory.

### Other methods

Follow the instructions below based on your local operating system and the operating system of the purchased Lighthouse instance.

Local OS	Lighthouse Instance OS (Linux)	Lighthouse Instance OS (Windows)
Windows	<a href="#">Upload files to a Lighthouse instance via WinSCP</a> <a href="#">Upload files to a Lighthouse instance via FTP</a>	<a href="#">Upload files to a Lighthouse instance via remote desktop</a>
Linux	<a href="#">Upload files to a Lighthouse instance via SCP</a> <a href="#">Upload files to a Lighthouse instance via FTP</a>	<a href="#">Upload files to a Lighthouse instance via remote desktop</a>
macOS		<a href="#">Upload files to a Lighthouse instance via remote</a>



		desktop
--	--	---------

For example, if you use Windows on your local computer and have a Linux Lighthouse instance, you can use WinSCP to upload files to the instance.

## Subsequent Operations

If you need to back up important business data or personal files, you can create a snapshot of the Lighthouse instance's system disk after uploading the files to the instance. For more information on the use cases and usage methods of snapshots, see [Managing Snapshot](#).

## Problem?

[Submit a ticket](#) or use related documentation to troubleshoot.

# Uploading File from Windows to Linux Lighthouse Instance via WinSCP

Last updated : 2022-05-12 12:24:12

## Overview

WinSCP is an open-source graphical SFTP client that uses SSH in Windows environment and supports SCP protocol. Its main feature is to copy files securely between the local and remote computers. Unlike uploading codes via FTP, you can directly use your instance account in WinSCP to access the instance without any additional configuration.

## Prerequisites

WinSCP has been downloaded and installed on the local computer. [Download the latest WinSCP](#).

You have obtained the Lighthouse instance admin account and password.

The default admin username of a Linux Lighthouse instance is `root`, and that of an Ubuntu instance is `ubuntu`.

You can also customize the username.

If you forgot your password, you can [reset it](#).

## Directions

### Logging in to WinSCP

1. Open WinSCP, and the "WinSCP Login" box pops up, as shown below:

**Login**

New Site

Session

File protocol:  
SFTP

Host name: Port number:  
22

User name: Password:

Save Advanced...

Tools Manage Login Close Help

☒ Show Login dialog on startup and when the last session is closed

2. Configure the following parameters:

**Protocol:** Either SFTP or SCP.

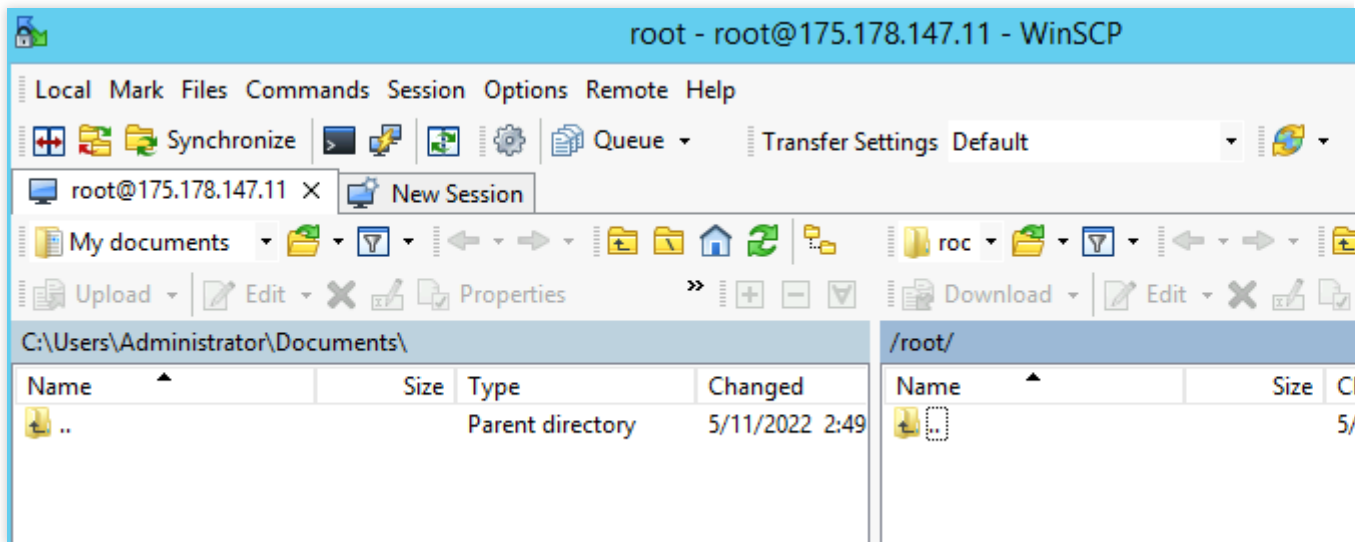
**Hostname:** Lighthouse instance public IP, which can be viewed in the [Lighthouse console](#).

**Port:** 22 by default.

**Username:** Lighthouse instance system username.

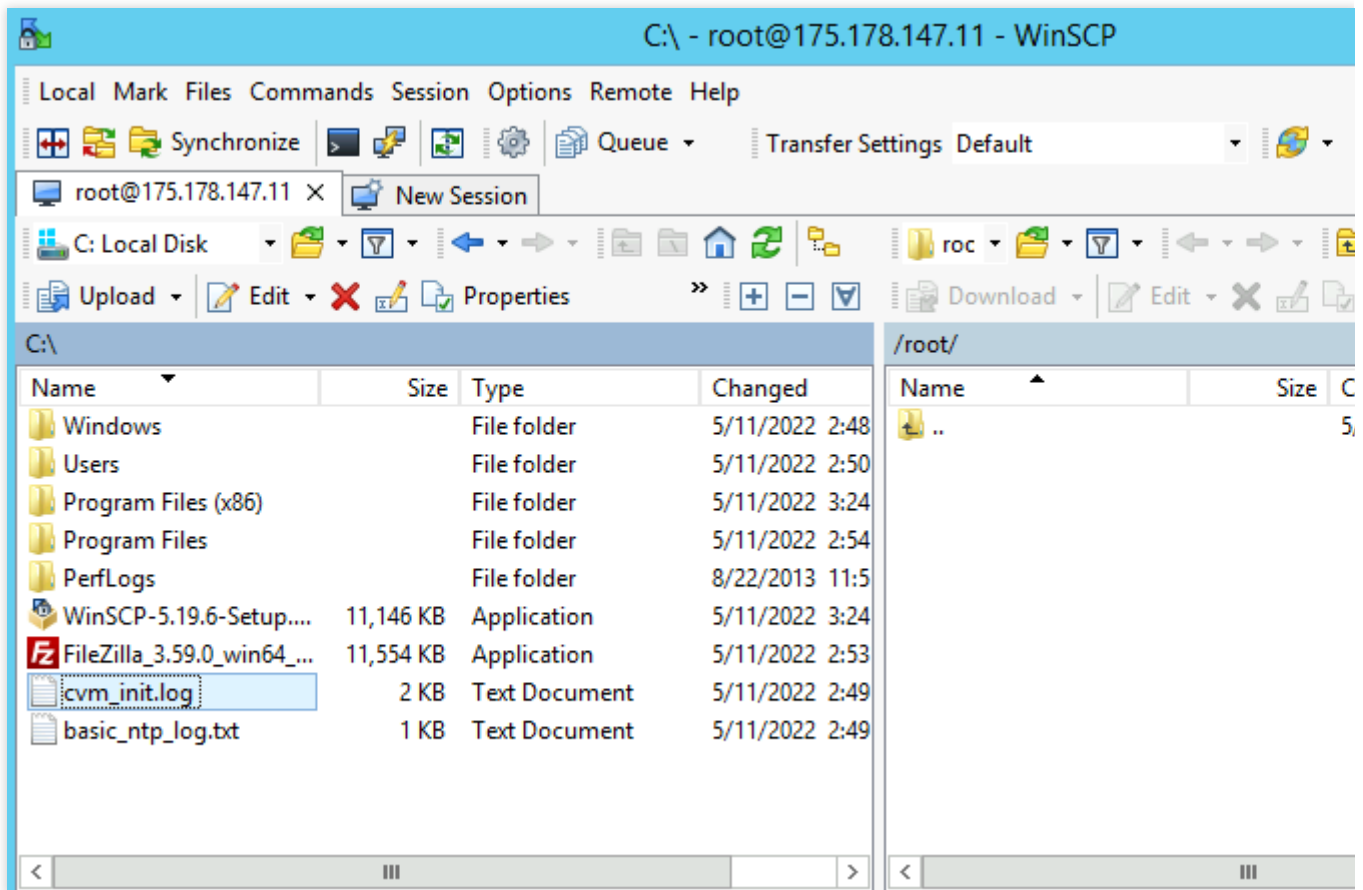
**Password:** Password of the Lighthouse instance system username.

3. Click **Login** to enter the **WinSCP** file transfer window as shown below:



## Uploading files

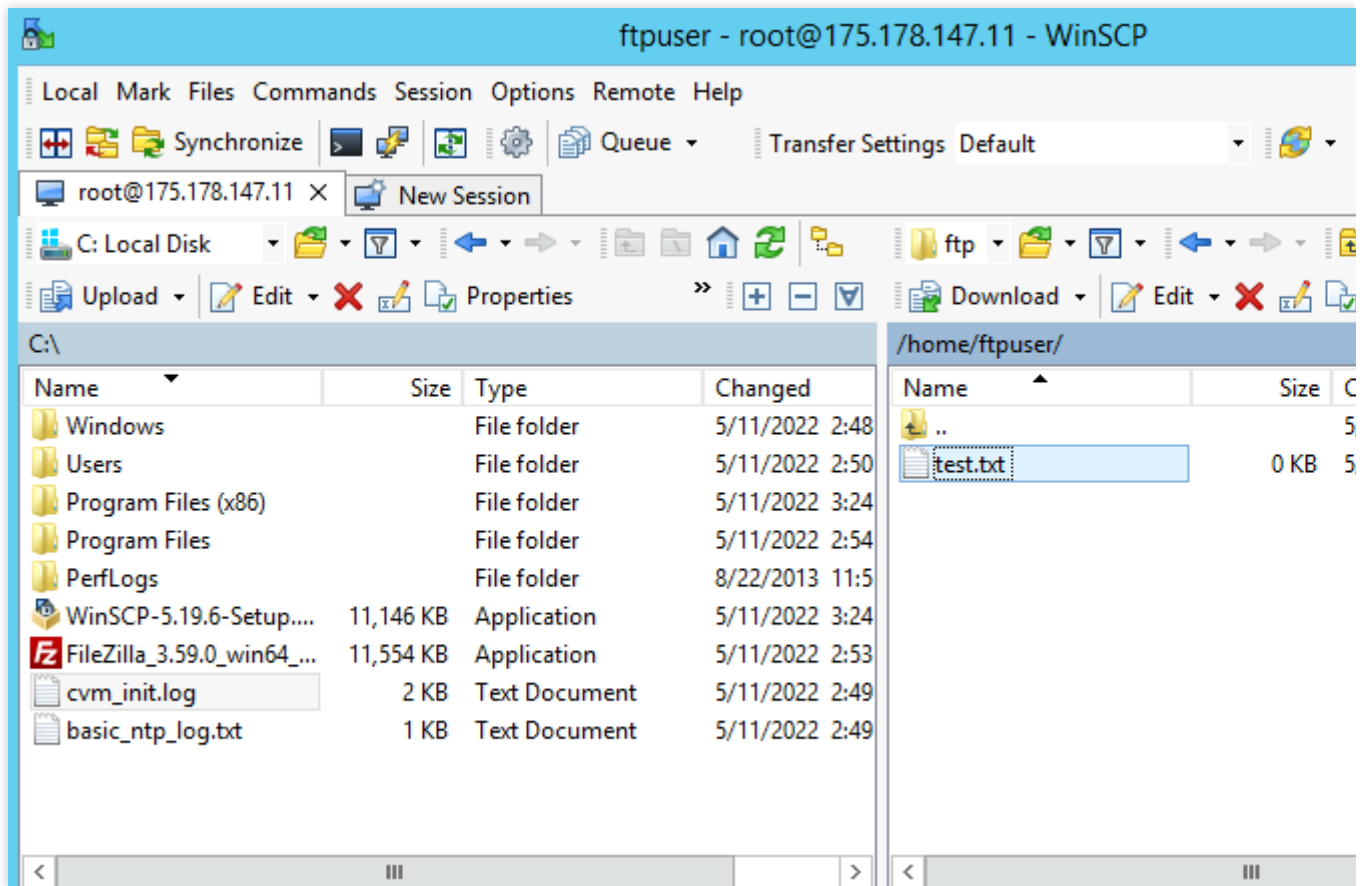
1. In the right pane of the "WinSCP" file transfer interface, select the directory where the files are to be stored on the server, such as "/user".
2. In the left pane, select the directory where the files are stored on the local computer, such as `F:\SSL` `certificate\Nginx` , and then select the files to be transferred.
3. In the left menu, click **Upload** as shown below:



4. In the "Upload" box that pops up, confirm the files to be uploaded and the remote directories, and click **OK** to upload the files from the local computer to the Lighthouse instance.

## Downloading files

1. In the left pane of the "WinSCP" file transfer page, select the local computer directory to store the downloaded files, such as "F:\SSL certificate\Nginx".
2. In the right pane, select the directory where the files locate, such as `/user` , and then select the file to be transferred.
3. In the right menu, click **Download** as shown below:



4. In the "Download" box that pops up, confirm the files to be downloaded and the remote directories, and click **OK** to download the files from the Lighthouse instance to the local computer.

# Uploading File from Windows to Lighthouse Instance via FTP

Last updated : 2022-05-12 12:30:33

## Overview

This document describes how to use the FTP service to upload files from a local Windows computer to a Lighthouse instance or download files from a Lighthouse instance to a local file system.

## Prerequisites

You have set up the FTP service in the Lighthouse instance.

## Directions

### Connecting to Lighthouse instance

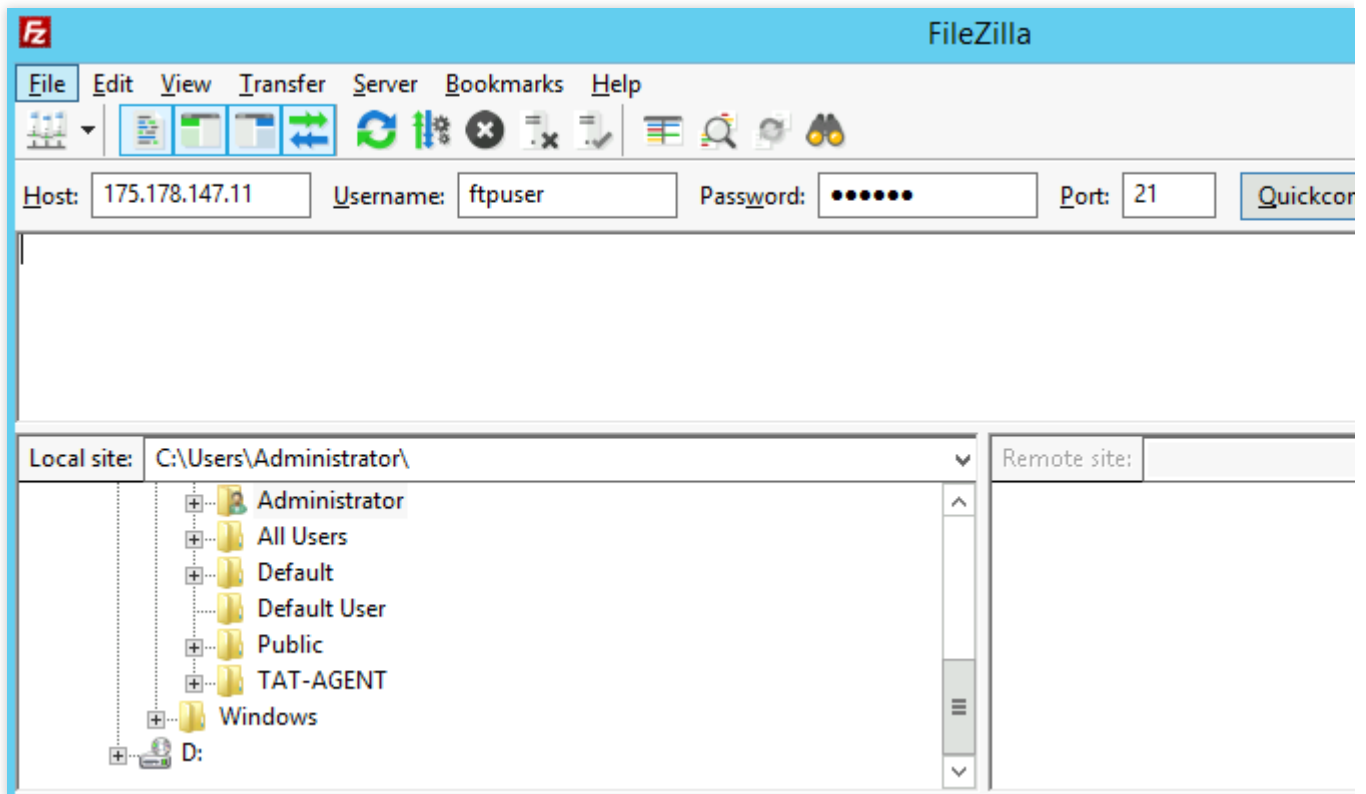
1. Download and install the open-source FileZilla locally.

**Note:**

If you use version 3.5.3 of FileZilla to upload files via FTP, the upload may fail. We recommend you download and use versions 3.5.1 or 3.5.2 of FileZilla from its [official website](#).

