Hyper Elastic Cloud Server User Guide

FAQs

Issue	**06**
Date	**2021-01-08**



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

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

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

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

Notice

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

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

Contents

1 Product Consultation 1
1.1 How Do I Register with HUAWEI CLOUD and Complete Real-Name Authentication? 1
1.2 What Are the Differences Between HECS and ECS? 1
1.3 What Are the HECS Performance Metrics? 3
1.4 Why Is My HECS Not Displayed on the Management Console? 3
1.5 Why Does the Console Display a Message Indicating that the Agent Is Not Installed? 5
2 Billing 8
2.1 What Should I Do If I Want to Retain My HECS After It Expires? 8
2.2 How Do I Unsubscribe from My HECS? 8
2.3 What Are HECS Billing Modes? 9
3 Creation and Deletion 10
3.1 What Types of Images Can Be Used to Create HECSs? 10
4 Login and Connection 12
4.1 What Should Be Prepared for Logging In to an HECS? 12
4.2 What Are the Username and Password for Remote Logins? 13
4.3 Can I Retrieve My Remote Login Password? 13
4.4 Why Can't I Log In to My Windows HECS? 14
4.5 Why Can't I Log In to My Linux HECS? 22
4.6 How Can I Enable Multi-User Login on a Windows HECS? 28
4.7 Applying for a License for Authenticating Multi-User Sessions and Activating the HECS 42
5 Network Configurations 57
5.1 Why Can't an EIP Be Pinged? 57
5.2 Why Is Outbound Access Through TCP Port 25 Restricted? 64
5.3 What Should I Do If My Windows HECS Cannot Access the Internet? 65
5.4 Why Can't the Website Deployed on an HECS Be Accessed? 66
5.5 Why Accessing a Website Outside the Chinese Mainland Is Slow on an HECS? 74
6 File Uploading 83
6.1 How Can I Upload a File to a Windows HECS? 83
6.2 How Can I Transfer Data Between a Local Host and a Windows HECS? 86
6.3 How Can I Use WinSCP to Upload a File to a Linux HECS? 90

 Copyright © Huawei Technologies Co., Ltd.

7 Disk Management 92
7.1 What Is the Mapping Between Device Names and Disks? 92
7.2 What Should I Do If a Disk Is Offline? 94
7.3 What Should I Do If the Data Disk of a Windows HECS Becomes Offline After the HECS Specifications Are Modified? 95
7.4 What Should I Do If the Disk of a Linux HECS Becomes Offline After the HECS Specifications Are Modified? 98
7.5 What Are the Restrictions on Attaching an EVS Disk to an HECS? 100
8 Password Management 101
8.1 Resetting the Password for Logging In to a Windows HECS Without Password Reset Plug-ins Installed 101
8.2 Resetting the Password for Logging In to a Linux HECS Without Password Reset Plug-ins Installed 104
9 Resource Monitoring 106
9.1 Why Is My Windows HECS Running Slowly? 106
9.2 Why Is My Linux HECS Running Slowly? 111
10 Change History 116

 Copyright © Huawei Technologies Co., Ltd.

1 Product Consultation

1.1 How Do I Register with HUAWEI CLOUD and Complete Real-Name Authentication?

If you already have a HUAWEI CLOUD account, skip this part. If you do not have a HUAWEI CLOUD account, perform the following operations to create an account:

1. Visit official HUAWEI CLOUD website.
2. Click **Register** and complete the registration as instructed.

   After the registration, the system automatically redirects you to your personal information page.
3. Complete real-name authentication for individual or enterprise accounts. For details, see Individual Real-Name Authentication Process.

More information:

- For details about HECS pricing, see Product Pricing Details.
- Before purchasing HECSs, ensure that your account balance is sufficient. Top up an account if required.

1.2 What Are the Differences Between HECS and ECS?

Differences between HECS and ECS:

- HECSs can be created based on preset configurations and can be used to deploy, configure, and manage applications more conveniently and efficiently in light-load scenarios.
- ECSs have various billing modes, flavors, image types, and disk types. You can customize your ECS configuration based on service scenarios.

Table 1-1 describes the differences between HECS and ECS.

Table 1-1 Differences between HECS and ECS:

Item	HECS	ECS
Application	Light-load scenarios, such as	All service scenarios

 Copyright © Huawei Technologies Co., Ltd.

Item	HECS	ECS
scenario	website deployment and R&D	
Billing mode	Yearly/Monthly	• Yearly/Monthly • Pay-per-use • Spot price
Specifications	Preset configurations with different ratios of vCPU and memory You can select an entry, basic, or advanced configuration, or customize your own one. For details, see Select a Configuration.	A variety of ECS types and specifications
Image	• HECS creation: public or Marketplace image • OS reinstallation and change: public, private, or shared image (You need to replicate a shared image first and rename it to make it available in the private image list.)	Public, private, Marketplace, or shared image
Disk	Use the disk type in the selected preset configuration. Supported disk types: • High I/O • Ultra-high I/O	Select a required disk type. For the disk types supported by an ECS, see Disk Types and Disk Performance.
Network	• An EIP is automatically assigned. If you customize the configuration when purchasing an HECS and set **Bandwidth** to **Do not configure**, you can bind an EIP to the HECS after the HECS is purchased. • Use the EIP type in the selected preset configuration. • Billed by bandwidth	• Choose whether to bind an EIP. • Select an EIP type as required. • Billed by bandwidth, traffic, or shared bandwidth
Login mode	Password	Password or key pair
Integrated service	• Host Security Service (HSS) • Cloud Eye (Alarm rules can be configured on the HECS console.).	HSS
Supported operation	The following lists the functions that are frequently used: • Log in to a Linux HECS using CloudShell.	The following lists the functions that are frequently used: • Log in to a Linux ECS using CloudShell.

 Copyright © Huawei Technologies Co., Ltd.

Item	HECS	ECS
	• Attach, expand, and add disks. • Configure security groups. • Add, delete NICs, and change VPCs. • Reinstall, change the OS, and modify specifications. • View distribution of HECSs in different regions. • Deploy an application.	• Attach, expand, and add disks. • Configure security groups. • Add, delete NICs, and change VPCs. • Reinstall, change the OS, and modify specifications. • View distribution of HECSs in different regions.

1.3 What Are the HECS Performance Metrics?

- Ratio of vCPU/memory (GB): 1:1, 1:2, or 1:4
- vCPUs: 1-8
- Base frequency: 2.2 GHz to 2.6 GHz
- Turbo frequency: 3.2 GHz
- Maximum PPS: 500,000
- Maximum intranet bandwidth: 3 Gbit/s

1.4 Why Is My HECS Not Displayed on the Management Console?

Symptom

After I logged in to the management console, I could not find my HECS.

Possible Causes

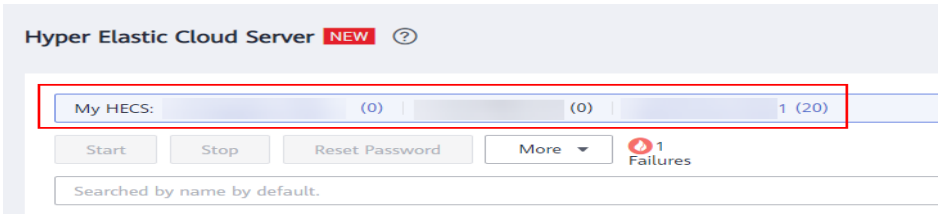
- The HECS is not in the current region.
- You are not on the HECS management console.

Solution

1. Log in to the HECS management console.
2. In the upper left of the HECS list, you can view your HECS quantity in each region.

 Copyright © Huawei Technologies Co., Ltd.