2. Open FileZilla.

3. In the FileZilla window, enter host, user name, password, and port information, and click **Quickconnect**, as shown below:



#### Configuration description:

**Host:** Lighthouse instance public IP, which can be viewed in the [Lighthouse console](#).

**Username:** FTP user account configured during FTP service setup. Here, `ftpuser1` is taken as an example in the image.

**Password:** Password of the FTP user account configured during FTP service setup.

**Port:** FTP listening port, which is **21** by default.

After the connection is successful, you can view the files on the remote Lighthouse instance site.

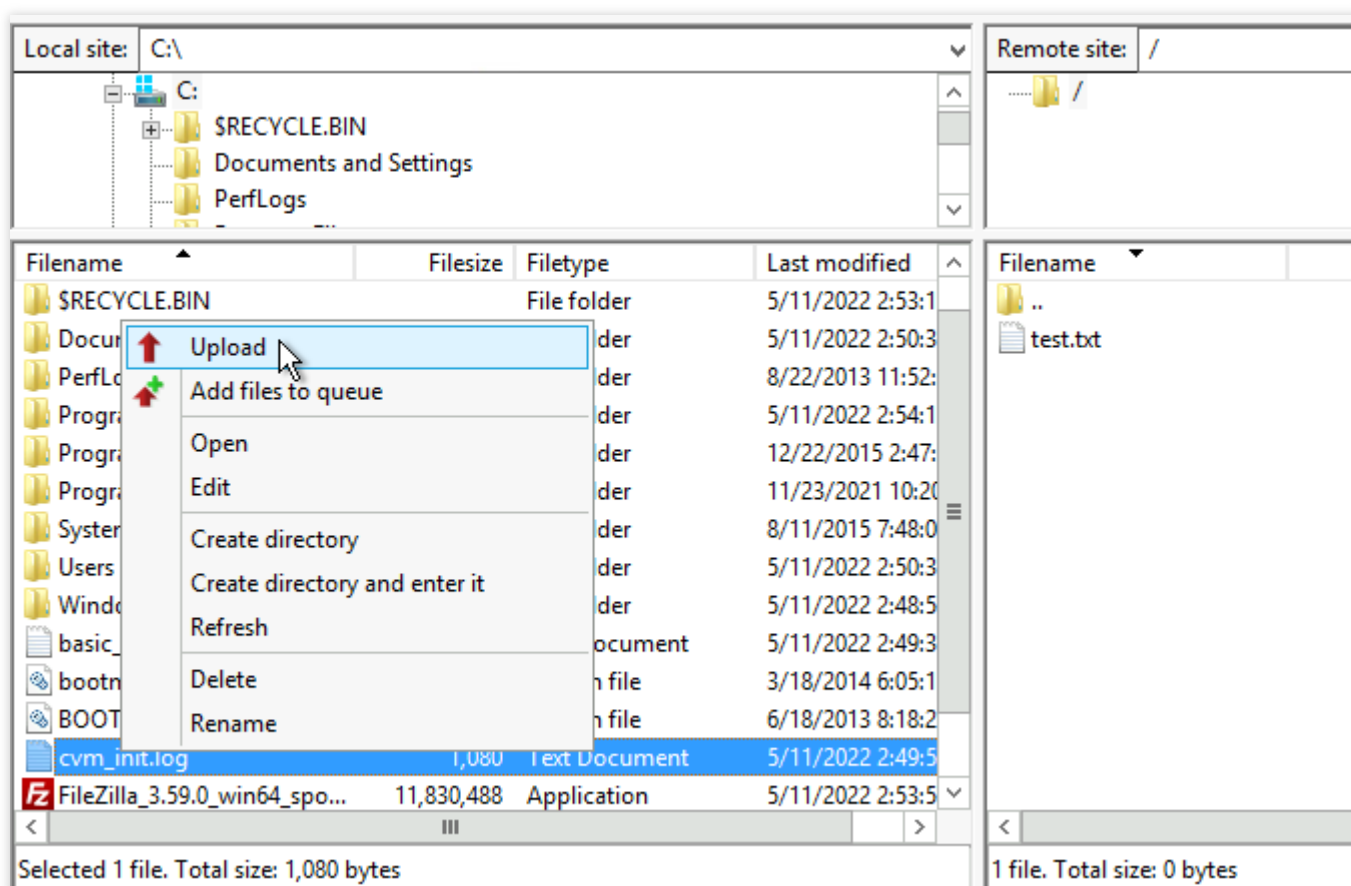
#### Uploading files

In the lower-left **Local site** window, right-click the local file to be uploaded and select **Upload** to upload it to a Linux Lighthouse instance, as shown below:

#### Note:

The Lighthouse FTP path does not support the automatic decompression or deletion of uploaded compressed tar files. The remote site path is the default path for uploading files to a Linux Lighthouse instance.





## Downloading files

In the lower-right **Remote site** window, right-click the Lighthouse instance file to be downloaded and choose **Download** to download it to a local directory as shown below:

Local site: C:\

C:

SRECYCLE.BIN

Documents and Settings

PerfLogs

Filename	Filesize	Filetype	Last modified
SRECYCLE.BIN		File folder	5/11/2022 2:53:1
Documents and Settings		File folder	5/11/2022 2:50:3
PerfLogs		File folder	8/22/2013 11:52:
Program Files		File folder	5/11/2022 2:54:1
Program Files (x86)		File folder	12/22/2015 2:47:
ProgramData		File folder	11/23/2021 10:20
System Volume Informati...		File folder	8/11/2015 7:48:0
Users		File folder	5/11/2022 2:50:3
Windows		File folder	5/11/2022 2:48:5
basic_ntp_log.txt	38	Text Document	5/11/2022 2:49:3
bootmgr	398,356	System file	3/18/2014 6:05:1
BOOTNXT	1	System file	6/18/2013 8:18:2
cvm_init.log	1,080	Text Document	5/11/2022 2:49:5
FileZilla_3.59.0_win64_spo...	11,830,488	Application	5/11/2022 2:53:5

Selected 1 file. Total size: 1,080 bytes

Remote site: /

..

test.txt

cvm\_init.log

Download

Add files to

View/Edit

Create direc

Create direc

Create new

Refresh

Delete

Rename

Copy URL(s)

File permiss

Filename	Filesize	Filetype	Last modified
..		File folder	
test.txt		Text Document	
cvm_init.log		Text Document	

Selected 1 file. Total size: 0 bytes

# Uploading File from Windows to Windows Lighthouse Instance via Remote Desktop Connection

Last updated : 2022-05-12 12:24:13

## Overview

Remote Desktop Connection is commonly used for file upload to a Windows Lighthouse instance. This document describes how to upload files from a Windows computer to a Windows Lighthouse instance by using Remote Desktop Connection or download files from the instance to a local file system.

## Prerequisites

You have obtained the Lighthouse instance admin account and password.

The default admin account of a Windows Lighthouse instance is `Administrator`.

If you forgot the login password, you can [reset it](#).

## Directions

### Note:

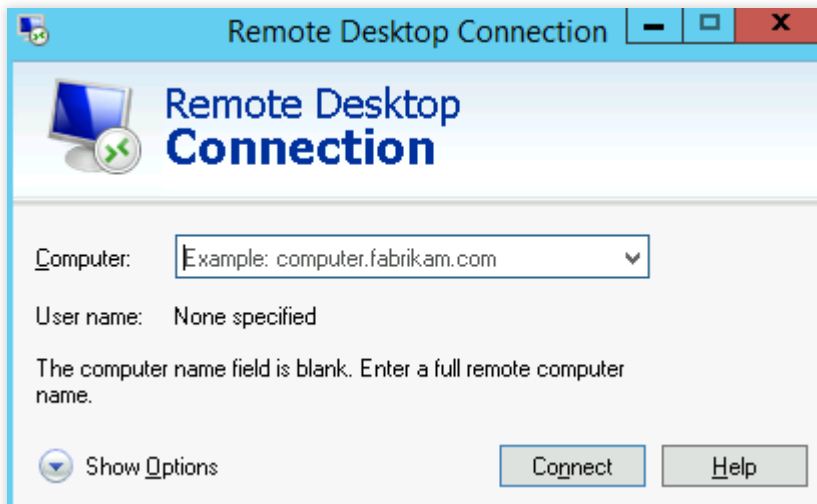
This document uses a Windows 7 computer as an example. The procedure may vary slightly according to the operating system version.

### Obtaining public IP

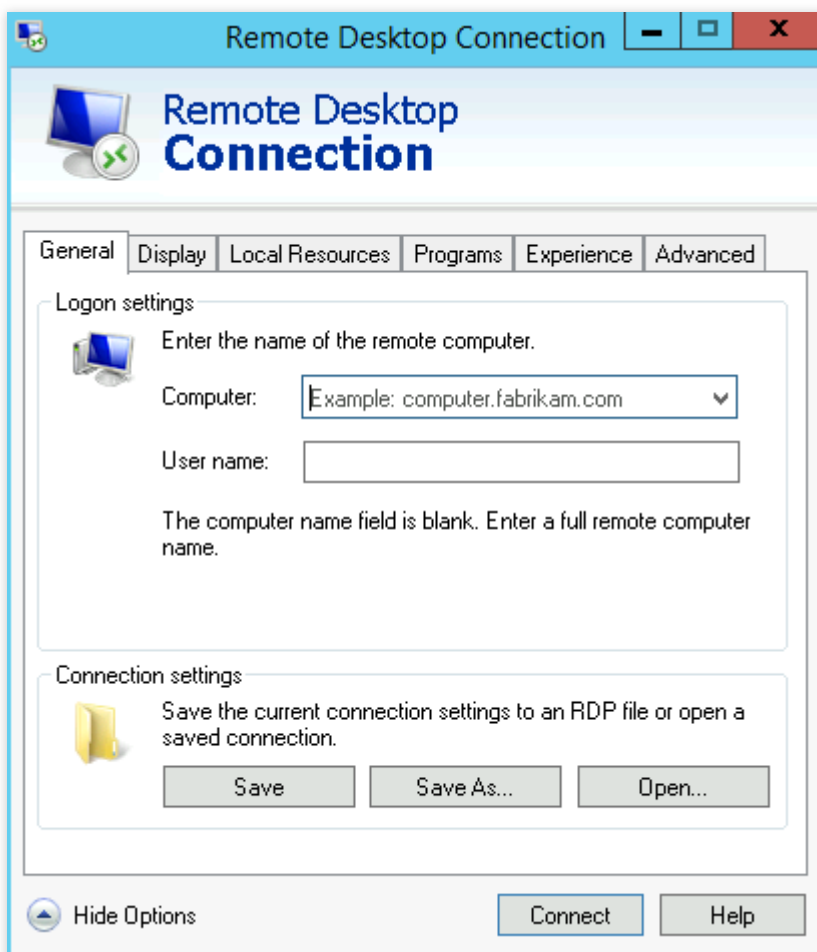
Log in to the [Lighthouse console](#) and get the public IP of the target Lighthouse instance on the **Instances** page.

### Uploading files

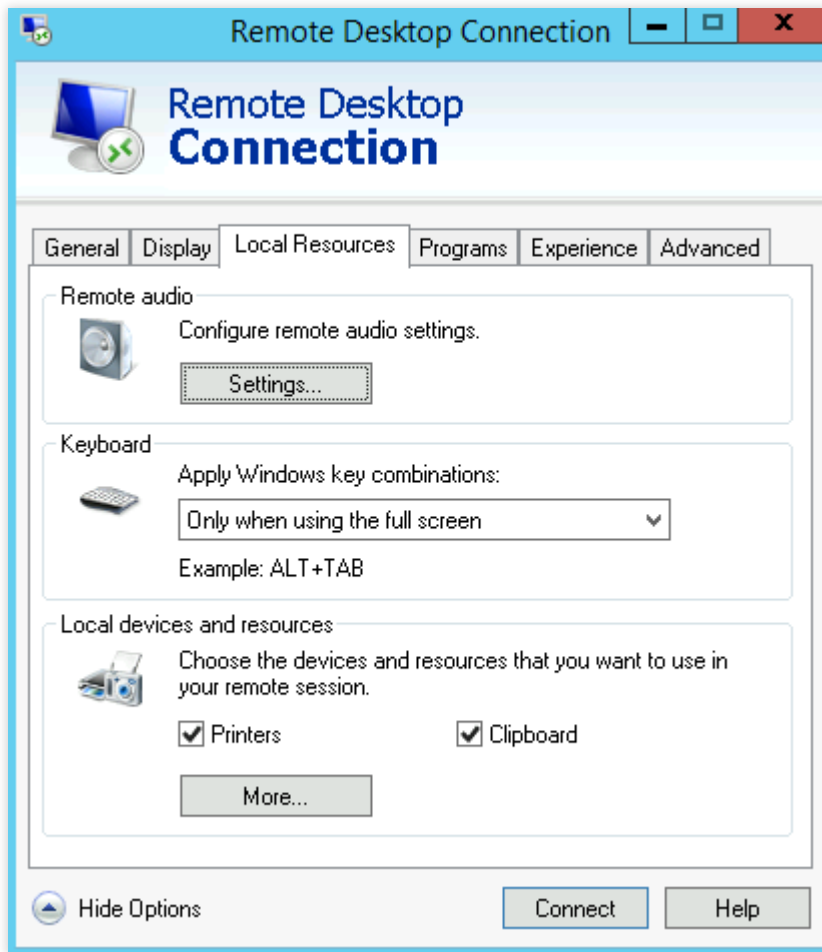
1. Press **Windows + R** on the local computer to open the **Run** window.
2. In the **Run** pop-up window, enter **mstsc**, and click **OK** to open the **Remote Desktop Connection** dialog box.
3. In the pop-up dialog box, enter the public IP address of the Lighthouse instance and click **Show Options** as shown below:



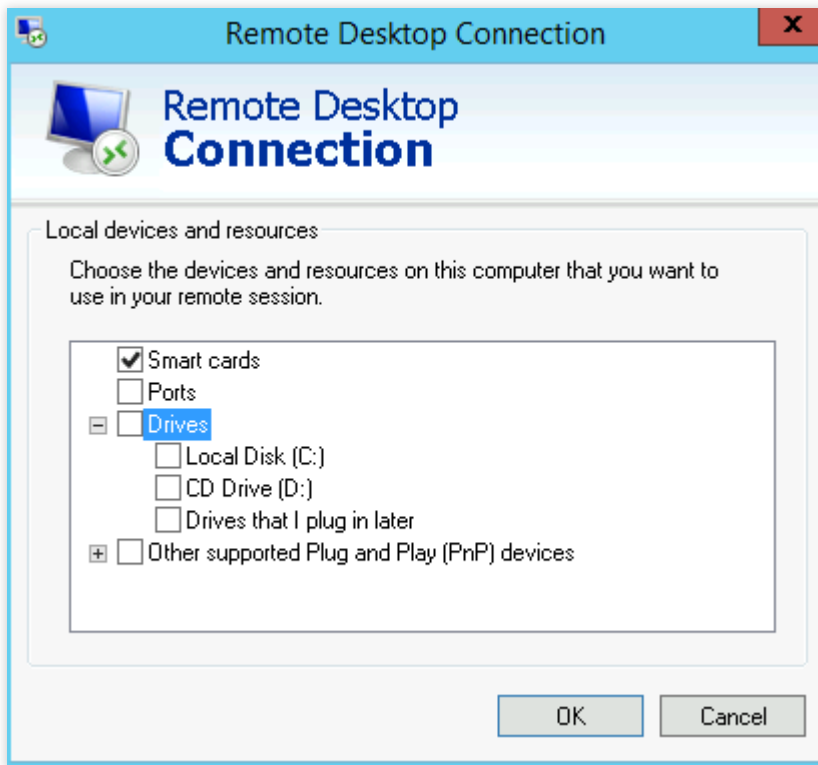
4. On the **General** tab, enter the Lighthouse instance public IP address and username "Administrator" as shown below:



5. Select the **Local Resources** tab and click **More**, as shown below:



6. In the **Local devices and resources** pop-up window, select the **Drives** module, check a local disk that contains files to upload to the Windows Lighthouse instance, and click **OK** as shown below:

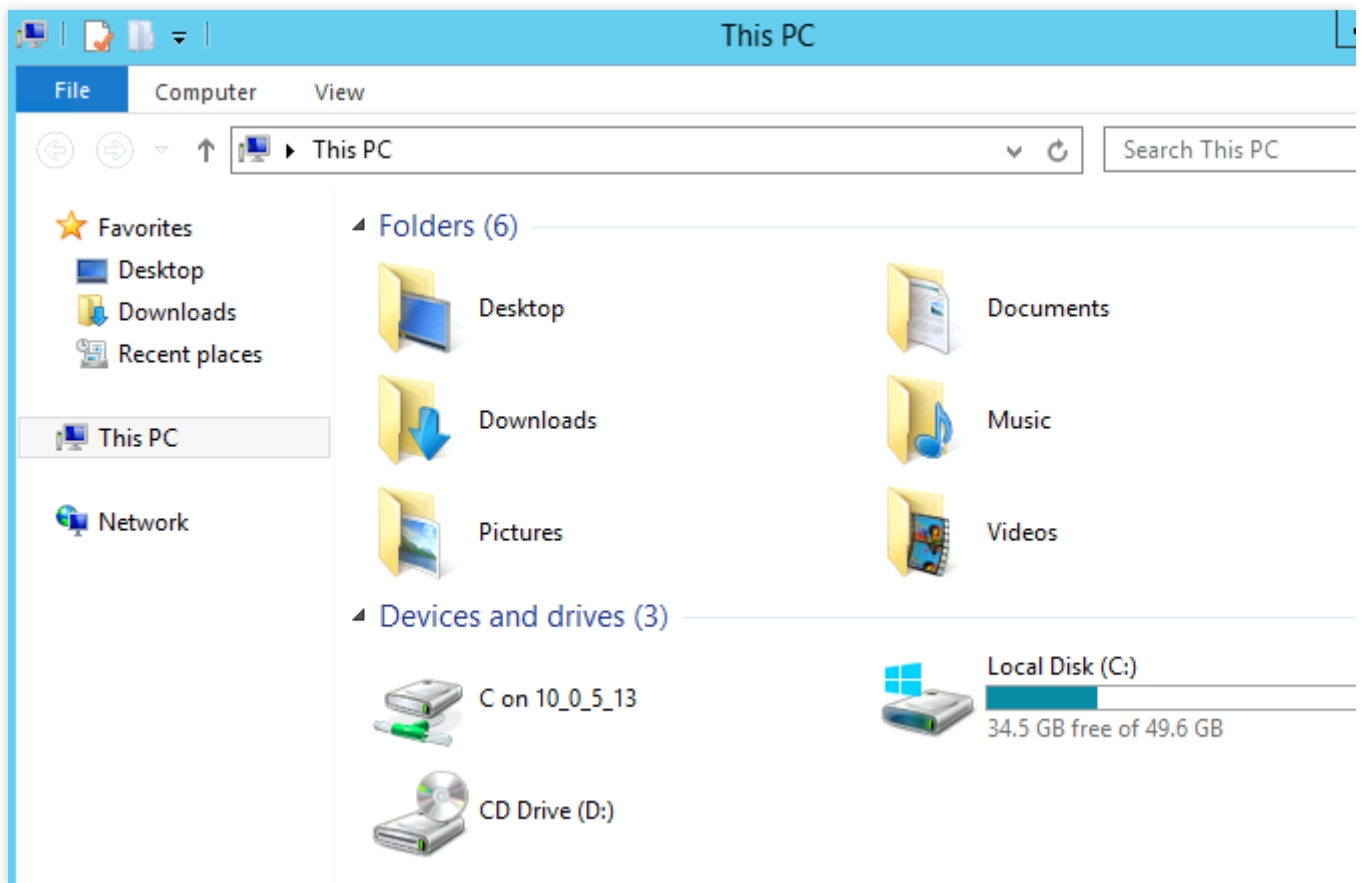


7. After the local configuration is completed, click **Connect** to log in to Windows Lighthouse instance remotely.

8. Click



> **Computer** in the Windows Lighthouse instance, and you can see the local disk mounted as shown below:



9. Double-click to open the attached local disk. Copy desired local files to another drive of the Windows Lighthouse instance.

For example, copy the file A from the local drive E to the C drive of the Windows Lighthouse instance.

## Downloading files

To download files from the Windows Lighthouse instance to your computer, you only need to copy desired files from the instance to the attached local disk.

# Uploading File from Linux or macOS to Linux Lighthouse Instance via SCP

Last updated : 2022-08-15 18:03:47

## Overview

The document uses a Lighthouse instance with CentOS 7.6 as an example to describe how to upload and download files via SCP.

### Note:

To get started, ensure that you have configured the Lighthouse instance admin account and password. If you haven't set or forgot the password, please [reset password](#).

## Directions

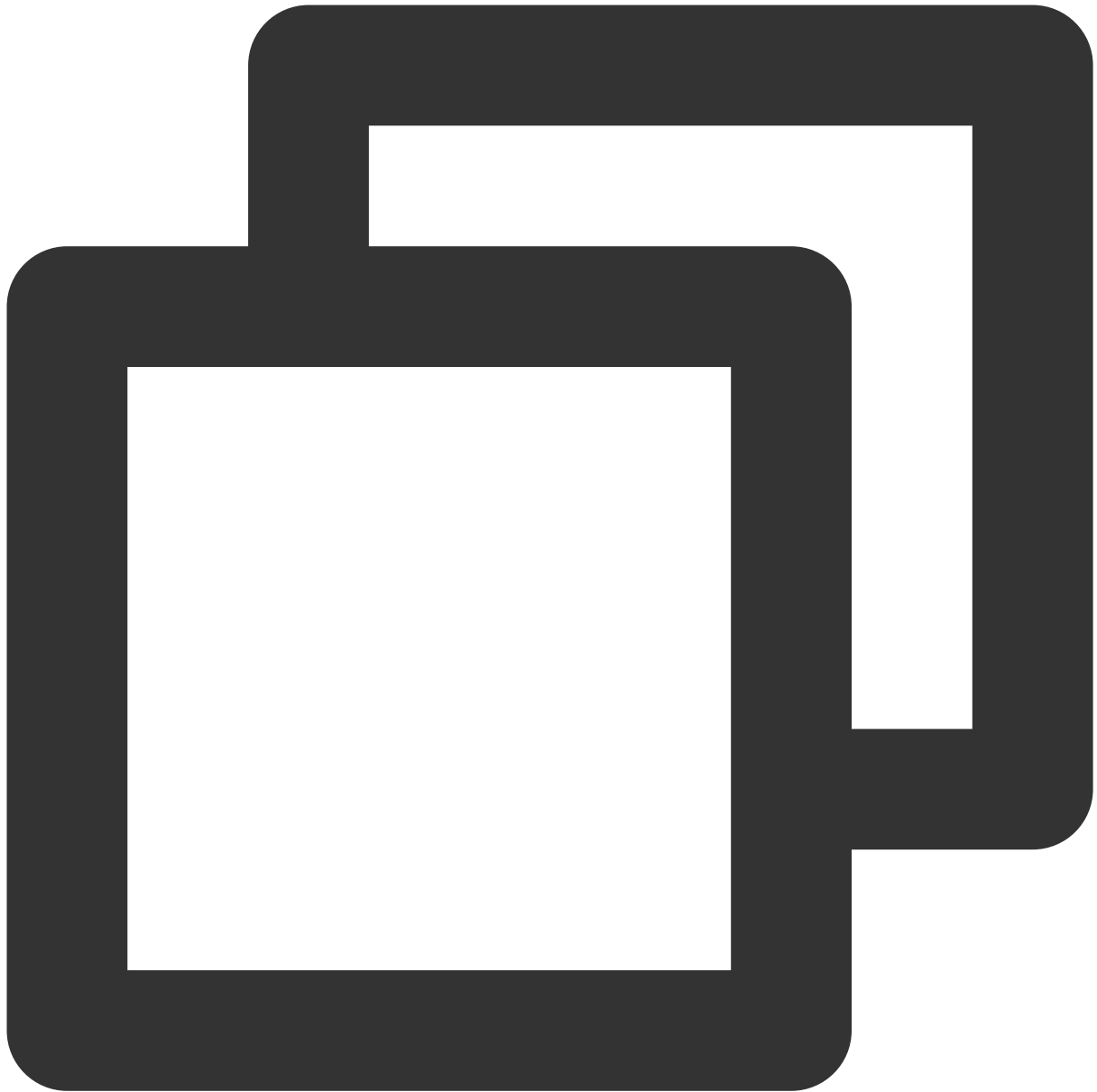
### Obtaining a public IP

Log in to the [Lighthouse console](#) and obtain the public IP of the target Lighthouse instance on **Instances** page.

### Uploading files

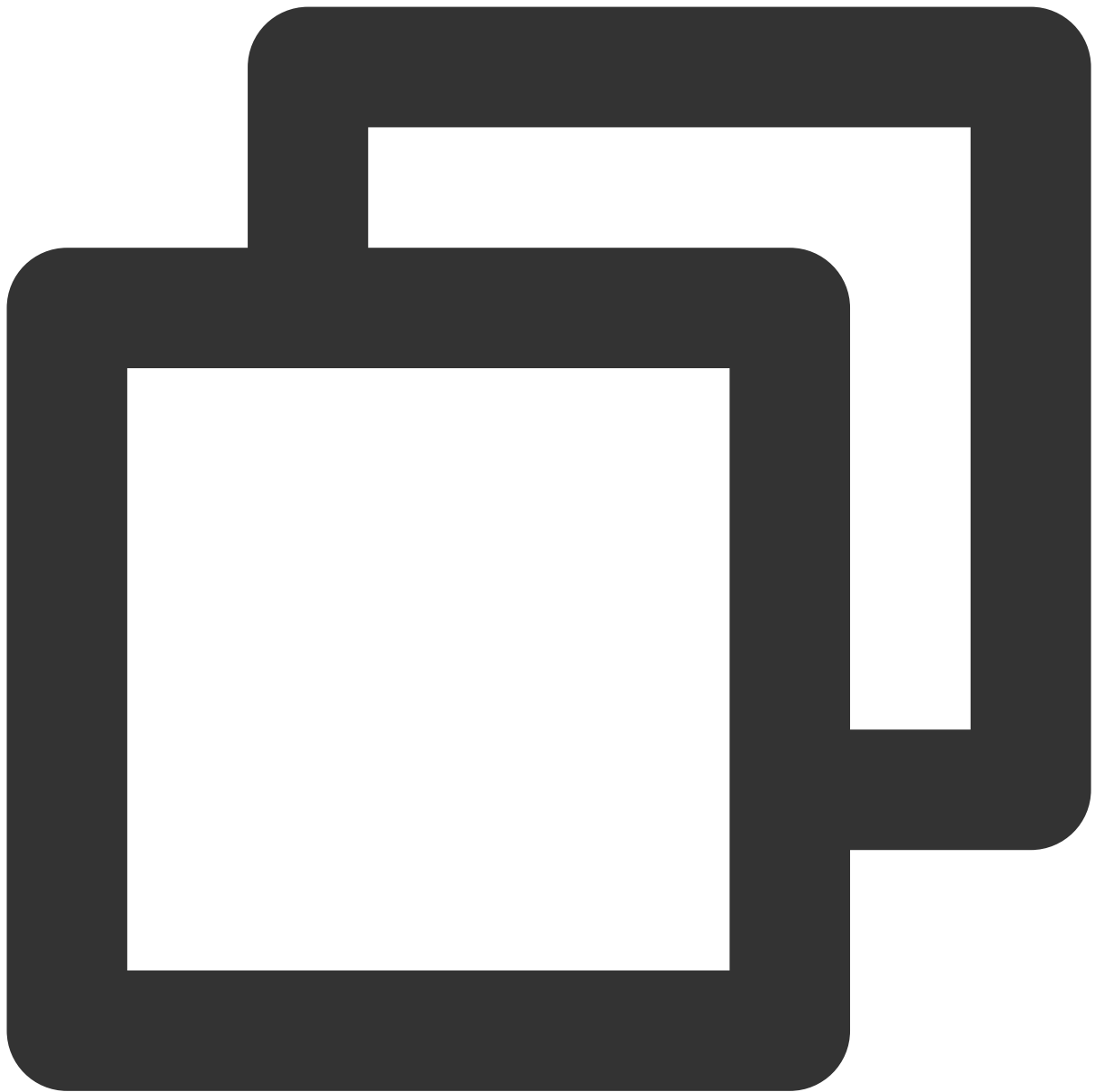
1. Run the following commands on the local server, and upload the files to the Linux-based Lighthouse instance.





```
scp Local file address Lighthouse instance account@Lighthouse instance public IP/do
```

For example, you can run the following command to upload the local file `/home/lnmp0.4.tar.gz` to the same directory of the Lighthouse instance whose public IP is `129.20.0.2` :

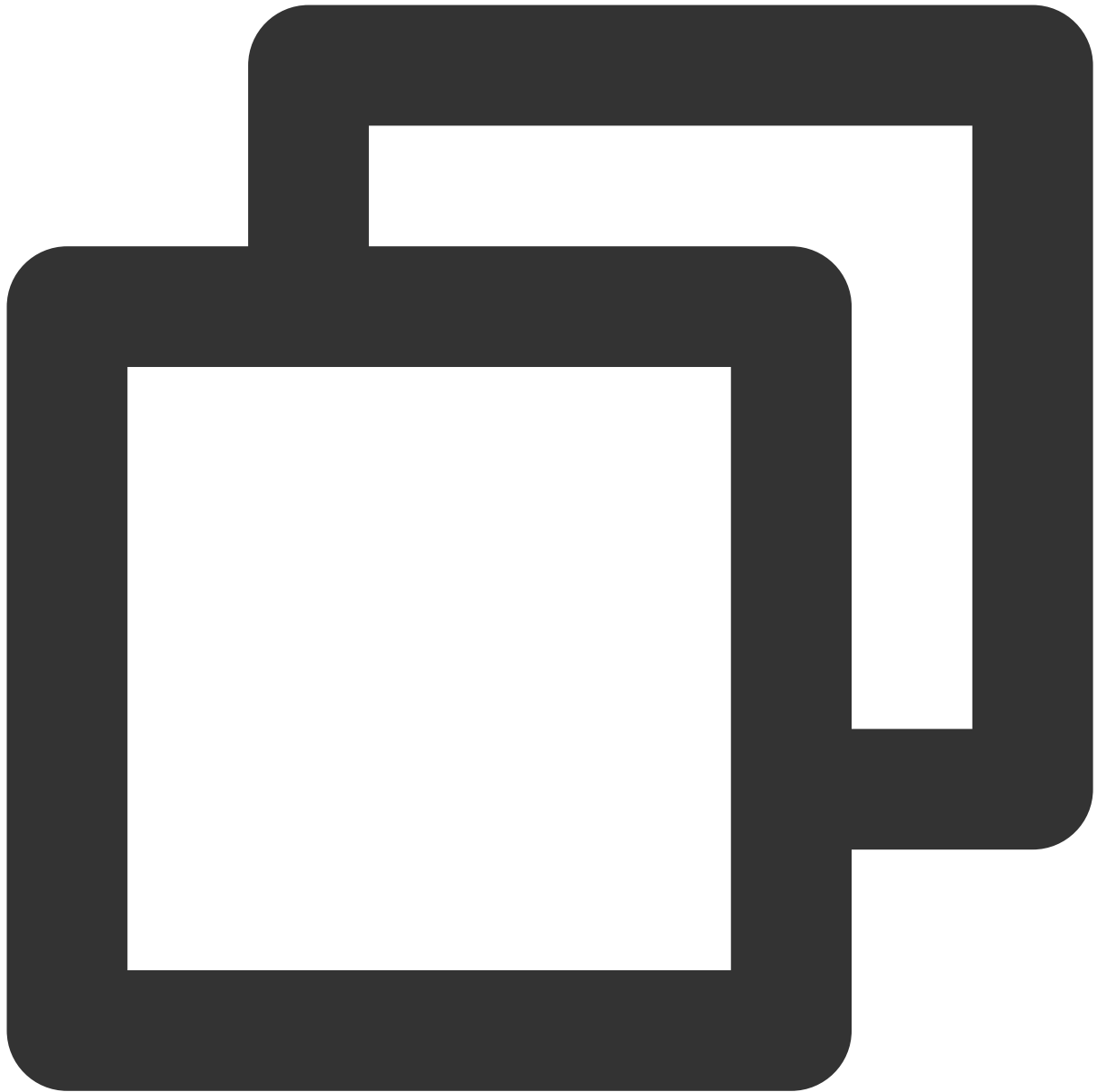


```
scp /home/Inmp0.4.tar.gz root@129.20.0.2:/home/Inmp0.4.tar.gz
```

2. Enter **yes** and press **Enter** to confirm the upload and enter the login password to complete the upload.

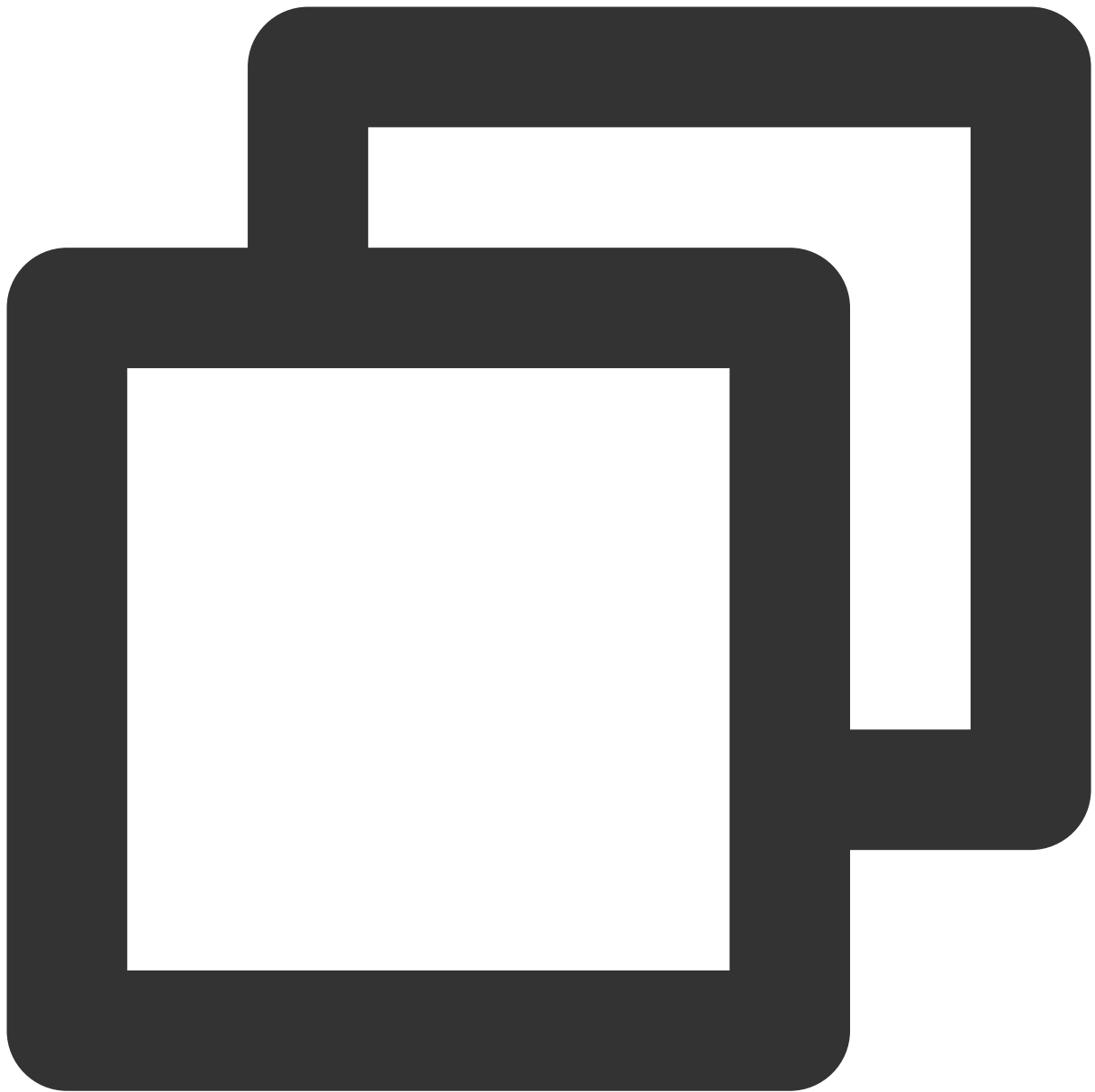
## Downloading files

Run the following command on the local server to download a file from a Linux-based Lighthouse instance.



```
scp Lighthouse instance account@Lighthouse instance public IP/domain name:Lighthouse
```

For example, you can run the following command to download the file `/home/lnmp0.4.tar.gz` from the Lighthouse instance whose public IP is `129.20.0.2` to the same local directory:



```
scp root@129.20.0.2:/home/Inmp0.4.tar.gz /home/Inmp0.4.tar.gz
```

# Uploading File from Linux or macOS to Lighthouse Instance via FTP

Last updated : 2022-05-12 12:24:13

## Overview

This document describes how to use the FTP service to upload files from a local Linux or macOS computer to a Lighthouse instance.