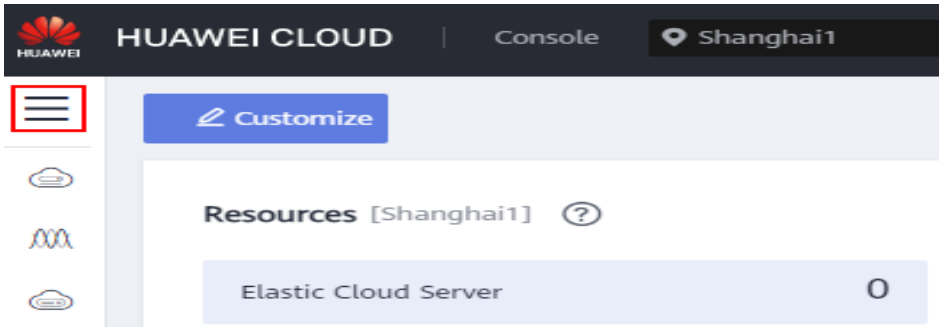
Figure 1-1 Viewing HECSs in each region



3. On the console homepage, follow HECS. You can then view the HECS resources in the current region on the console homepage.

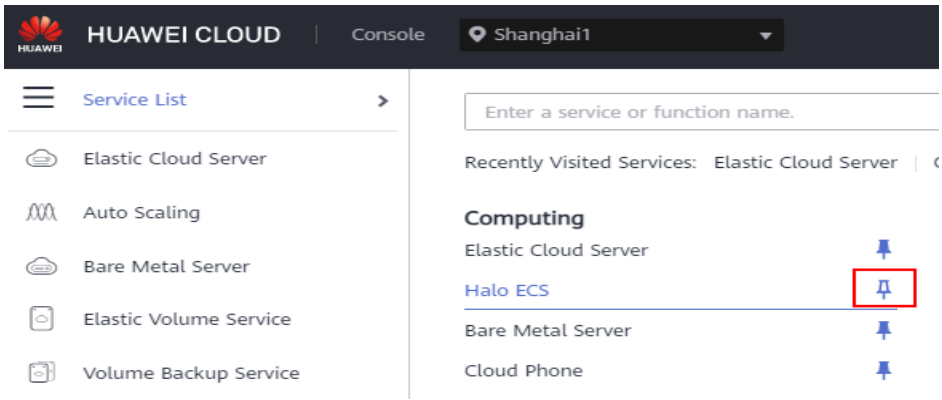
   a. On the console homepage, click ☰.

   Figure 1-2 Set followed resources



   b. Add HECS to followed resources.

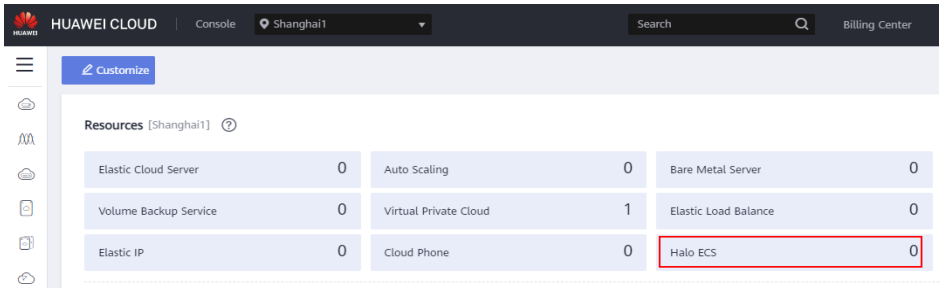
   Figure 1-3 Adding HECS to followed resources



   After HECS is added, you can view the HECS resources in the current region on the console homepage.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-4 Viewing HECS resources

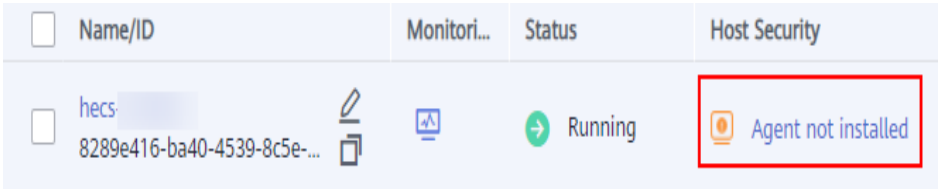


1.5 Why Does the Console Display a Message Indicating that the Agent Is Not Installed?

Symptom

After you purchase an HECS, **Agent not installed** is displayed in the **Host Security** column on the management console.

Figure 1-5 Agent not installed



Fault Locating

The possible causes are as follows:

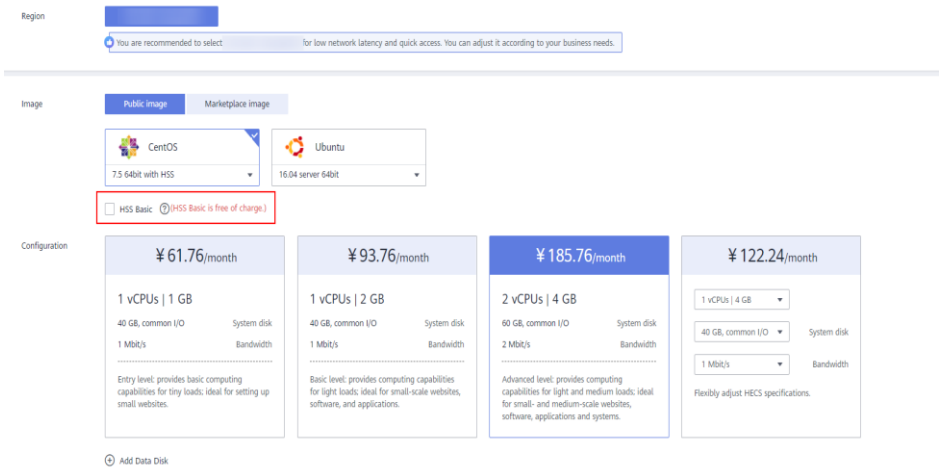
- The Agent is being installed.

  The Agent is being installed because the HECS is newly created. Refresh the page later.
- The Agent is not installed.

  If you do not enable host security (basic) when purchasing an HECS, the Agent is not installed. If you want to install the agent, refer to Installing an Agent.

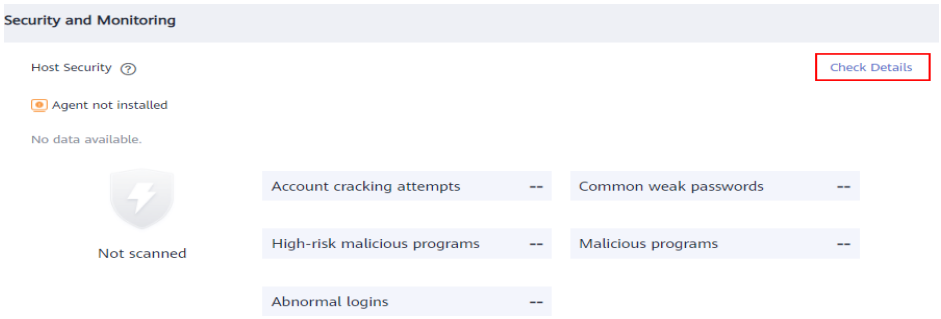
 Copyright © Huawei Technologies Co., Ltd.

Figure 1-6 Host security is not enable when you purchase the HECS.



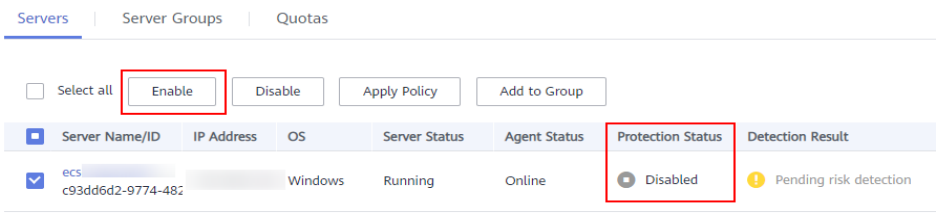
- The Agent has been installed but fails to be started.
  a. On the HECS console, click **Agent not installed**. The HECS details page is displayed.
  b. In the **Security and Monitoring** area, click **Check Details** to go to the HSS console.

  Figure 1-7 Viewing protection status



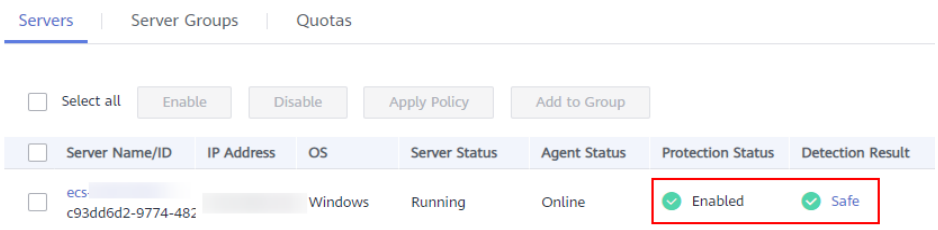
  c. Enable host security on the HSS console.

  Figure 1-8 Host security not enabled



 Copyright © Huawei Technologies Co., Ltd.

Figure 1-9 Host security enabled



2 Billing

2.1 What Should I Do If I Want to Retain My HECS After It Expires?

On the **Hyper Elastic Cloud Server** page, click **More** in the **Operation** column and select **Renew** from the drop-down list.

2.2 How Do I Unsubscribe from My HECS?

A yearly/monthly HECS can be unsubscribed, including the renewed resources and the resources that are being used. The HECS is unavailable after unsubscription. A handling fee will be charged for unsubscribing from a resource.

Notes

- Unsubscribing from an HECS involves the renewed resources and the resources that are being used. The HECS is unavailable after unsubscription.
- Solution product portfolios can only be unsubscribed from as a whole.
- If an order contains resources in a primary-secondary relationship, you must unsubscribe from the resources separately.
- For instructions on how to unsubscribe from a resource, see Unsubscription Rules.

Procedure

NOTICE

- Before requesting an unsubscription, ensure that you have migrated or backed up any data saved on the HECS that will be unsubscribed from. The HECS and any data it contains will be permanently deleted when unsubscription is complete.
- The middle of the unsubscription page displays a message showing the number of unsubscriptions you have performed and the remaining allowed number.

1. Locate the row that contains the target HECS, click **More** in the **Operation** column, and select **Unsubscribe**.

 Copyright © Huawei Technologies Co., Ltd.

2. View the unsubscription information and select the resources to be unsubscribed from.
3. (Optional) Select the reason for unsubscription.
4. Click **Unsubscribe**.

2.3 What Are HECS Billing Modes?

HECSs are billed in yearly/monthly payments. In this billing mode, the settlement is based on the service duration of the order, offering a large discount.

For details about the HECS pricing, see *Hyper Elastic Cloud Server Pricing Details*.

 Copyright © Huawei Technologies Co., Ltd.

3 Creation and Deletion

3.1 What Types of Images Can Be Used to Create HECSs?

Both public and Marketplace images can be used to create HECSs.

A private image cannot be used to create an HECS.

Table 3-1 Public, Private and Marketplace images

Image Type	Description	Scenario Recommendation
Public image	A public image contains only the initial OS. It does not contain any application or environment data.	A public image provides only the initial environment. You can install desired applications. If you are familiar with system and application environment configurations, select a public image.
Private image	An image available only to the user who created it. It contains an OS, preinstalled public applications, and the user's private applications. A system disk image contains an OS and pre-installed application software for running services. It can be used to create HECSs and migrate your services to the cloud. **NOTE** • Private images can only be used when changing OSs. • Only system disk images or full-HECS images can be used to change OSs with private images.	Using a private image to create HECSs removes the need to configure multiple HECSs repeatedly. For details about how to create a private image, see *Image Management Service User Guide*.
Marketplace image	A Marketplace image can be used to deploy a specific software environment. It contains the following	Using Marketplace images enables enterprises to quickly build specified software environments, without having to manually configure environments or

 Copyright © Huawei Technologies Co., Ltd.

Image Type	Description	Scenario Recommendation
	configuration: • OS • Runtime environment desired for applications • Applications and their initialization data	installing software. This is suitable for Internet startups.

For details about Marketplace image types and the OSs supported by public images, see Images in *Hyper Elastic Cloud Server Service Overview*.

 Copyright © Huawei Technologies Co., Ltd.

4 Login and Connection

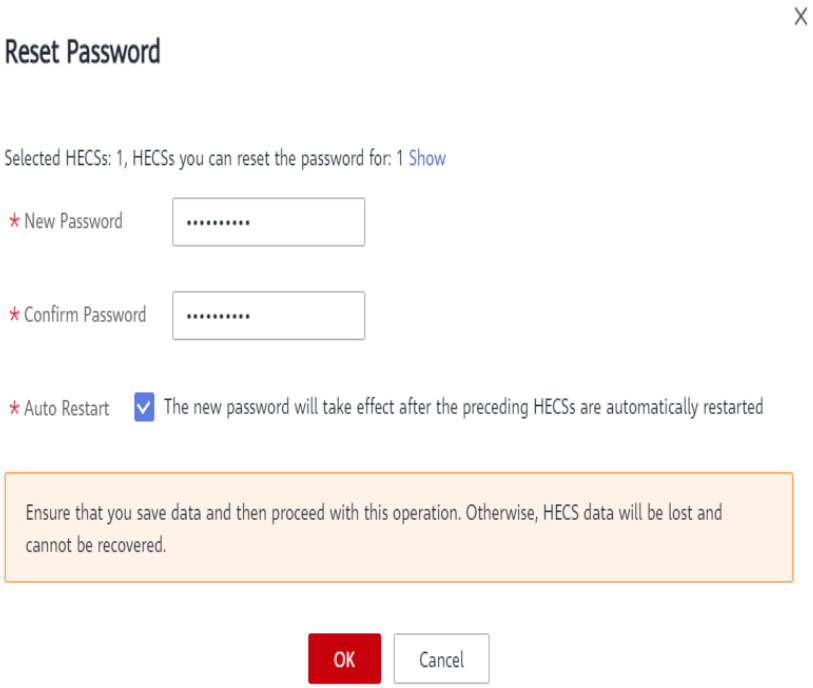
4.1 What Should Be Prepared for Logging In to an HECS?

Windows

- Obtain the login password.

  HECSs created using a public image have one-click password reset plug-ins installed by default. If you have forgotten the password, use the password reset function to obtain a new password for logging in to the HECS.

  Figure 4-1 Reset Password

- Ensure that the HECS has an EIP bound (only required for MSTSC logins).

  By default, an EIP is bound to an HECS after the HECS is purchased.

 Copyright © Huawei Technologies Co., Ltd.

- Ensure that the remote desktop protocol has been enabled on the HECS (only required for MSTSC logins).

  By default, RDP has been enabled on the HECS.

Linux

- Obtain the login password.

  HECSs created using a public image have one-click password reset plug-ins installed by default. If your password was forgotten or has expired, use the password reset function to obtain a new password for logging in to the HECS.
- Ensure that the HECS has an EIP bound (only required for SSH logins).

  SSH logins apply to only Linux HECSs. You can use a remote login tool, such as PuTTY, to log in to your HECS. In such a case, the HECS must have an EIP bound.

  – Verify that the HECS has an EIP bound.

    By default, an EIP is bound to an HECS after the HECS is purchased.

  – Check whether the EIP bound to the HECS can be pinged.

    Ensure that the security group has allowed ICMP. If the EIP cannot be pinged, resolve this issue by following the instructions provided in 5.1 Why Can't an EIP Be Pinged?