## Prerequisites

You have set up the FTP service in the Lighthouse instance.

## Directions

### Obtaining public IP

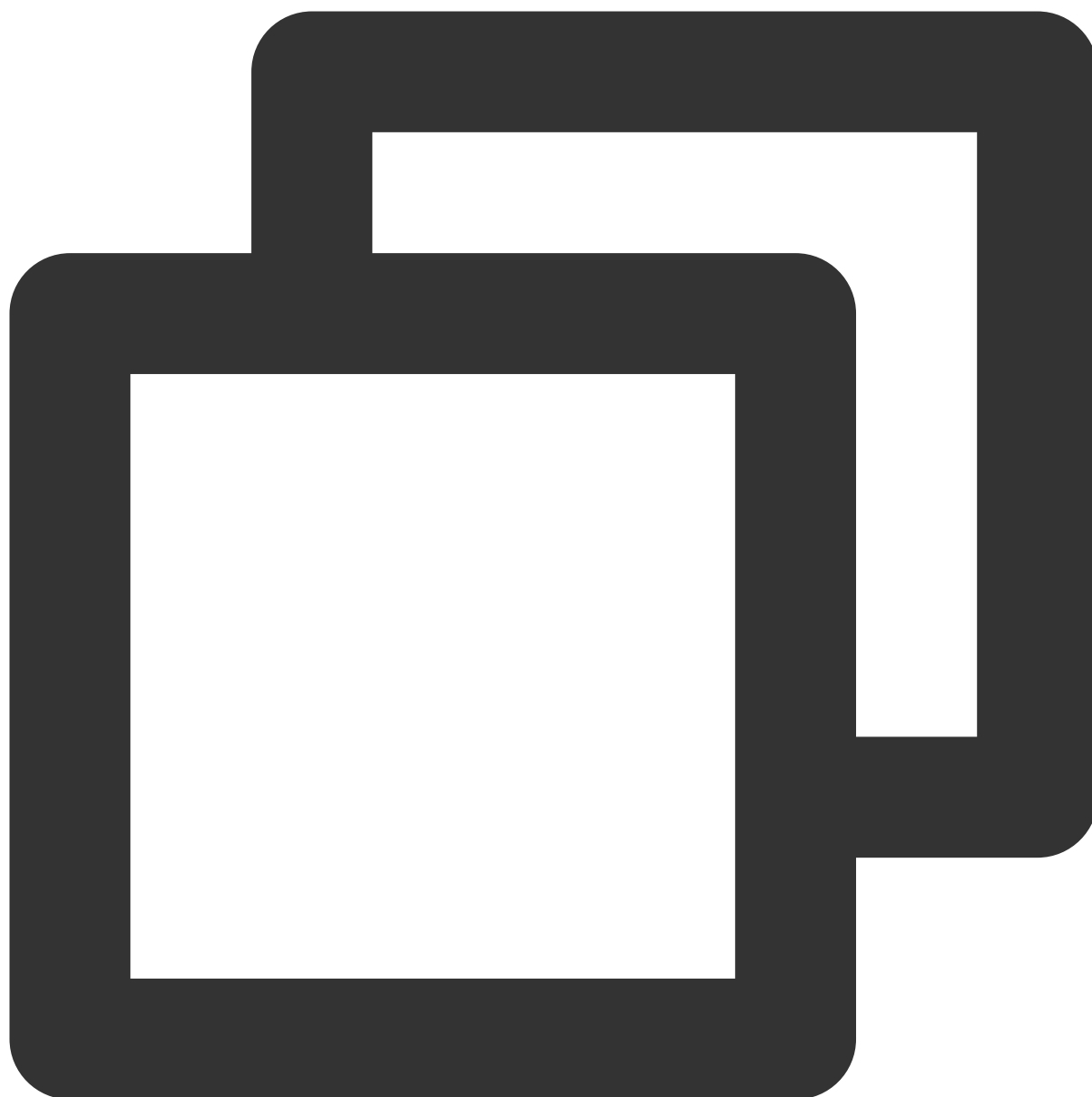
Log in to the [Lighthouse console](#) and get the public IP of the target Lighthouse instance on the **Instances** page.

### Using FTP service on Linux

1. Run the following command to install the FTP service.

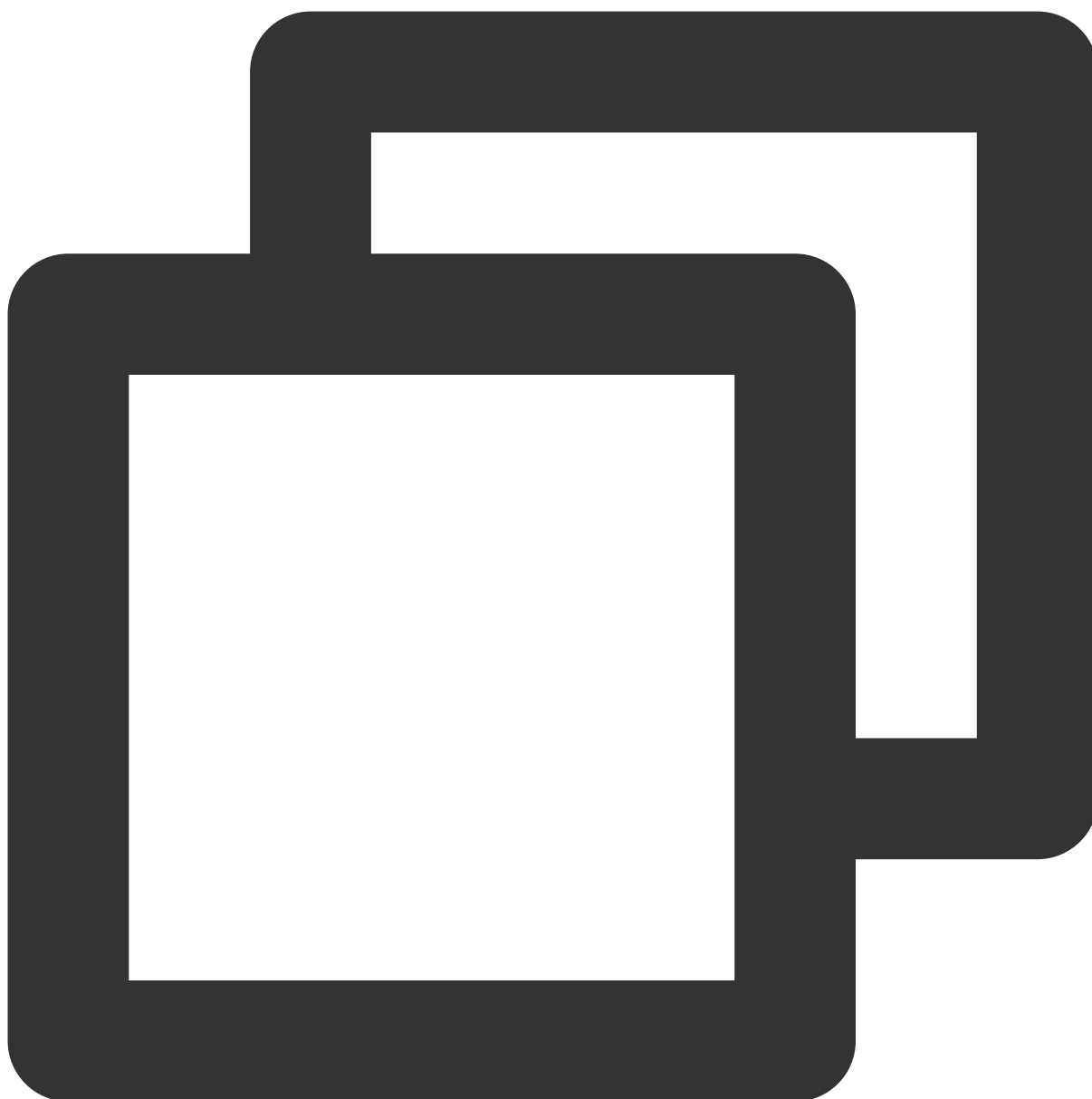
#### Note:

If the FTP service has already been installed on the local Linux computer, skip this step.



```
yum -y install ftp
```

2. Run the following command to connect to the Lighthouse instance and enter the FTP service username and password as prompted.



```
ftp Lighthouse instance IP address
```

If the following interface appears, the connection has been established successfully.

```
[root@VM_0_118_centos ~]# ftp 192.168.1.100
Connected to 192.168.1.100 (192.168.1.100).
220 Microsoft FTP Service
Name (192.168.1.100:root): ftpuser
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> █
```

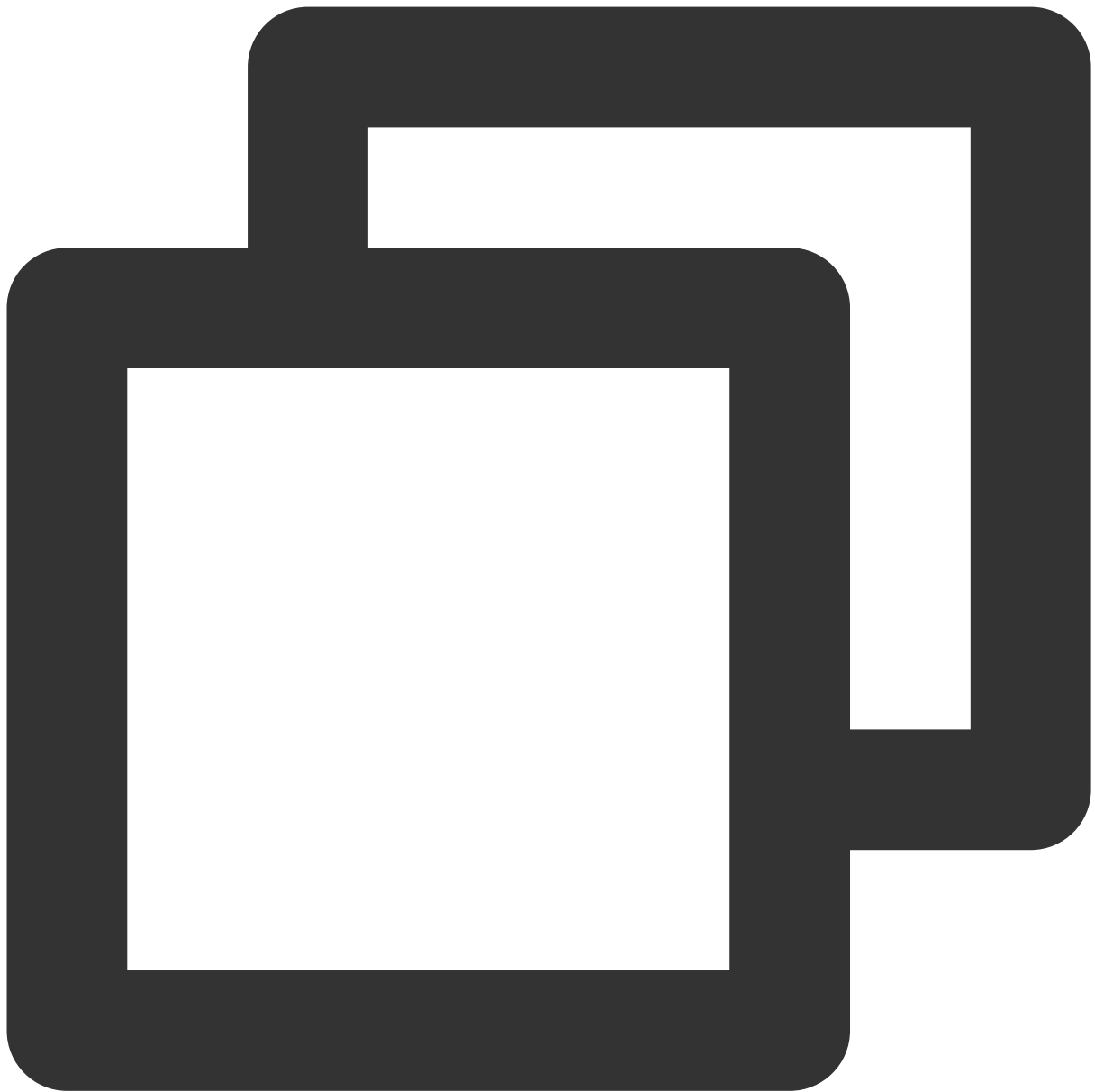
## Uploading and downloading file

Uploading file

Downloading file

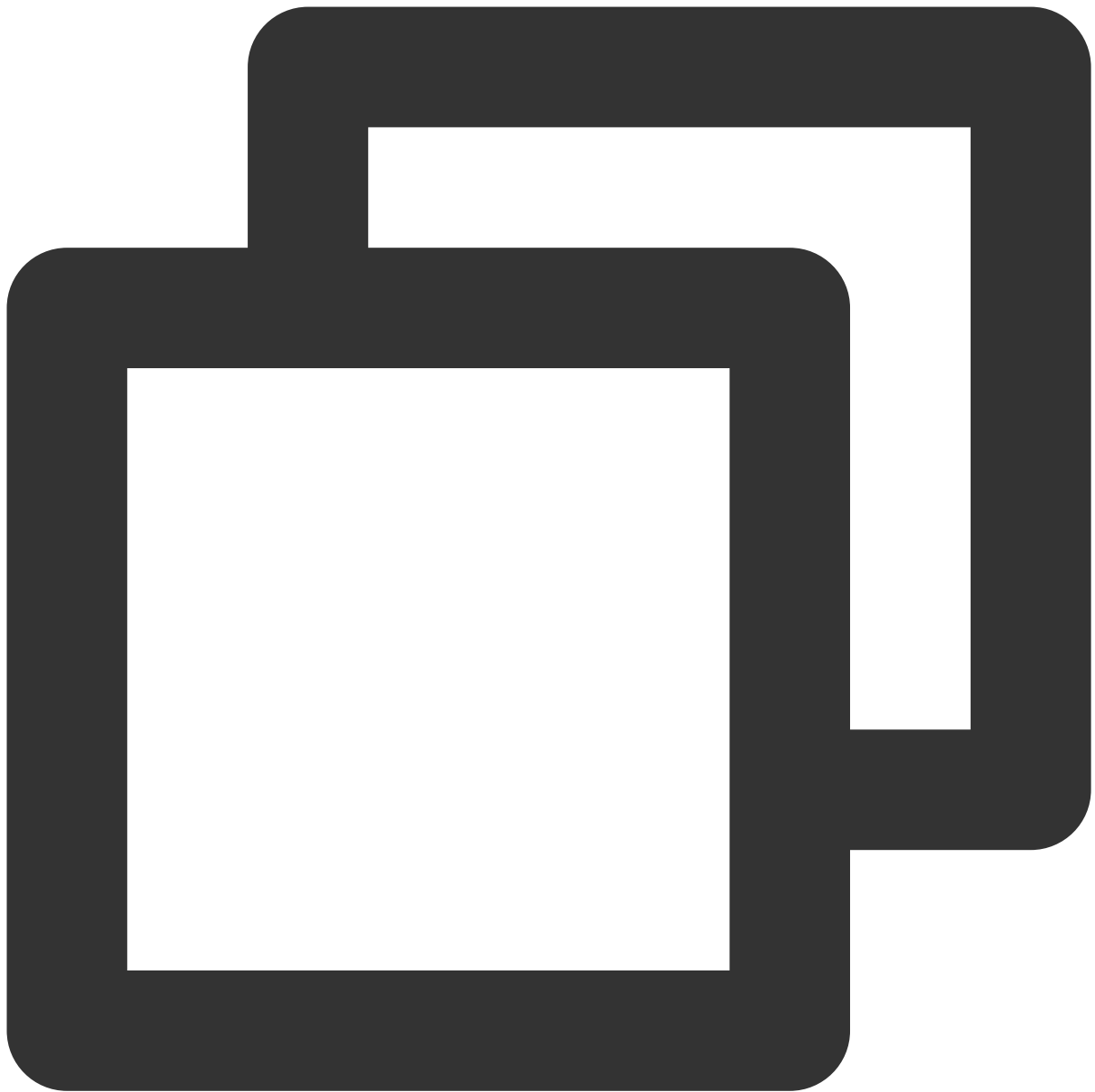
Run the following command to upload a local file to the Lighthouse instance:





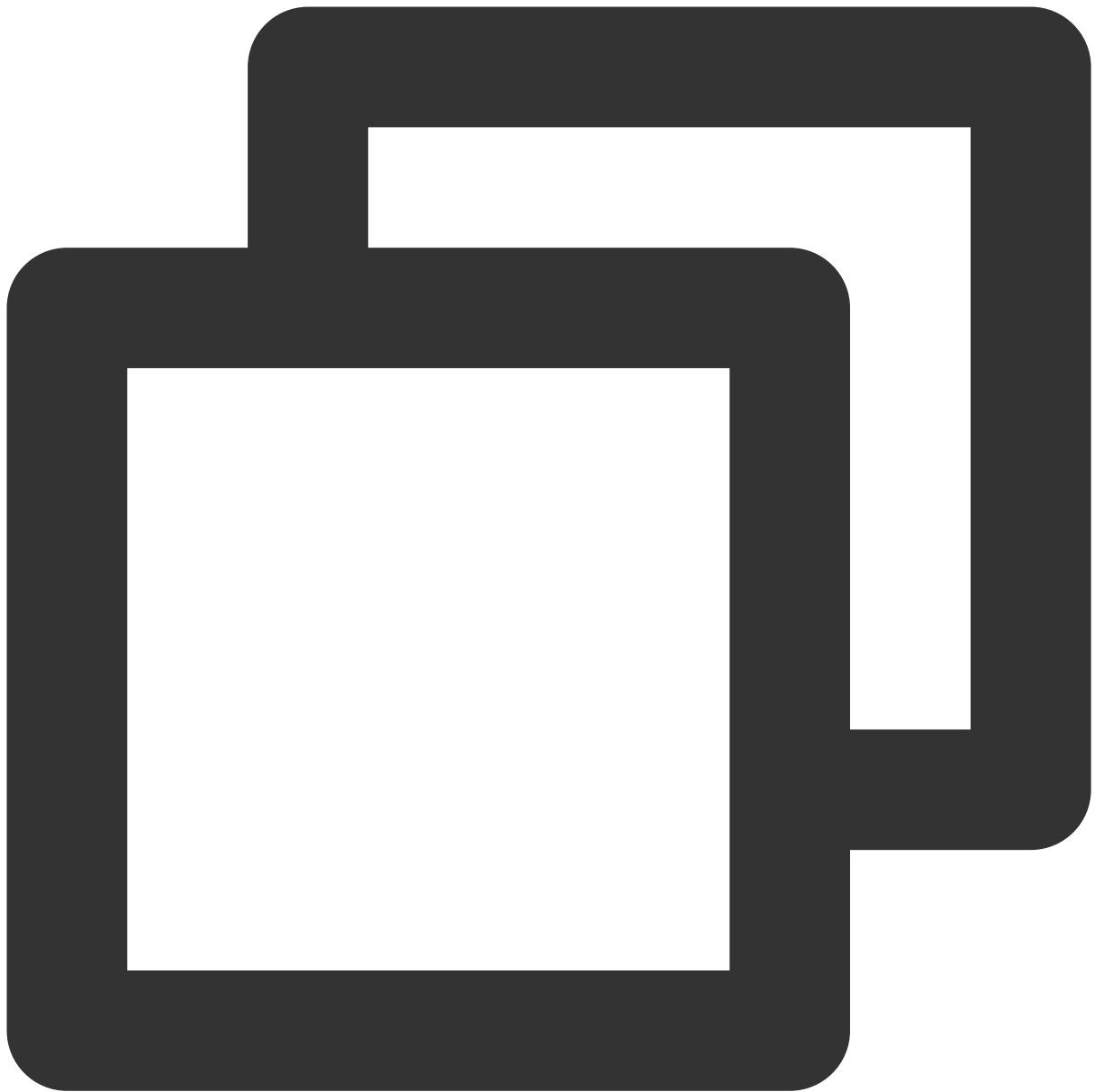
```
put local-file [remote-file]
```

For example, to upload the local `/home/1.txt` file to the Lighthouse instance, run the following command:



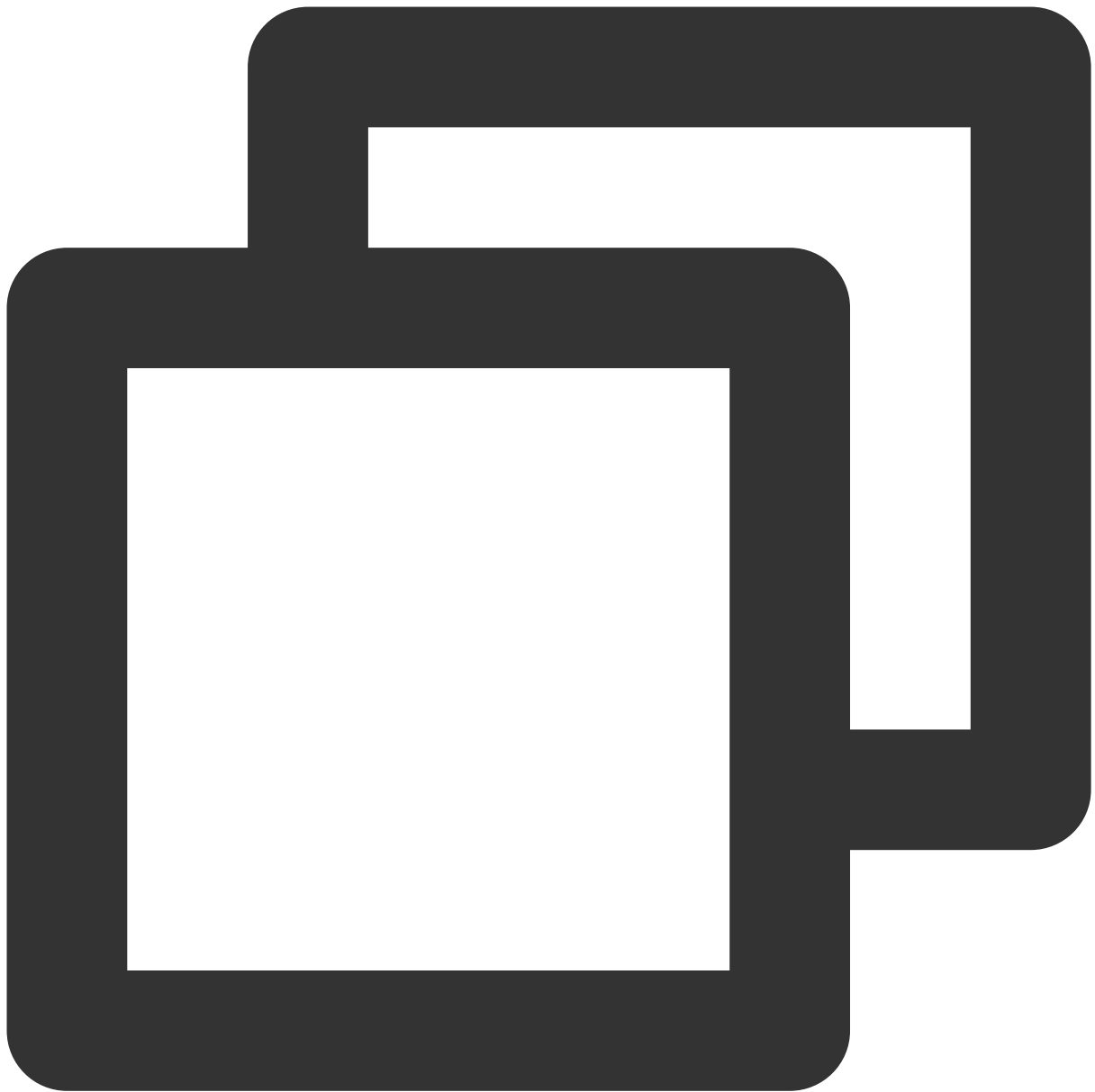
```
put /home/1.txt 1.txt
```

Run the following command to download a file from the Lighthouse instance to a local directory.



```
get [remote-file] [local-file]
```

For example, to download the `A.txt` file from the Lighthouse instance to the local `/home` directory, run the following command.



```
get A.txt /home/A.txt
```

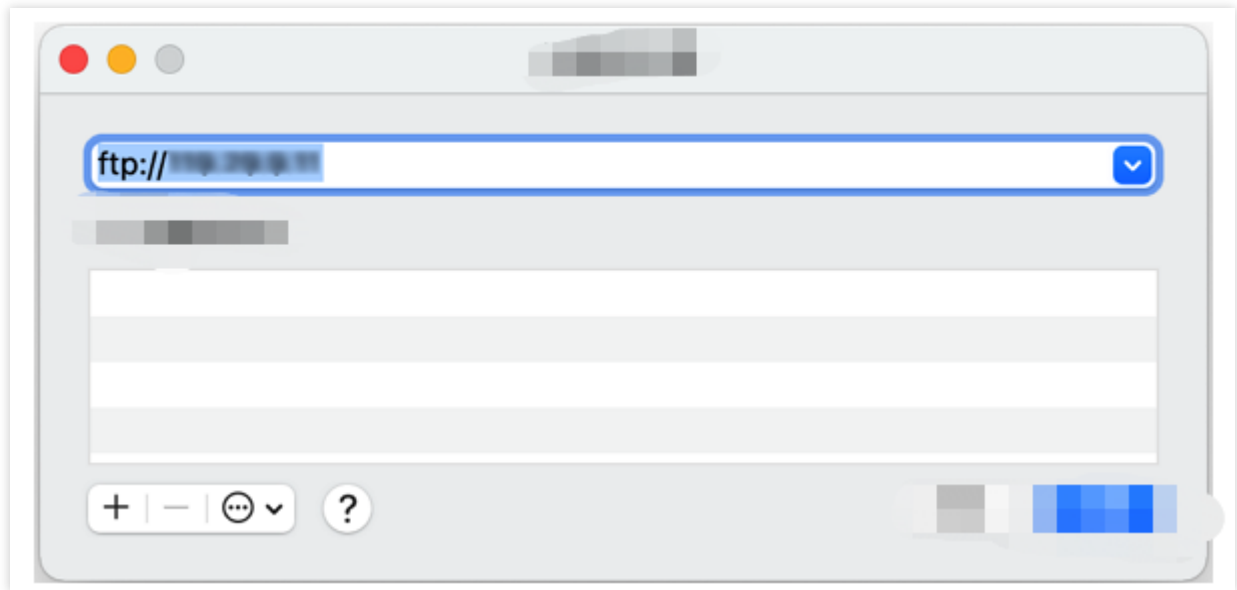
## Using FTP service on macOS

1. Click



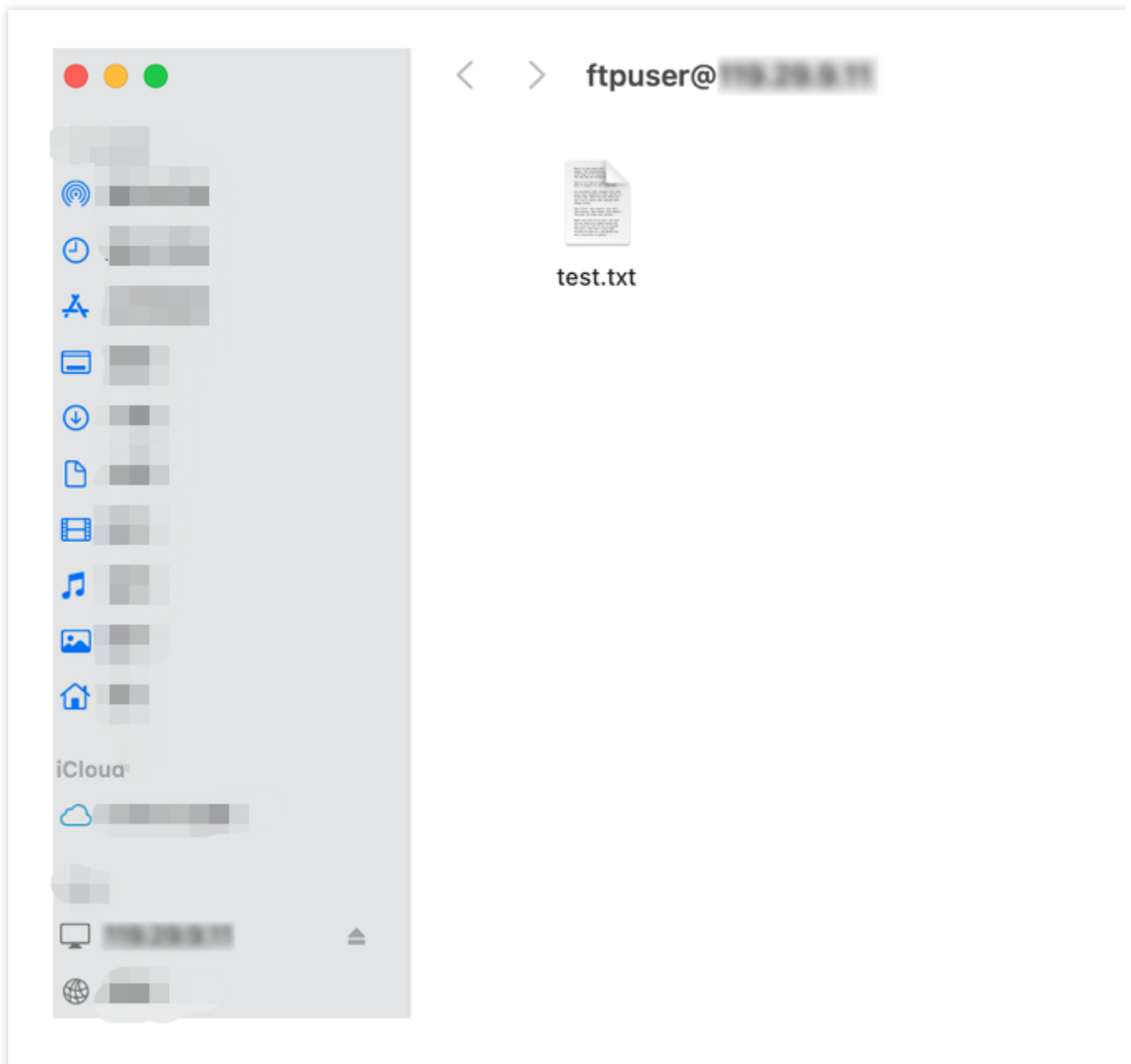
in the bottom-left corner and select **Go > Connect to Server** on the menu bar in the top-right corner.

2. In the **Connect to Server** window, enter `ftp://Lighthouse instance IP address` and click **Connect** as shown below:



3. In the pop-up window, select **Registered User**, enter the FTP service username and password, and click **Connect**.

If the following interface appears, the connection has been established successfully.



### Uploading and downloading file

You can directly copy files to the FTP window in Finder to upload them.

To download files from the Lighthouse instance to your computer, you only need to copy desired files from the instance to the attached local disk.

# Uploading File from Linux to Windows Lighthouse Instance via rdesktop

Last updated : 2022-05-12 12:24:13

## Overview

rdesktop is an open source client for Remote Desktop Protocol (RDP) that allows a local computer to connect to a Windows Lighthouse instance. This document describes how to use it to upload files from a Linux computer to a Lighthouse instance with the Windows Server 2012 R2 operating system.

## Prerequisites

You have obtained the Lighthouse instance admin account and password.

The default admin account of a Windows Lighthouse instance is `Administrator` .

If you forgot the login password, you can [reset it](#).

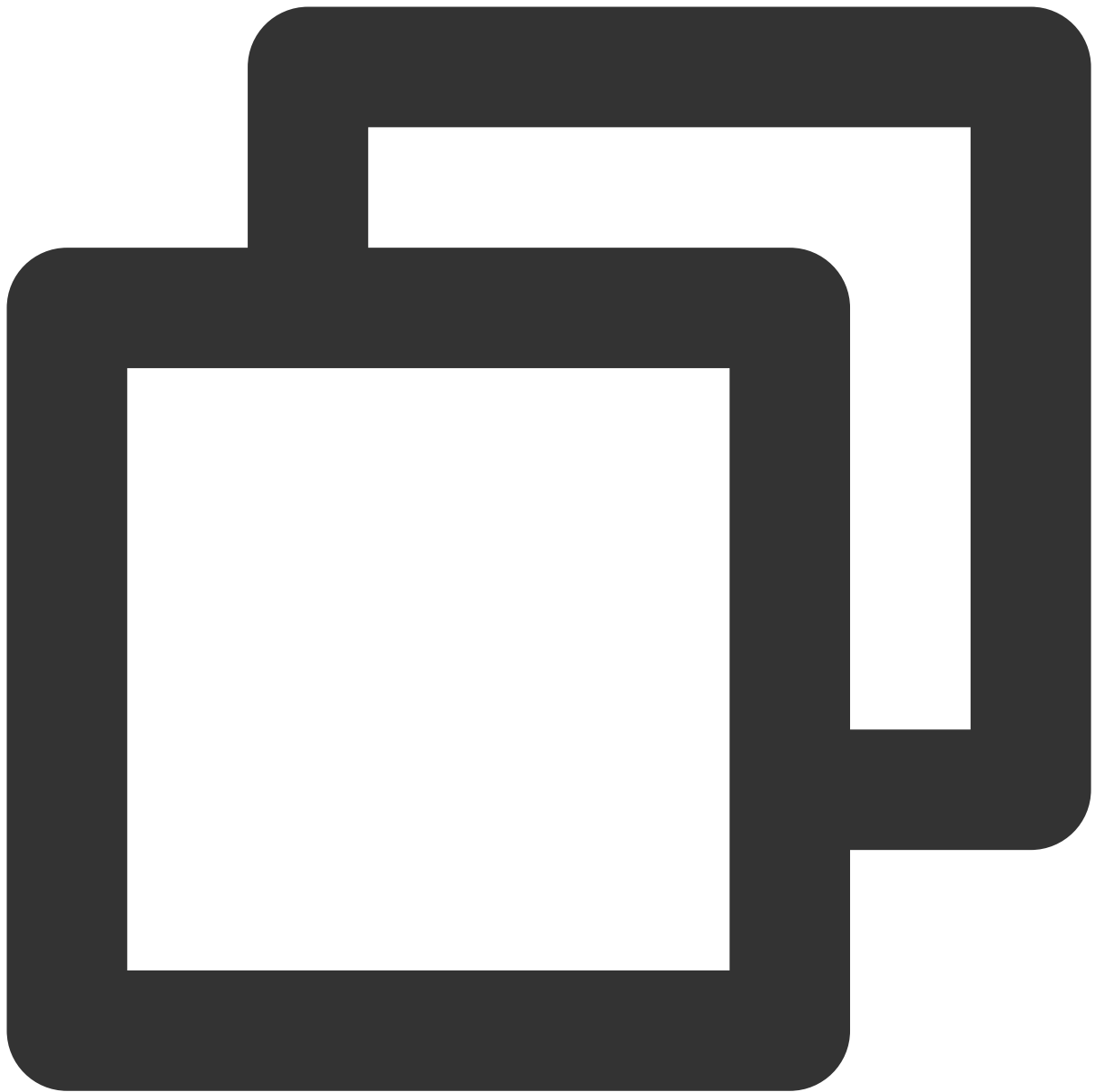
## Directions

### Obtaining public IP

Log in to the [Lighthouse console](#) and get the public IP of the target Lighthouse instance on the **Instances** page.

### Installing rdesktop

1. Open a terminal window and run the following command to download rdesktop. This step uses rdesktop v1.8.3 as an example.

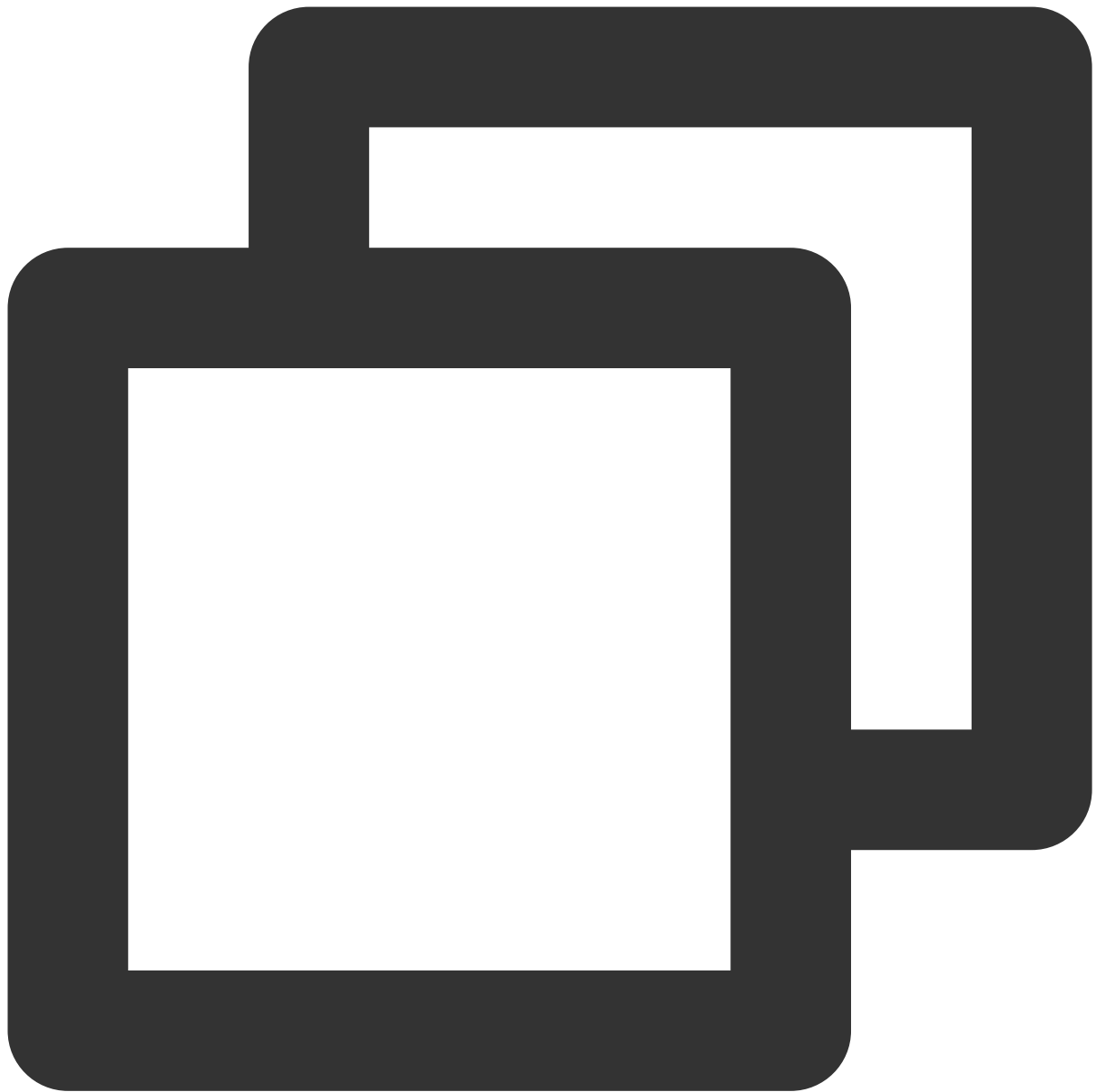


```
wget https://github.com/rdesktop/rdesktop/releases/download/v1.8.3/rdesktop-1.8.3.t
```

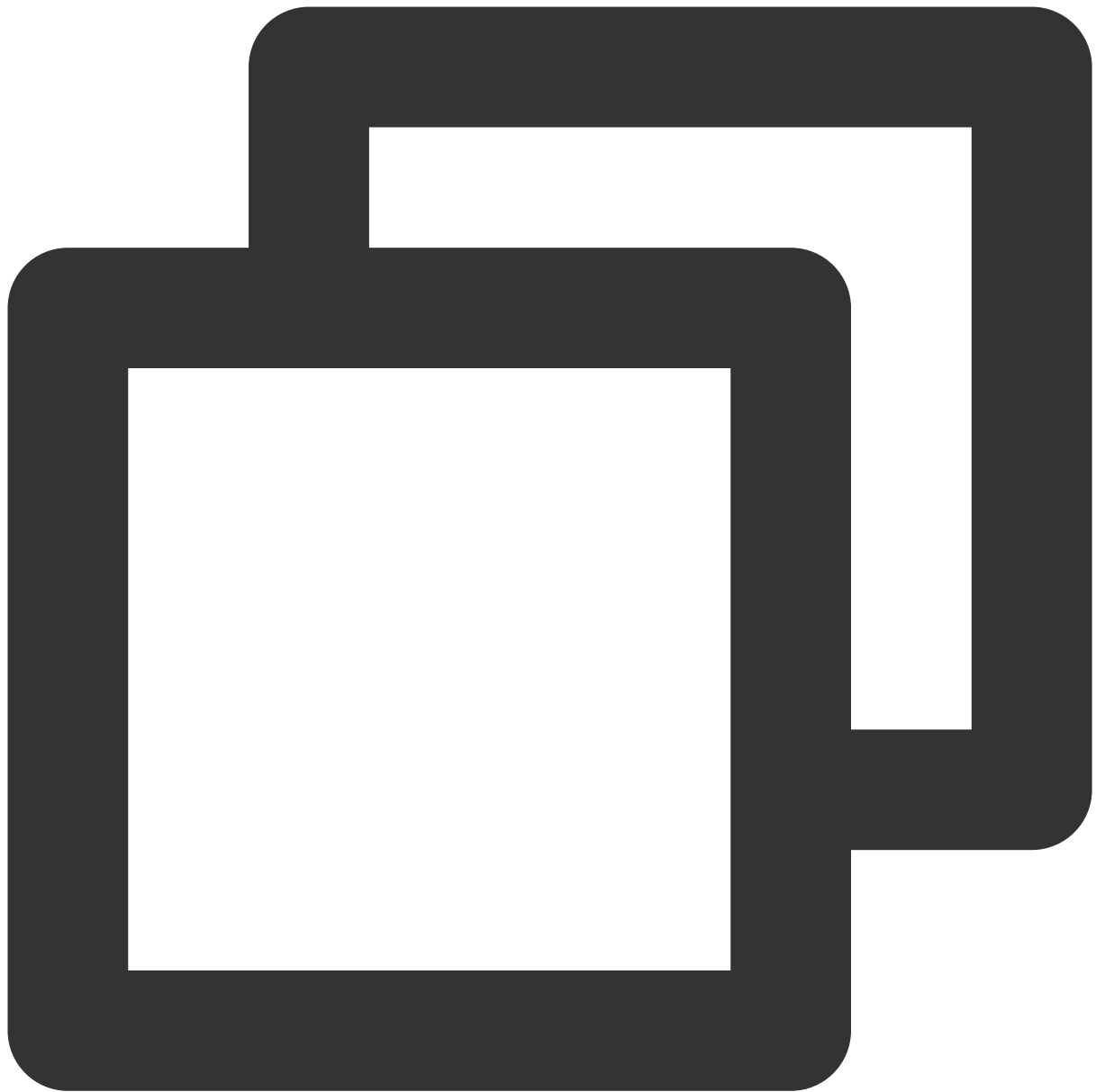
If you want to install the latest version, visit [the rdesktop page on GitHub](#) to find it. Then replace the path in the command with that of the latest version.

2. Run the following commands to decompress the installation package and enter the directory.



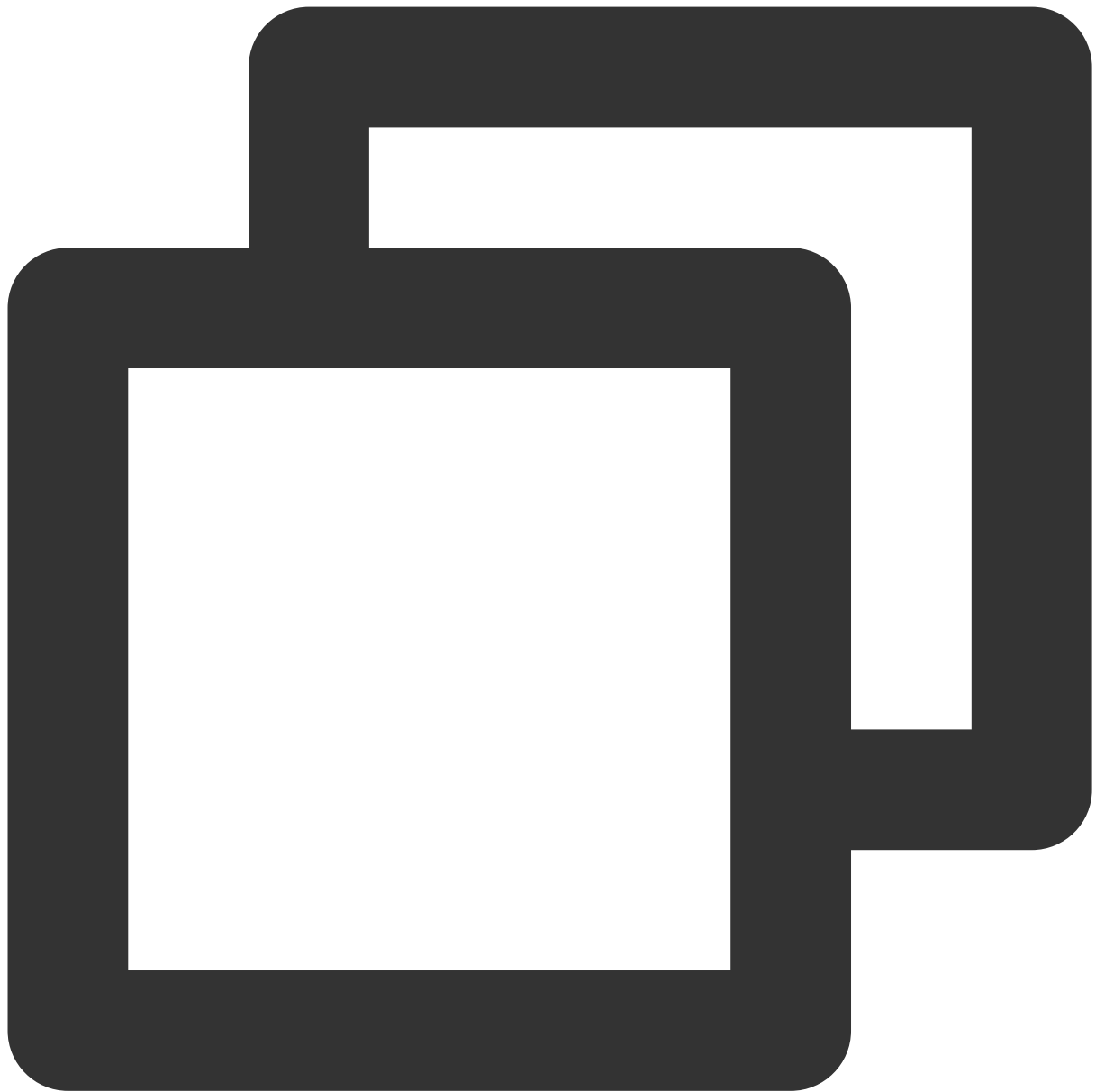


```
tar xvzf rdesktop-1.8.3.tar.gz
```