4.2 What Are the Username and Password for Remote Logins?

Username for logging in to an HECS:

- For Windows: **Administrator**
- For Linux: **root**

If you forgot your login password is forgotten, reset password on the management console to set a new password.

To reset a password, locate the row containing the target HECS and click **Reset Password** in the **Operation** column.

4.3 Can I Retrieve My Remote Login Password?

If you did not set a password when creating an HECS, or the password has been set but it is forgotten or expires, reset password on the management console.

To reset a password, locate the row containing the target HECS and click **Reset Password** in the **Operation** column.

NOTE

Keep your password secure.

 Copyright © Huawei Technologies Co., Ltd.

4.4 Why Can't I Log In to My Windows HECS?

Description

An HECS cannot be logged in for some reason, for example, the network is malfunctioning, the local port for accessing the remote desktop is denied on the firewall, or the CPU is overloaded on the HECS.

If this issue occurs, follow the instructions provided in Attempting Login Using VNC on the Management Console. Then, locate the login fault based on Fault Locating.

Attempting Login Using VNC on the Management Console

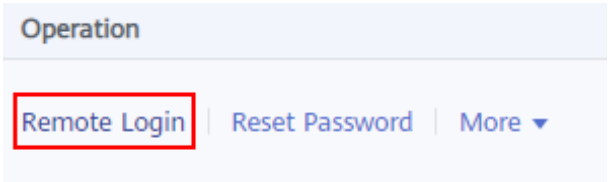
If the remote login fails, check whether you can log in to the HECS using VNC on the management console.

NOTE

Click 4.1 What Should Be Prepared for Logging In to an HECS? to learn the preparations for logging in to an HECS.

1. Log in to the management console.
2. Under **Computing**, click **Hyper ECS**.
3. In the **Operation** column of the target HECS, click **Remote Login**.

Figure 4-2 Remote Login



If the login using VNC fails after the preceding operations are performed, record your resources and the time when the fault occurred. Then, click **Service Tickets** in the upper right corner of the management console, choose **Create Service Ticket**, and submit a ticket for technical support.

Fault Locating

If you can log in to the HECS using VNC but cannot log in to it using a remote desktop connection, locate the fault by following the following procedure.

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-3 Fault locating



Table 4-1 Fault locating

Possible Cause	Handling Measure
The HECS is frozen or stopped.	Ensure that the HECS is in the **Running** state. For details, see Checking the HECS Status.
Incorrect username or password.	The default username for Windows HECSs is **Administrator**. If the password is incorrect, reset the password using the password reset function on the management console. For details, see Checking the Login Password.
The HECS is overloaded.	Check the bandwidth or vCPU usage of the HECS. If the bandwidth or vCPU usage is excessively high, login failures may occur. For details, see Checking the HECS Load.
No EIP is bound to the HECS.	Bind an EIP to the HECS if you want to log in to the HECS using an RDP file or remote desktop connection (MSTSC). For details, see Checking the HECS EIP.
The access is blocked by the Internet service provider (ISP).	Access the HECS using another hotspot or network. For details, see Checking the Network.
The access is blocked	Disable the firewall and try again. For details, see Checking the

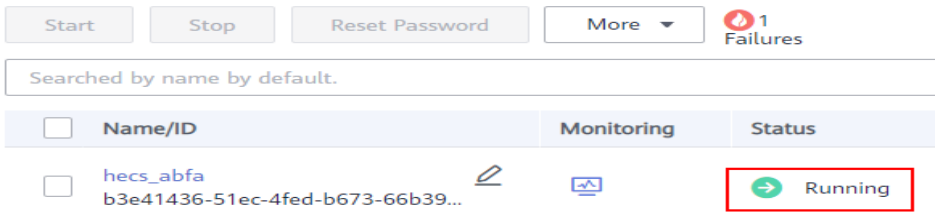
 Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Handling Measure
by the firewall.	Firewall.
The remote login port has been disabled in the security group or on the HECS.	Check whether the remote login port is enabled in the security group and on the HECS. For details, see Checking the Port.
An IP address whitelist for SSH logins has been configured.	Check whether an SSH login IP address whitelist is configured in HSS. For details, see Checking the IP Address Whitelist for SSH Logins (with HSS Enabled).
The remote desktop protocol has been disabled on the HECS.	Make sure that the remote desktop protocol has been enabled on the HECS (only required for RDP and MSTSC logins). For details, see Checking the Remote Desktop Protocol.
The access is blocked by third-party antivirus software.	Disable or uninstall the third-party antivirus software and try again. For details, see Checking the Antivirus Software.
The cause is displayed in the error message.	If an error message is displayed during a remote login, check the operation guide based on the error information. For details, see Checking Whether an Error Occurred During the Remote Login.

Checking the HECS Status

Check whether the HECS is in the **Running** status on the management console. If the HECS is stopped, start it and try again.

Figure 4-4 Checking the HECS status

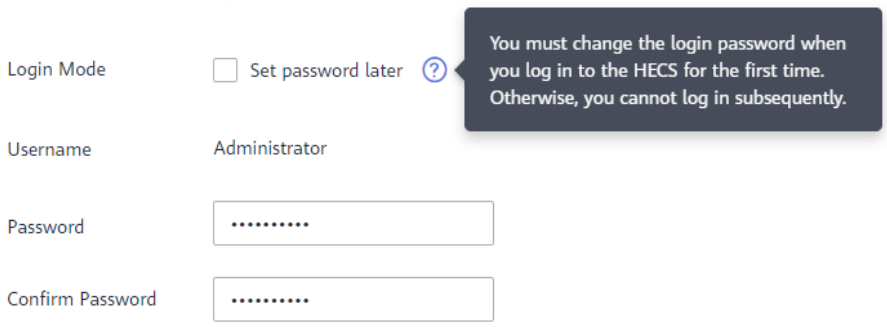


Checking the Login Password

Check the login password you set when or after you create the HECS.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-5 Login password



- Set the password during HECS creation: Check whether the password is correct. If your password is forgotten, reset the password, restart the HECS, and log in to it using the new password.
- Set the password after HECS creation: If you choose not to set a password when you create the HECS, you can use the password reset function (available in the **Operation** column of the HECS) to obtain the login password after the HECS is created. Then, restart and log in to it using the new password.

Checking the HECS Load

If the bandwidth or vCPU usage is excessively high, you may fail to log in to the HECS.

If you have created an alarm rule using Cloud Eye, the system automatically generates an alarm when the bandwidth or CPU usage reaches the threshold specified in the rule.

To handle this issue, perform the operations described in 9.1 Why Is My Windows HECS Running Slowly?.

- If the login failure is caused by high vCPU usage, perform the following operations to reduce the vCPU usage:
  - Stop the processes that are not being used and try again.
  - Verify that the Windows Update process is not running on the backend.
  - Restart the HECS.
  - Reinstall the HECS OS. Back up important data before the reinstallation.
  - If the OS cannot be reinstalled due to important data, replace the disk attached to the HECS. To do so, back up the data on the original disk, detach the disk from the HECS, attach the new disk to the HECS, and copy the data to the new disk.

  You can also upgrade the vCPUs and memory by modifying the HECS specifications.
- If the login fails because the bandwidth exceeds the limit, perform the following operations:

  Check whether the bandwidth exceeds the configured bandwidth size. For details, see How Do I Check Whether the Bandwidth Exceeds the Limit?

After you perform the preceding operations, try to remotely log in to the HECS again.

Checking the HECS EIP

An HECS can access the Internet after it is bound with an EIP.

 Copyright © Huawei Technologies Co., Ltd.

Before logging in to an HECS using RDP or MSTSC, make sure that an EIP has been bound to the HECS. For details, see Assigning an EIP and Binding It to an ECS.

NOTE

When logging in to an HECS through an intranet, for example, through VPN or Direct Connect, you do not need to bind an EIP to the HECS.