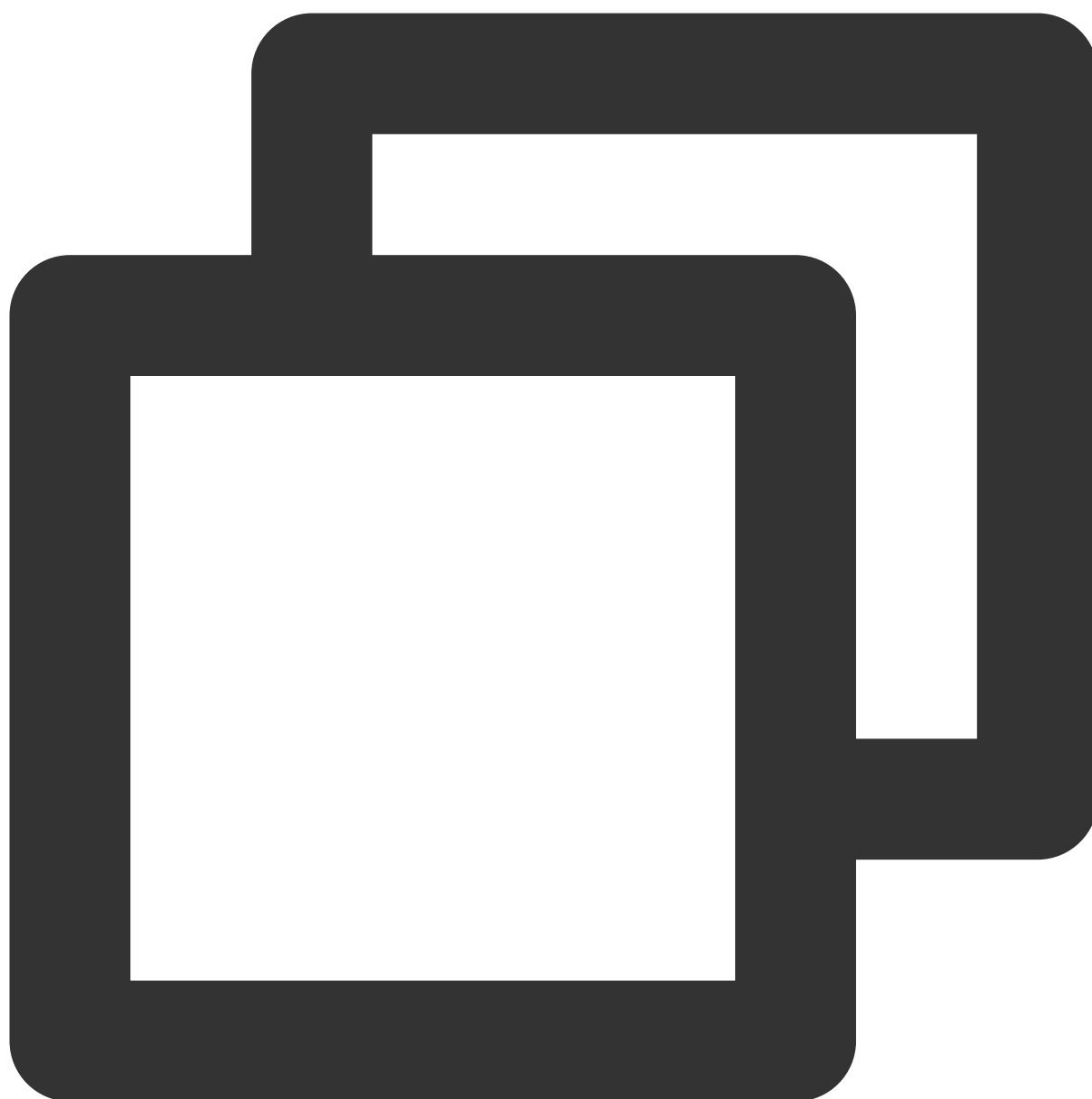


```
cd rdesktop-1.8.3
```

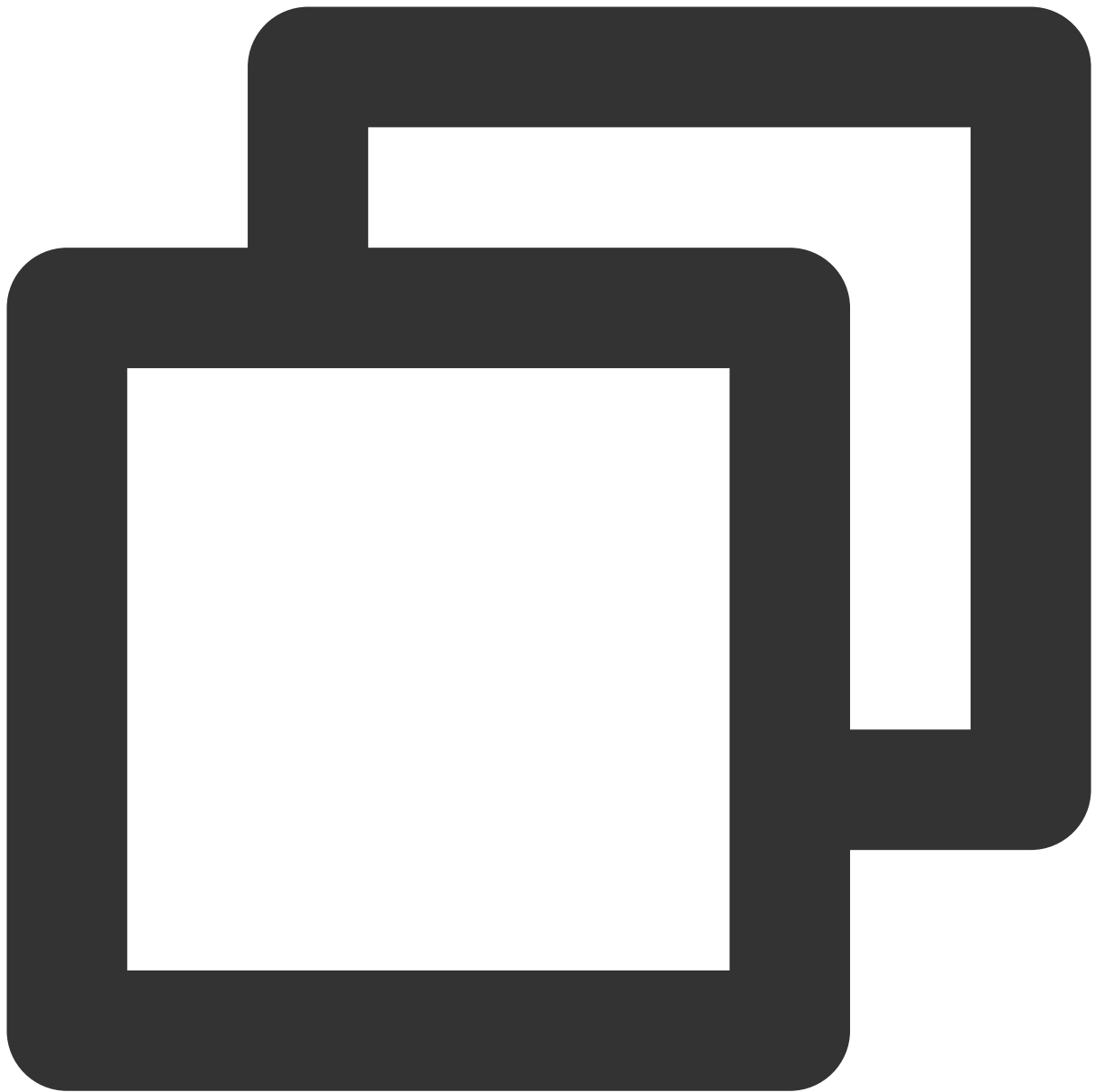
3. Run the following commands to compile and install rdesktop.



```
./configure
```

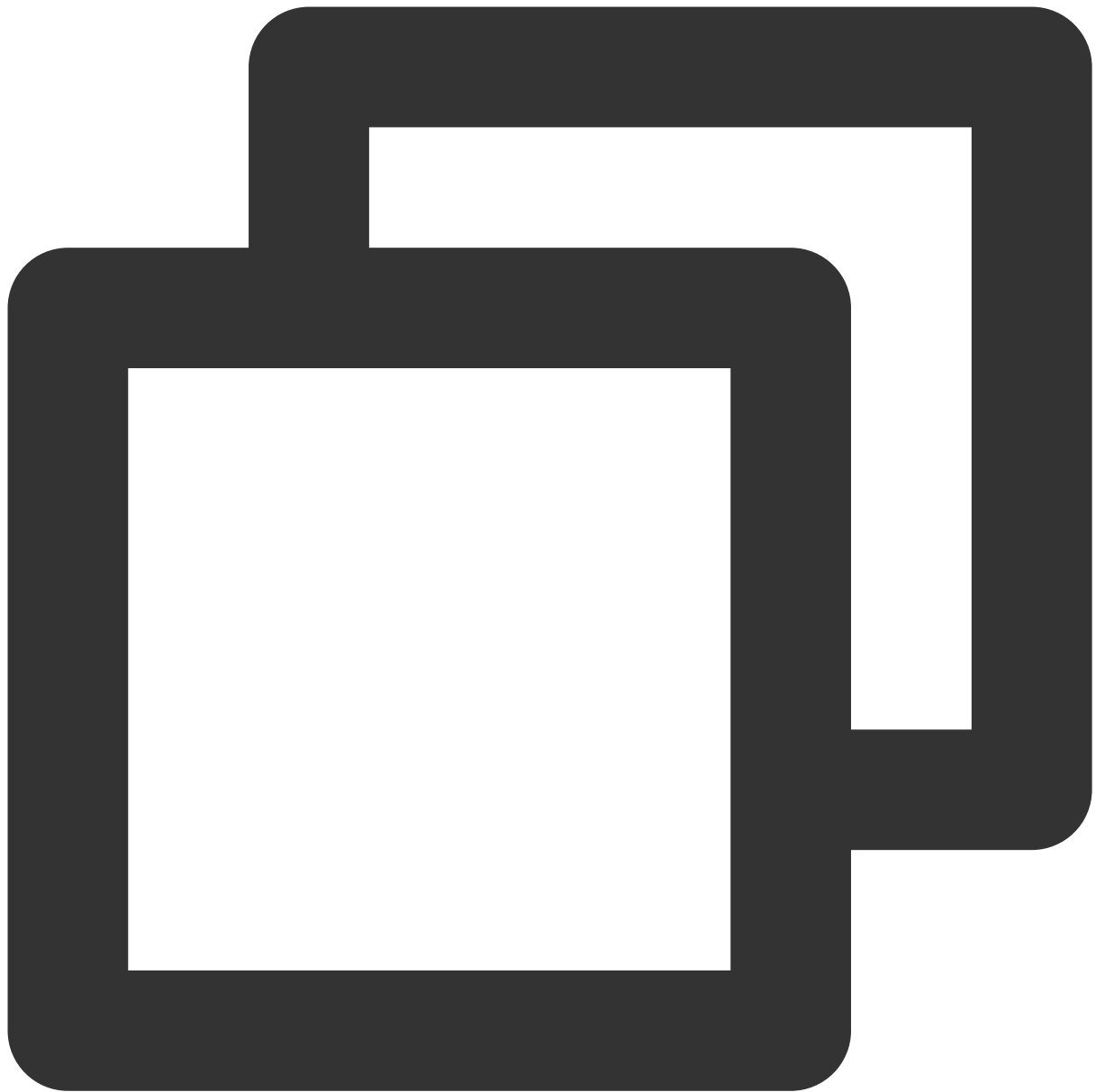


make



```
make install
```

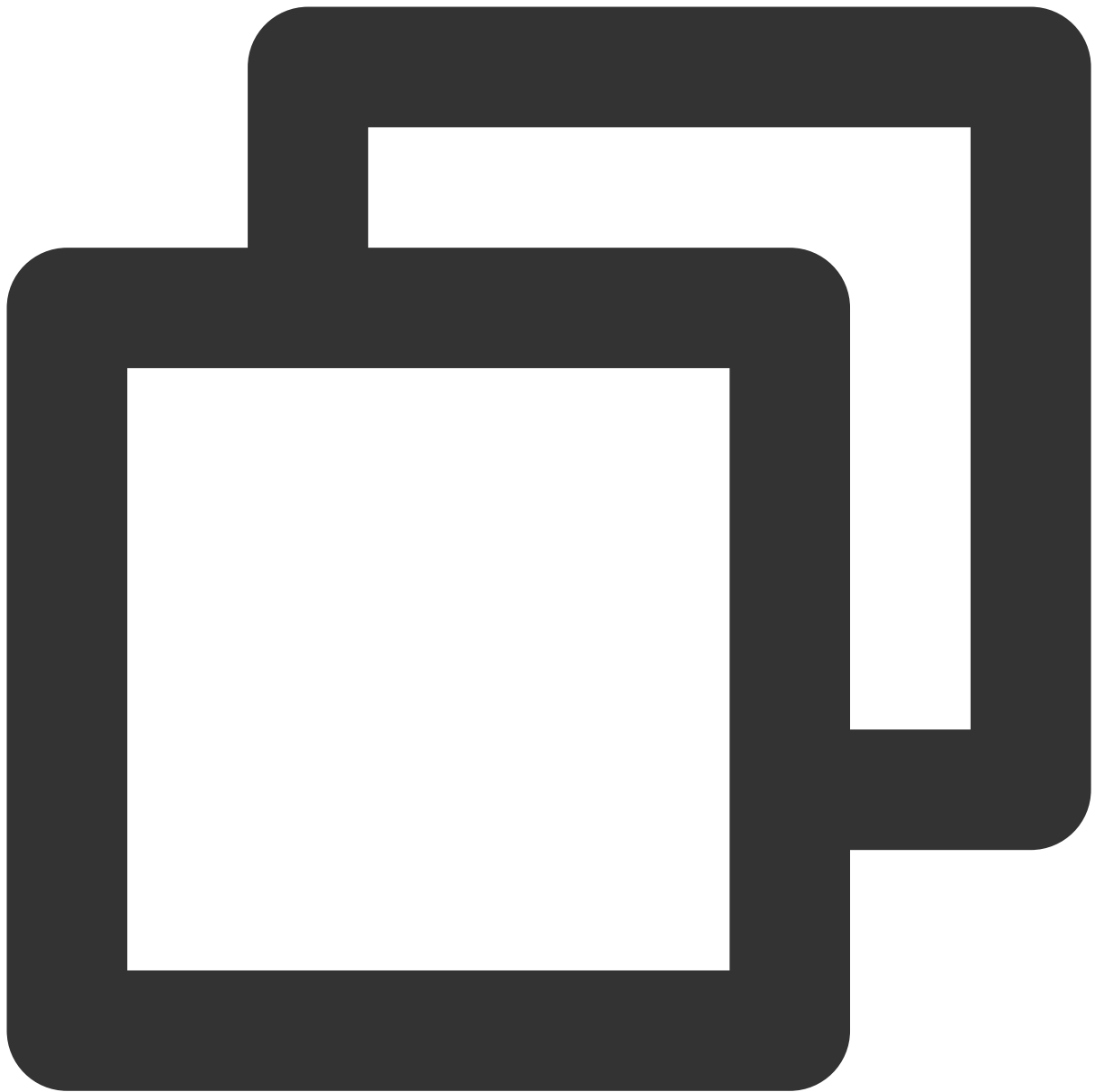
4. After the installation is complete, run the following command to check if rdesktop is successfully installed:



```
rdesktop
```

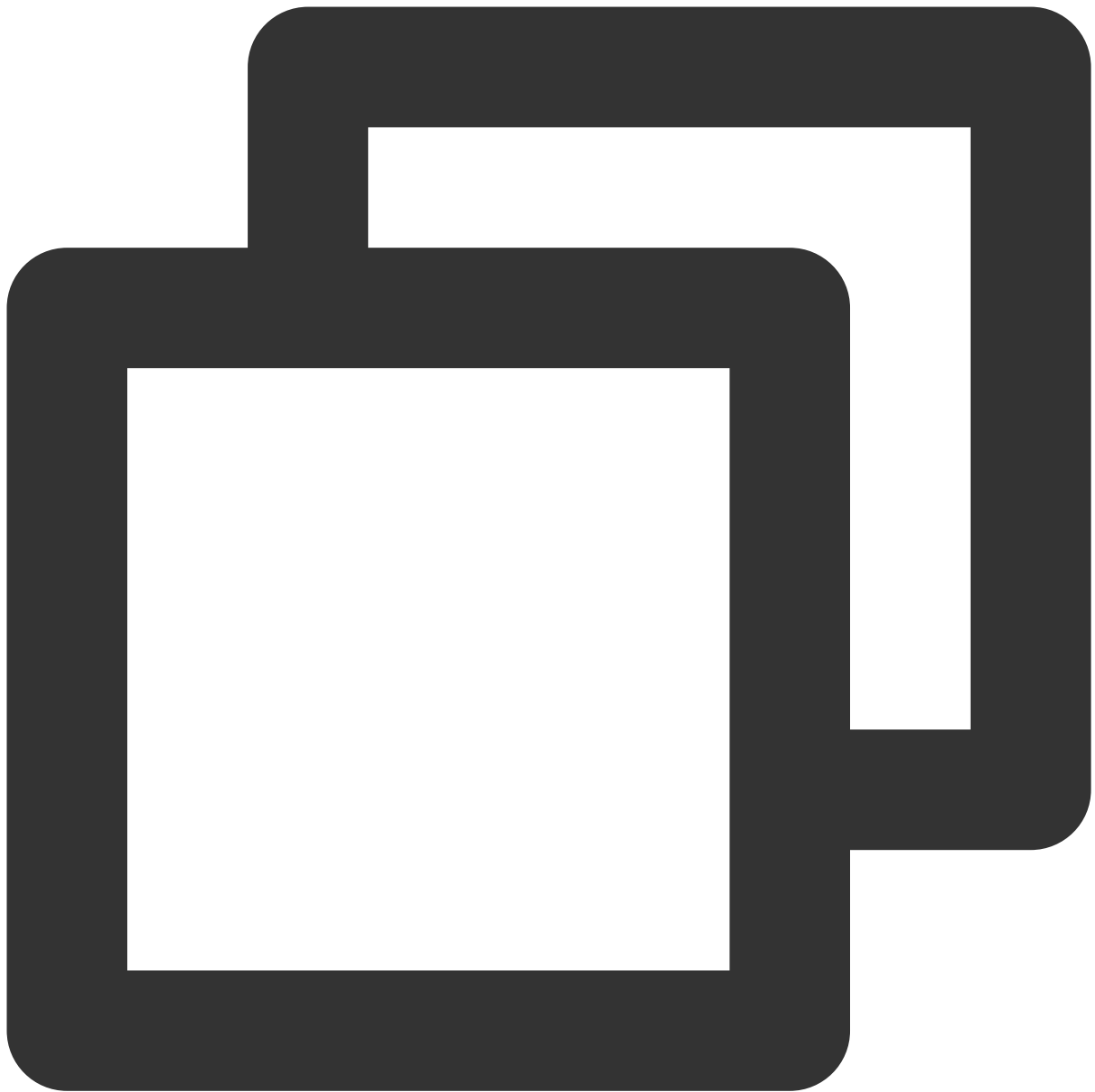
## Uploading files

1. Run the following command to specify the folder shared to the Lighthouse instance:



```
rdesktop Lighthouse instance public IP -u Lighthouse instance account -p Lighthouse
```

For example, run the following command to share the `/home` folder on your local Linux computer with the specified Lighthouse instance, and rename it as `share` .



```
rdesktop 118.xx.248.xxx -u Administrator -p 12345678 -r disk:share=/home
```

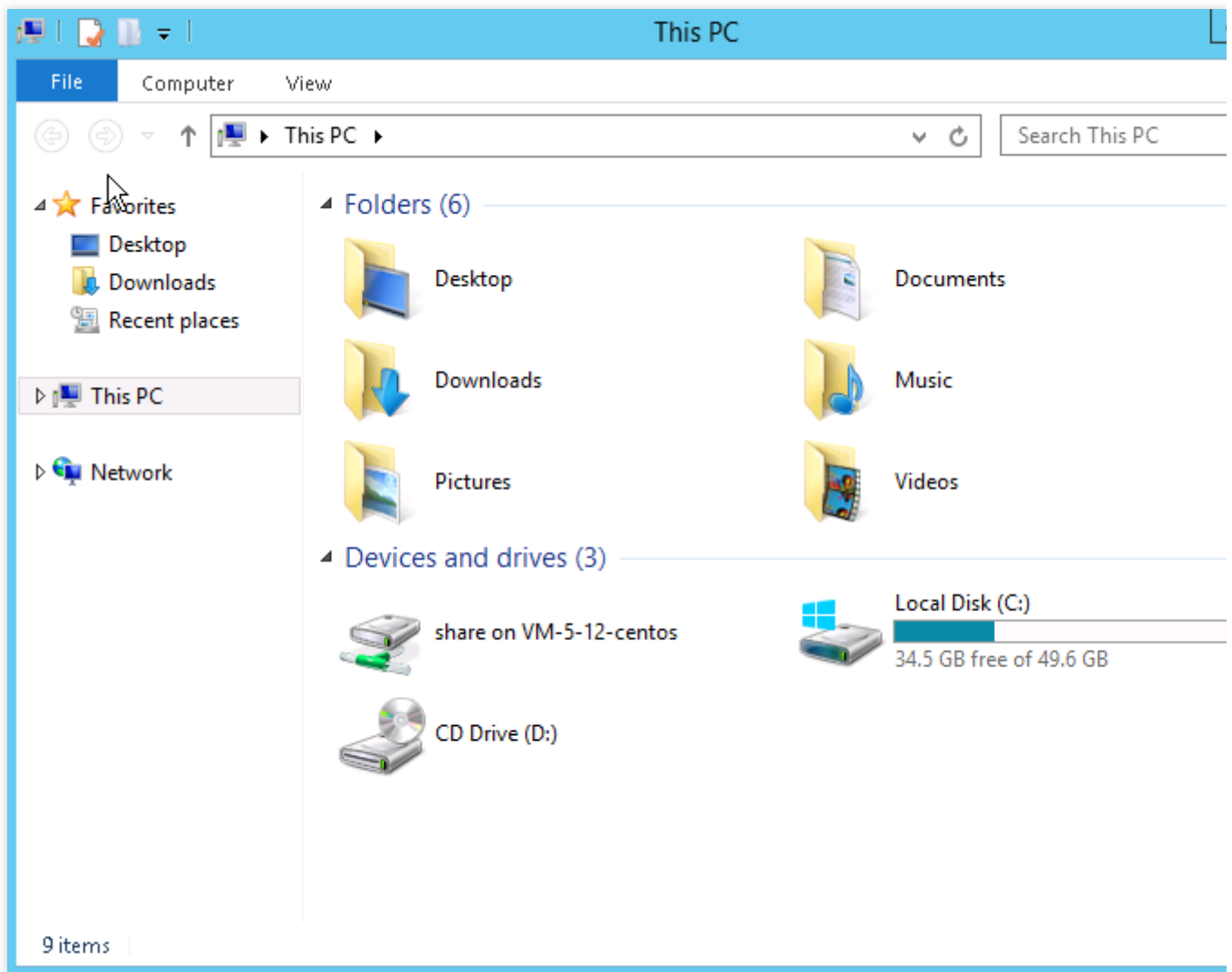
If the operation is successful, the Windows desktop will appear.