Checking the Network

Use a local PC in another network or use another hotspot to access the HECS. Check whether the fault occurs on the local network. If so, contact the carrier to resolve this issue.

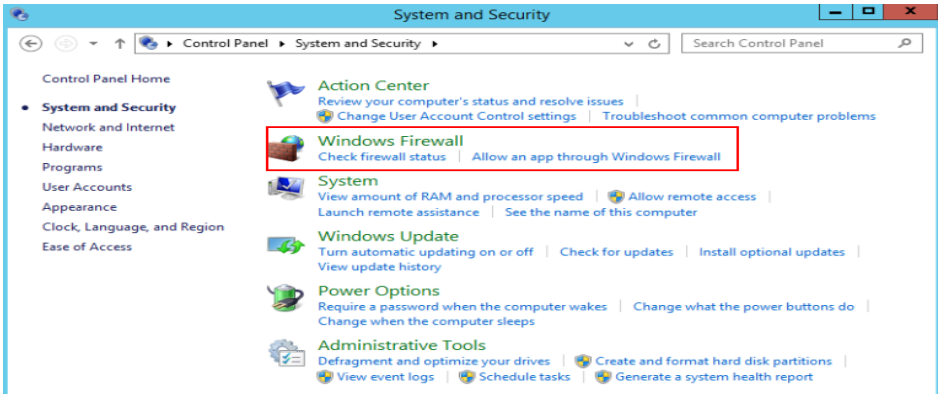
After you perform the preceding operations, try to remotely log in to the HECS again.

Checking the Firewall

Check whether the firewall is enabled.

1. Log in to the Windows HECS.
2. Click the Windows icon in the lower left corner of the desktop and choose **Control Panel** > **System and Security** > **Windows Firewall**.

Figure 4-6 Windows firewall

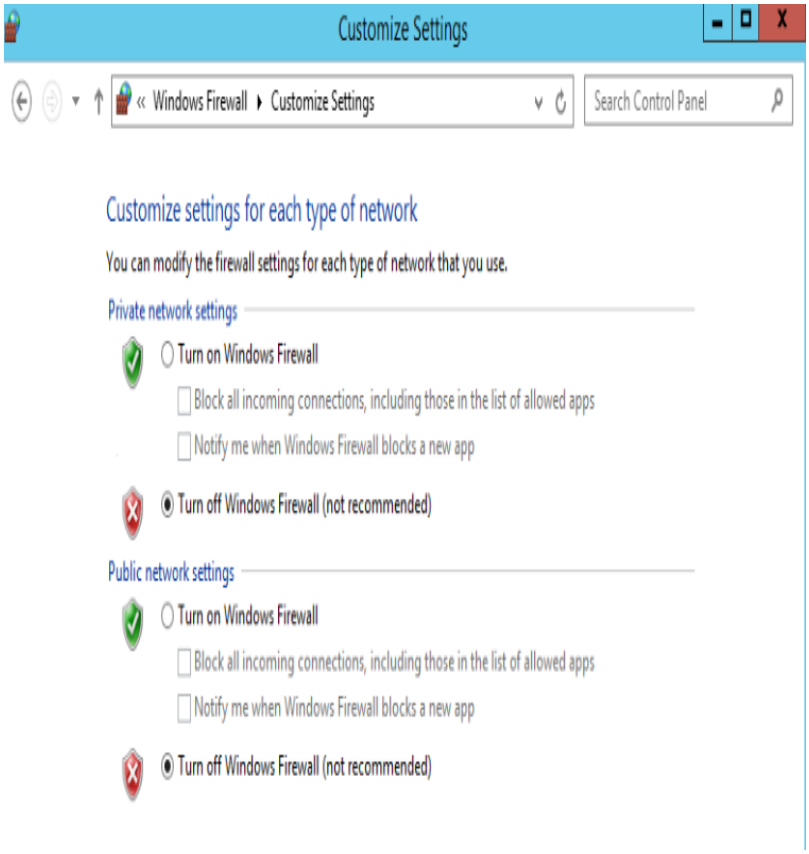


3. Choose **Check firewall status** > **Turn Windows Firewall on or off**.

   View and set the firewall status.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-7 Turning off a firewall



Ensure that the remote access port on the local end is allowed on the firewall. The default port is TCP 3389.

If the port configured in the inbound rule of the firewall is different from that configured on the remote server, the remote login fails. In such a case, add the port configured on the remote server to the inbound rule of the firewall.

For details, see Disabling a Windows ECS Firewall and Adding a Port Exception on a Windows ECS Firewall.

NOTE

The default port is 3389. If you use another port, add that port in the inbound rule of the firewall.

After performing the preceding operations, try to remotely log in to the HECS again.

Checking the Port

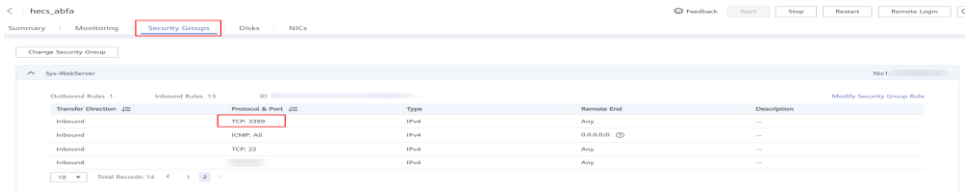
1. Check whether port 3389 (used by default) on the HECS is accessible.

   Ensure that port 3389 has been allowed in the inbound rule.

   On the page providing details about the HECS, click the **Security Groups** tab and view port 3389 in the inbound rule of the security group.

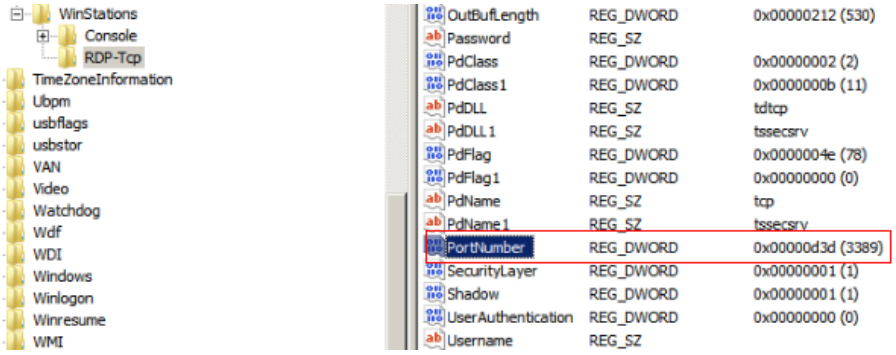
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-8 Checking security group rules



- View default security group rules.
- Learn how to modify a security group rule.

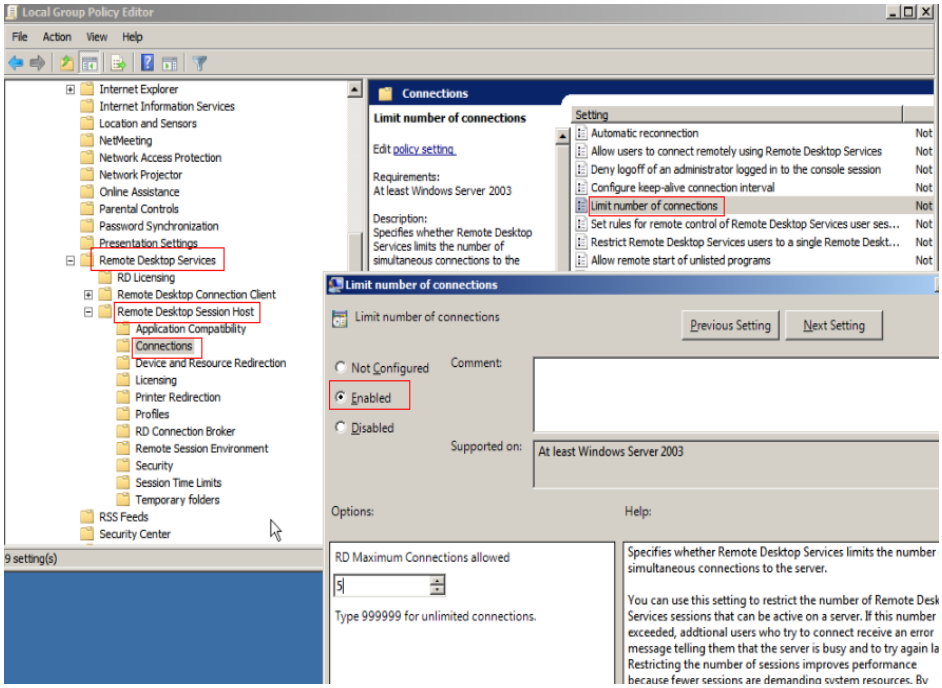
2. Check whether the remote access port on the HECS has been changed.
   a. Choose **Start** > **Run**, enter **cmd**, and press **Enter**. In the CLI, enter **regedit** to open **Registry Editor**.
   b. In **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP Tcp\PortNumber**, check whether the port is the default port 3389. If not, change the port to the one configured for remote logins.



3. Check whether the number of connections to the HECS is limited.

   Check the internal remote desktop configuration of the HECS.
   a. Choose **Start** > **Run**, enter **cmd**, and press **Enter**. In the CLI, enter **gpedit.msc** to open **Local Group Policy Editor**.
   b. Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**. Then, in the **Limit number of connections** dialog box, check whether the number is limited.

 Copyright © Huawei Technologies Co., Ltd.



NOTE

If **Limit number of connections** is set to **Enabled**, a remote connection to the Windows HECS may fail when the number of connections exceeds the limit. In such an event, disable **Limit number of connections** or set a larger limit for connections.

After performing the preceding operations, try to remotely log in to the HECS again.

Checking the IP Address Whitelist for SSH Logins (with HSS Enabled)

After HSS is enabled, you can configure an IP address whitelist for SSH logins as required. The IP address whitelist controls SSH access to HECSs, effectively preventing account cracking.

After you configure the whitelist, SSH logins will be allowed only from IP addresses in the whitelist.

1. On the **Events** page, check whether a local host IP address is intercepted due to brute force cracking.
2. Check whether the IP address whitelist for SSH logins has been enabled. If so, ensure that the IP address of the local host has been added to the IP address whitelist.

CAUTION

- Before enabling this function, ensure that all IP addresses that need to initiate SSH logins are added to the whitelist. Otherwise, you cannot remotely log in to your HECS through SSH.
- Exercise caution when adding a local IP address to the whitelist. This will make HSS no longer restrict access from this IP address to your HECSs.

For more details, see Security Configuration.

 Copyright © Huawei Technologies Co., Ltd.

Checking the Remote Desktop Protocol

Make sure that the remote desktop protocol has been enabled on the HECS (only required for RDP and MSTSC logins).

Log in to the HECS using VNC and enable the remote desktop protocol.

For details, see Login Using MSTSC.

Checking the Antivirus Software

Third-party antivirus software may lead to an access failure to the HECS.

If third-party antivirus software is running, check whether the remote connection is blocked by the software. If so, add the EIP of the HECS to the whitelist and try to access the HECS again.

Checking Whether an Error Occurred During the Remote Login

If an error message is displayed during a remote login, find the error information in the operation guide. The methods for resolving a remote login error for an HECS are the same as those for handling a remote login error for an ECS. For details, see Remote Login Errors on Windows.

If the error cannot be resolved, record the message and the time when the error occurred. Then, click **Service Tickets** in the upper right corner of the management console, choose **Create Service Ticket**, and submit a ticket for technical support.

After performing the preceding operations, try to remotely log in to the HECS again.

If the fault persists after you have performed the preceding operations, record the resource information and the time when the fault occurred. Then, click **Service Tickets** in the upper right corner of the management console, choose **Create Service Ticket**, and submit a ticket for technical support.

4.5 Why Can't I Log In to My Linux HECS?

Symptom

An HECS cannot be remotely logged in for some reason. For example, the network is malfunctioning, the local port for accessing the remote desktop is denied on the firewall, or the HECS vCPUs are overloaded.

If this issue occurs, log in to the HECS by referring to Attempting Login Using VNC. Then, locate the fault based on Fault Locating.

Attempting Login Using VNC

If the remote login fails, log in to the HECS using VNC on the management console.

NOTE

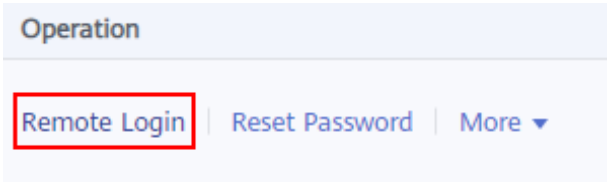
Learn the preparations for logging in to an HECS by referring to 4.1 What Should Be Prepared for Logging In to an HECS?.

1. Log in to the management console.

 Copyright © Huawei Technologies Co., Ltd.

2. Under **Computing**, click **Hyper ECS**.
3. In the **Operation** column of the target HECS, click **Remote Login**.

Figure 4-9 Remote Login



If the login fails, record resource information and the time when the fault occurred, and then submit a service ticket for technical support (click **Service Tickets** in the upper right corner of the console and choose **Create Service Ticket**).

Fault Locating

If you can log in to the HECS using VNC but cannot log in to it using a remote desktop connection, locate the fault by following the following procedure.

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one.

Figure 4-10 Fault locating



 Copyright © Huawei Technologies Co., Ltd.

Table 4-2 Fault locating

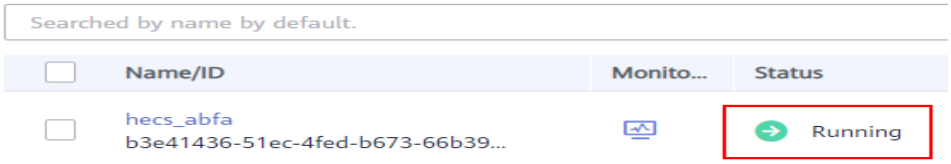
Possible Cause	Handling Measure
The HECS is frozen or stopped.	Ensure that the HECS is in the **Running** state. For details, see Checking the HECS Status.
Incorrect username or password.	The default username for Linux HECSs is **root**. If the password is incorrect, reset the password using the password reset function on the management console. For details, see Checking the Login Password.
The HECS is overloaded.	Check the bandwidth or vCPU usage of the HECS. If the bandwidth or vCPU usage is excessively high, login failures may occur. For details, see Checking the HECS Load.
No EIP is bound to the HECS.	Bind an EIP to the HECS if you want to log in to the HECS using an RDP file or remote desktop connection (MSTSC). For details, see Checking the HECS EIP.
The access is blocked by the Internet service provider (ISP).	Access the HECS using another hotspot or network. For details, see Checking the Network.
The remote login port is not allowed in the security group.	Ensure that the remote login port is allowed in the security group. For details, see Checking the Security Group Configuration.
The remote login port is incorrectly configured.	Configure the remote login port correctly on a local PC and the HECS. For details, see Checking the Remote Access Port.
An IP address whitelist for SSH logins has been configured.	Check whether an SSH login IP address whitelist is configured on the HECS. For details, see Checking the IP Address Whitelist for SSH Logins (with HSS Enabled).
An OS fault has occurred.	Ensure that the file system is not damaged. For details, see Checking the OS Fault.
Access is blocked by third-party antivirus software.	Disable or uninstall the third-party antivirus software and try again. For details, see Checking the Antivirus Software.
The cause is displayed in the error message.	If an error message is displayed during a remote login, check the operation guide based on the error information. For details, see Checking Whether an Error Occurred During the Remote Login.