Click



in the lower-left corner and select **My Computer** to see a list of shared folders as shown below:





2. Double-click a shared folder to open it. Copy desired local files to another drive of the Windows Lighthouse instance.

For example, copy the file A from the `share` folder to the C drive of the Windows Lighthouse instance.

## Downloading files

To download files from the Windows Lighthouse instance to your computer, you only need to copy desired files from the instance to a shared folder.

# Uploading File from macOS to Windows Lighthouse Instance via MRD

Last updated : 2024-03-20 14:41:01

## Overview

Microsoft Remote Desktop (MRD) is a remote desktop software developed by Microsoft. This document describes how to use it on macOS to upload files to a Lighthouse instance with Windows Server 2012 R2 installed.

## Prerequisites

You have downloaded and installed MRD on your local computer. Go to [Microsoft Remote Desktop for Mac Beta](#) to download and install it.

MRD supports macOS 10.10 and later versions. Make sure your operating system is compatible.

You have obtained the Lighthouse instance admin account and password.

The default admin account of a Windows Lighthouse instance is `Administrator`.

If you forgot the login password, you can [reset it](#).

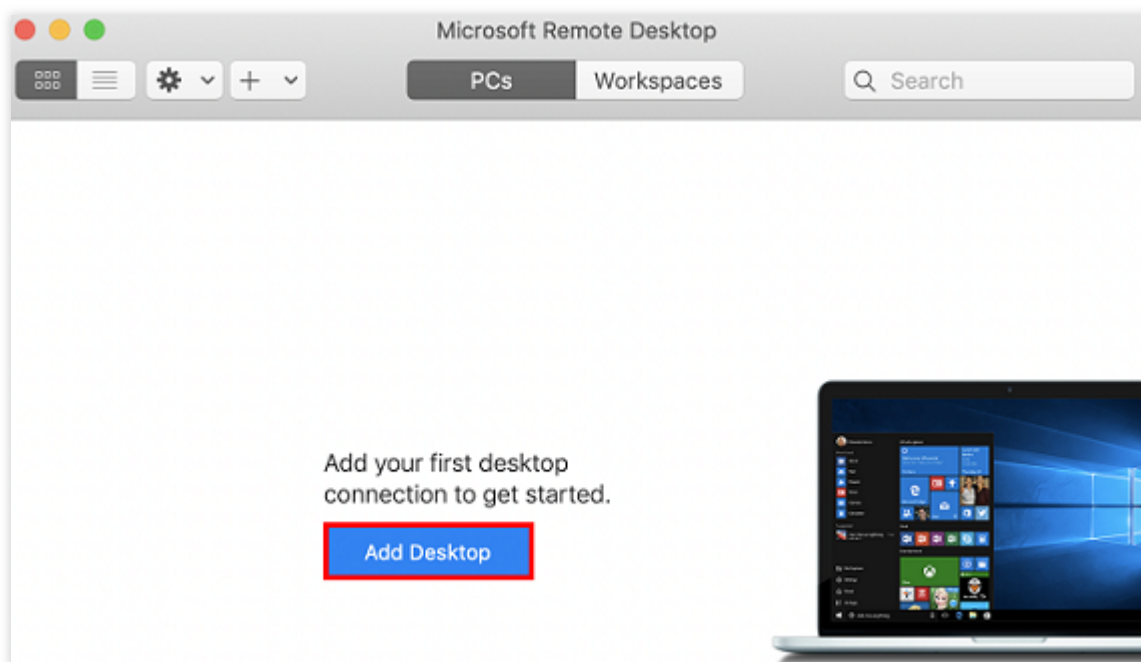
## Directions

### Obtaining public IP

Log in to the [Lighthouse console](#) and get the public IP of the target Lighthouse instance on the **Instances** page.

### Uploading files

1. Start MRD and click **Add Desktop**, as shown below:



2. In the **Add Desktop** pop-up window, follow the steps illustrated in the following image to select a folder to upload and establish a connection with your Windows instance.

**Add PC**

PC name: 118. [redacted]

User account: Ask when required

General Display Devices & Audio **Folders**

Choose the folders that you want to access in the remote session.

☒ Redirect folders

Name	Path
CVM-update	/Users/[redacted]/Documents/06-CVM...

+ -

Cancel Add

2.1 In the **PC name** text field, enter the public IP address of your Lighthouse instance.

2.2 Click **Folders** to redirect to the folder list.

2.3 Click

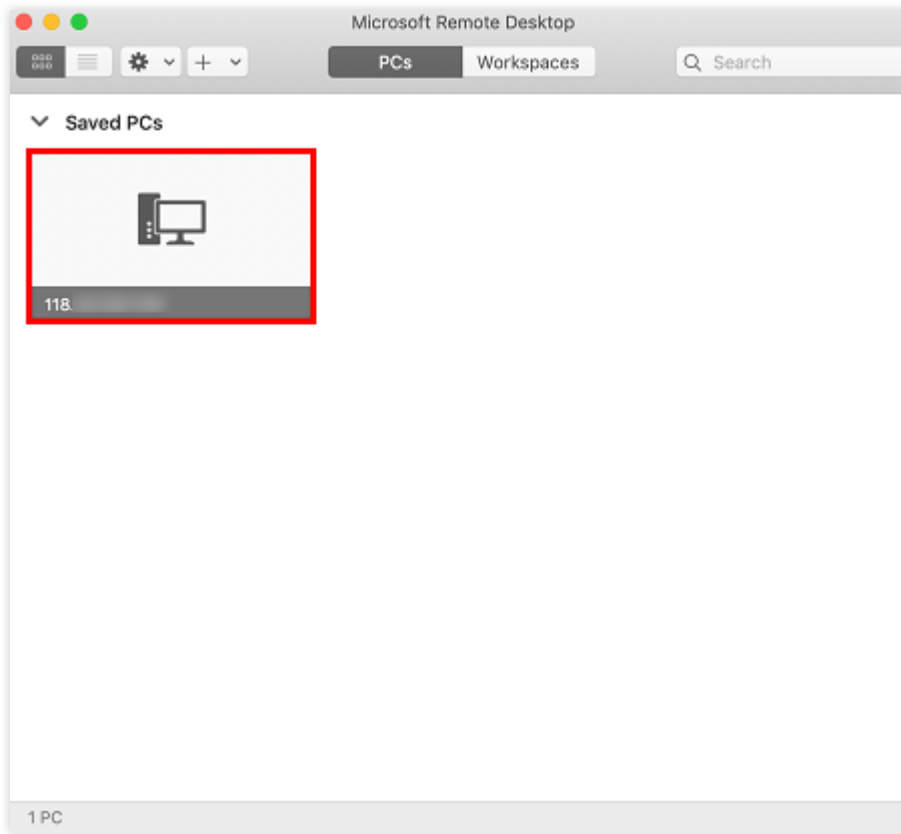


in the lower-left corner and select the folder to be uploaded in the pop-up window.

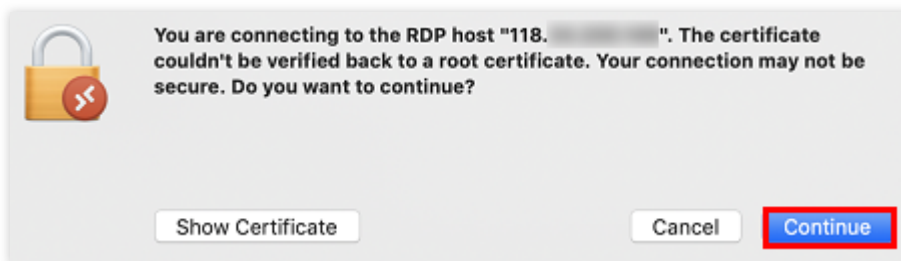
2.4 Check your list of folders to upload and click **Add**.

2.5 Retain the default settings for the other options and establish the connection.

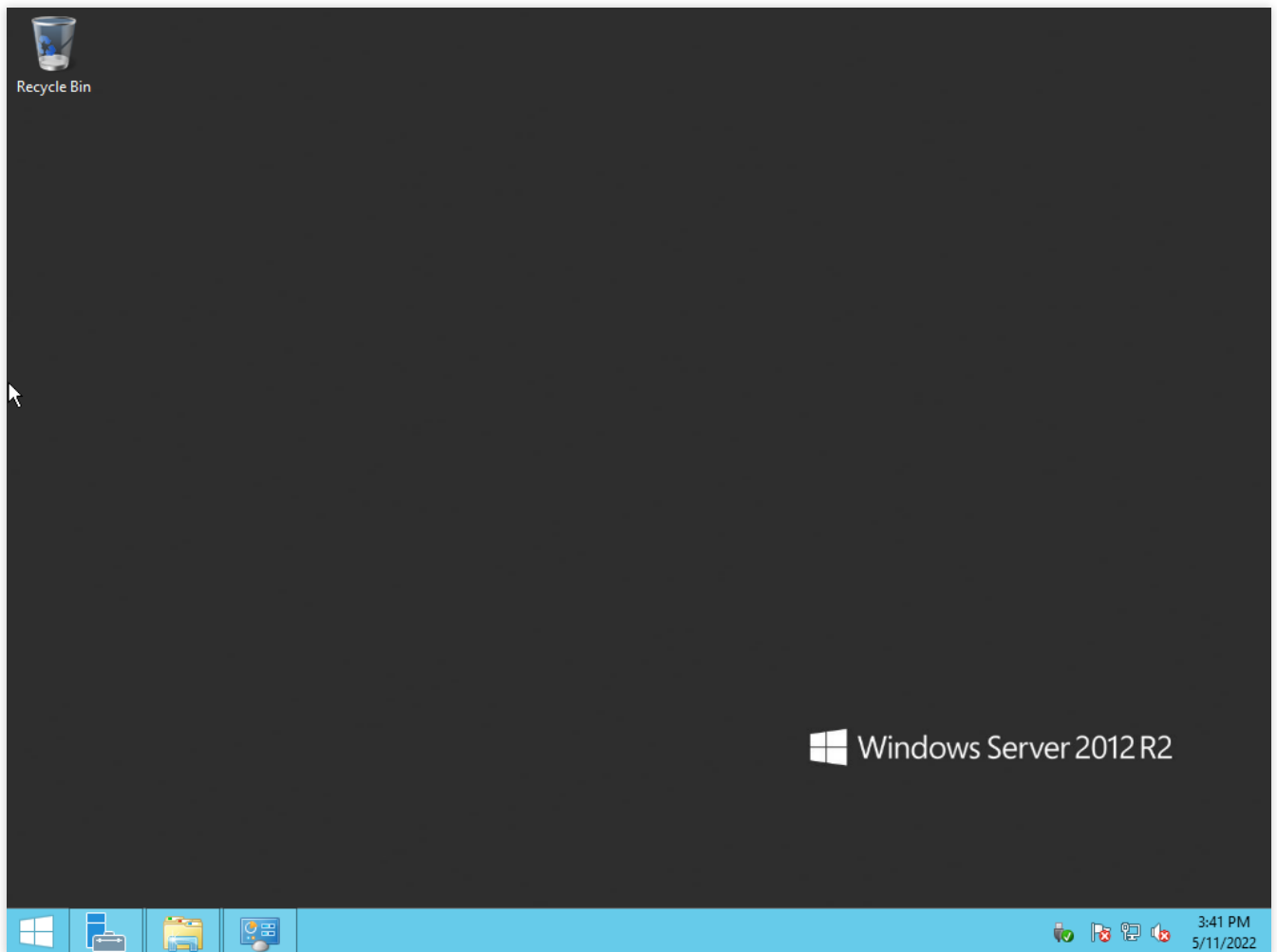
Your entry has now been saved, as shown below:



3. Double-click the new entry. Enter your username and password for the Lighthouse instance and click **Continue**.
4. In the pop-up window, click **Continue** to establish the connection, as shown below:



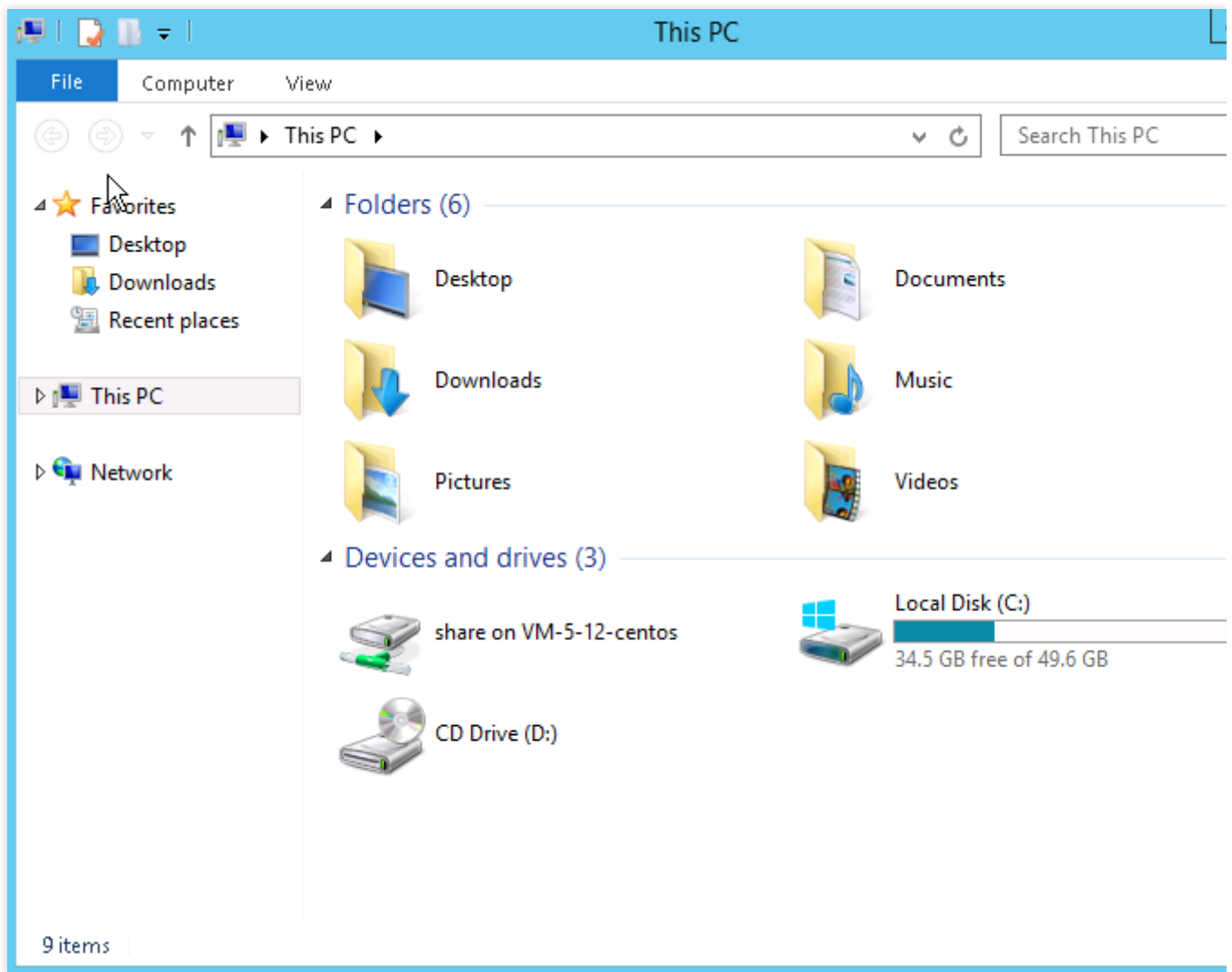
If the connection is successful, the following page will appear:



5. Click



in the lower-left corner and select **My Computer** to see a list of shared folders as shown below:



6. Double-click a shared folder to open it. Copy desired local files to another drive of the Windows Lighthouse instance.

For example, copy the file A from the folder to the C drive of the Windows Lighthouse instance.

## Downloading files

To download files from the Windows Lighthouse instance to your computer, you only need to copy desired files from the instance to a shared folder.