Checking the HECS Status

Check whether the HECS is in the **Running** status on the management console. If the HECS is stopped, start it and try again.

 Copyright © Huawei Technologies Co., Ltd.

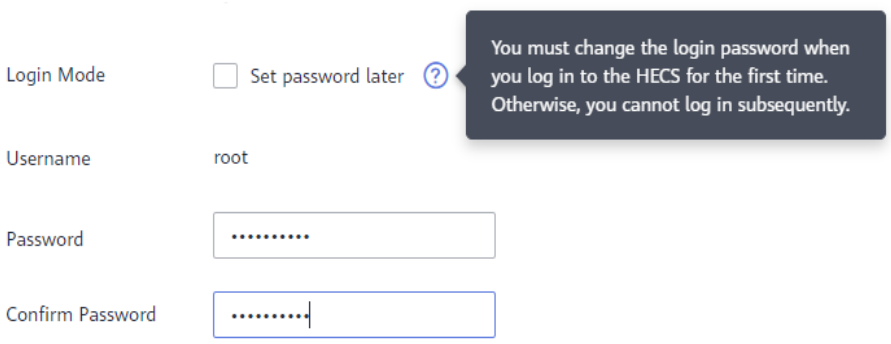
Figure 4-11 Checking the HECS status



Checking the Login Password

Check the login password you set when or after you create the HECS.

Figure 4-12 Login password



- Set the password during HECS creation: Check whether the password is correct. If your password is forgotten, reset the password, restart the HECS, and log in to it using the new password.
- Set the password after HECS creation: If you choose not to set a password when you create the HECS, you can use the password reset function (available in the **Operation** column of the HECS) to obtain the login password after the HECS is created. Then, restart and log in to it using the new password.

Checking the HECS Load

If the bandwidth or vCPU usage is excessively high, you may fail to log in to the HECS.

If you have created an alarm rule using Cloud Eye, the system automatically generates an alarm when the bandwidth or CPU usage reaches the threshold specified in the rule.

To handle this issue, perform the operations described in 9.2 Why Is My Linux HECS Running Slowly?.

- If the login failure is caused by high vCPU usage, perform the following operations to reduce the vCPU usage:
  - Stop the processes that are not being used and try again.
  - Restart the HECS.
  - Reinstall the OS. Back up important data before the reinstallation.

 Copyright © Huawei Technologies Co., Ltd.

  - If the OS cannot be reinstalled due to important data, replace the disk attached to the HECS. To do so, back up the data on the original disk, detach the disk from the HECS, attach the new disk to the HECS, and copy the data to the new disk.

  You can also upgrade the vCPUs and memory by modifying the HECS specifications.

- If the login fails because the bandwidth, check whether the bandwidth exceeds the configured bandwidth size. For details, see How Do I Check Whether the Bandwidth Exceeds the Limit?

After you perform the preceding operations, try to remotely log in to the HECS again.

Checking the HECS EIP

Bind an EIP to the HECS if you use CloudShell provided on the console or a remote login tool (such as PuTTY or XShell) to connect to a DB instance.

For details, see Binding an EIP to an ECS.

Checking the Network

Use a local PC in another network or use another hotspot to access the HECS. Check whether the fault occurs on the local network. If so, contact the carrier to resolve this issue.

After you perform the preceding operations, try to remotely log in to the HECS again.

Checking the Security Group Configuration

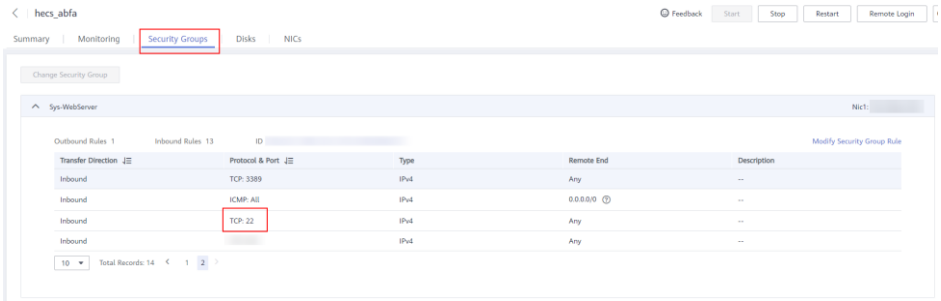
Check whether the local PC can access port 22 on the HECS:

telnet *Private IP address of the HECS*

If the port is inaccessible, check whether port 22 in the security group is allowed.

On the page providing details about the HECS, click the **Security Groups** tab and view port 22 in the inbound rule of the security group.

Figure 4-13 Checking security group rules



For instructions about how to modify a security group rule, see Modifying a Security Group Rule

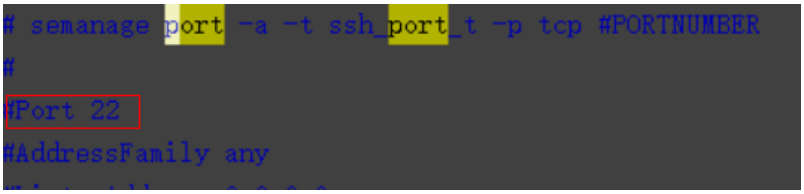
After you perform the preceding operations, try to remotely log in to the HECS again.

 Copyright © Huawei Technologies Co., Ltd.

Checking the Remote Access Port

Check the internal configuration of the HECS.

1. Verify that the sshd process is running.
2. Check whether the local PC is restricted on the HECS.
   a. Log in to the HECS and run the following command to check the configuration:
      vi /etc/hosts.deny
   b. If the IP address of the local PC is detected, the IP address is denied. In such a case, delete the IP address from the file.
3. Switch to the **ssh_config** file in **/etc/ssh** on the local PC and view the default login port. Then, check whether the SSH-enabled port in the **sshd_config** file on the HECS has been changed (the default port number is 22).



After you perform the preceding operations, try to remotely log in to the HECS again.

Checking the IP Address Whitelist for SSH Logins (with HSS Enabled)

After HSS is enabled, you can configure an IP address whitelist for SSH logins as required. The IP address whitelist controls SSH access to HECSs, effectively preventing account cracking.

After you configure the whitelist, SSH logins will be allowed only from IP addresses in the whitelist.

1. On the **Events** page, check whether a local host IP address is intercepted due to brute force cracking.
2. Check whether the IP address whitelist for SSH logins has been enabled. If so, ensure that the IP address of the local host has been added to the IP address whitelist.

CAUTION

- Before enabling this function, ensure that all IP addresses that need to initiate SSH logins are added to the whitelist. Otherwise, you cannot remotely log in to your HECS through SSH.
- Exercise caution when adding a local IP address to the whitelist. This will make HSS no longer restrict access from this IP address to your HECSs.

For more details, see Security Configuration.

Checking the OS Fault

- Password injection failure

  Failing to obtain a password is generally caused by a Cloud-Init-based password injection failure.
- File system damaged after a forcible stop

 Copyright © Huawei Technologies Co., Ltd.

The file system may be damaged. As a result, the HECS fails to be restarted.

After you perform the preceding operations, try to remotely log in to the HECS again.

Checking the Antivirus Software

Third-party antivirus software may lead to an access failure to the HECS.

If third-party antivirus software is running, check whether the remote connection is blocked by the software. If so, add the EIP of the HECS to the whitelist and try to access the HECS again.

You can also disable or uninstall the third-party antivirus software and try again.

Checking Whether an Error Occurred During the Remote Login

If an error message is displayed during a remote login, check the operation guide based on the error information. The handling method is the same as that for an ECS. For details, see ECS FAQs Remote Login Errors on Linux.

If the error cannot be handled, record the message and the time when the error occurred. Then, click **Service Tickets** in the upper right corner of the management console, choose **Create Service Ticket**, and submit a ticket for technical support.

If the fault persists after you have performed the preceding operations, record the resource information and the time when the fault occurred. Then, click **Service Tickets** in the upper right corner of the management console, choose **Create Service Ticket**, and submit a ticket for technical support.

4.6 How Can I Enable Multi-User Login on a Windows HECS?

Scenarios

This section uses an HECS running Windows Server 2012 as an example to describe how to enable concurrent logins by multiple users.

An HECS running Windows Server 2012, by default, allows concurrent logins by two users. To allow logins by more users, configure the remote desktop session host and remote desktop licensing.

NOTE

- After multi-user logins are configured, different users can log in to the HECS without affecting each other.
- The configuration in this section enables concurrent logins by multiple users or multiple concurrent logins using one account. However, a remote desktop license is valid for only 120 days. After the license expires, multi-user logins will be unavailable. For instructions on how to activate Remote Desktop Licensing, see 4.7 Applying for a License for Authenticating Multi-User Sessions and Activating the HECS.
- However, a remote desktop license is valid for only 120 days. After the license expires, multi-user logins will be unavailable. In this case, delete the remote desktop service. For details, see What Should I Do If the System Displays No Remote Desktop License Servers Available to Provide a License When I Log In to a Windows ECS?

 Copyright © Huawei Technologies Co., Ltd.

- After multi-user logins are configured on a Windows HECS, the browser may fail to be opened by multiple users. For details, see Troubleshooting a Browser Launch Error Occurred in Multi-User Login.

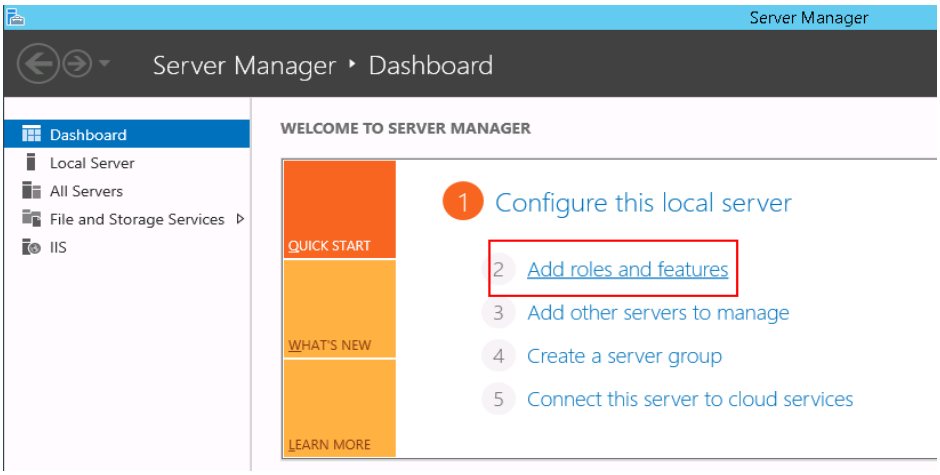
Procedure

1. Configuring Remote Desktop Session Host and Remote Desktop Licensing
2. Enabling Multi-User Logins
3. Adding a New User to the Remote Desktop Users Group

Configuring Remote Desktop Session Host and Remote Desktop Licensing

1. Log in to the Windows HECS.
2. On the OS, click  to open **Server Manager**. Click **Add roles and features**.

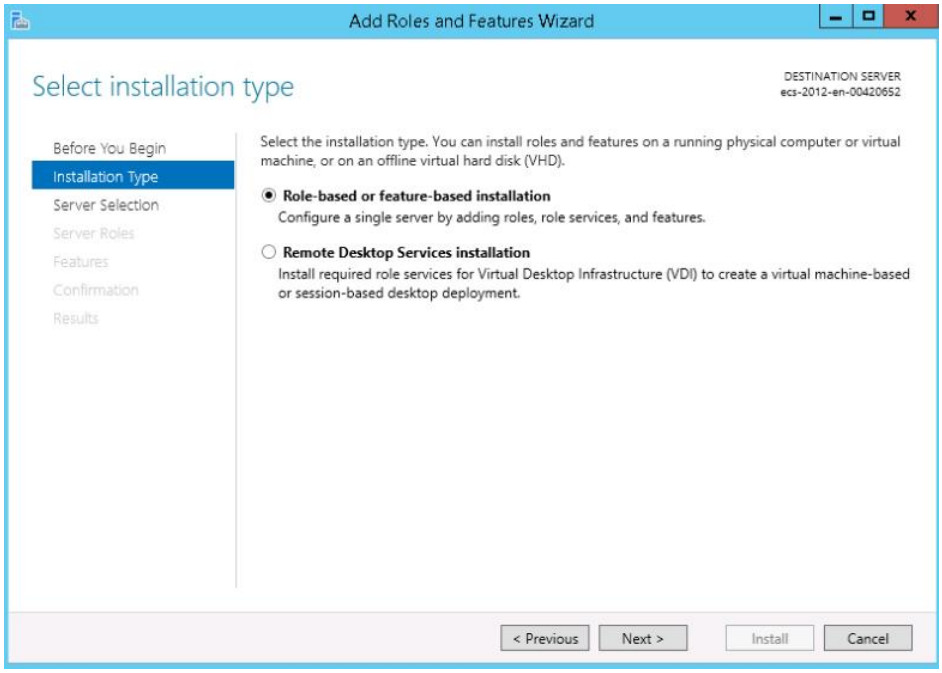
   Figure 4-14 Add roles and features



3. Retain default settings and click **Next**. On the displayed installation page, select **Role-based or feature-based installation** and click **Next**.

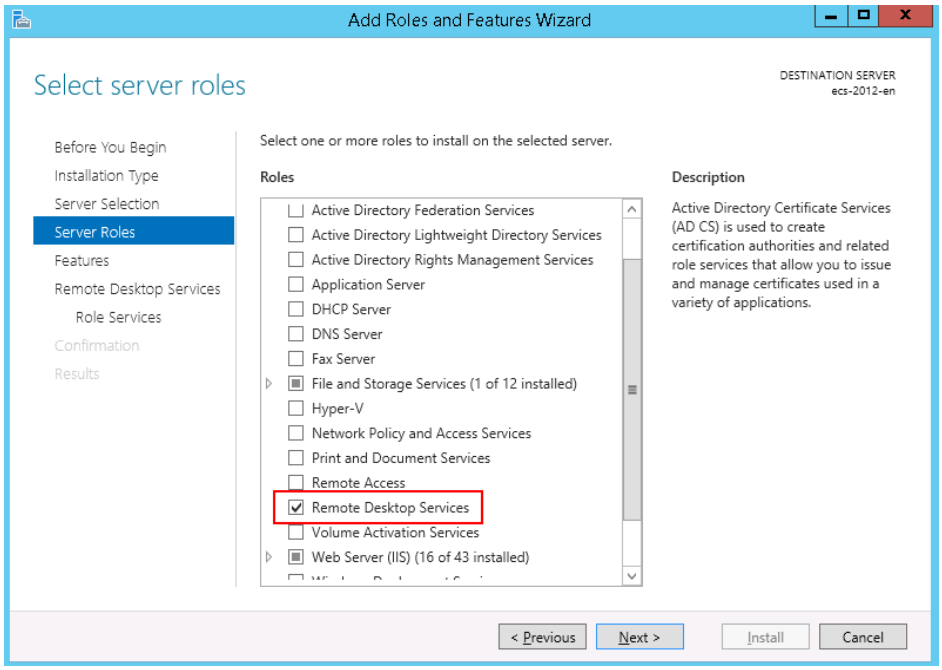
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-15 Selecting an installation type



4. Choose **Server Selection**, select **Select a server from the server pool**, and click **Next**.
5. Choose **Server Roles**, select **Remote Desktop Services**, and click **Next**.

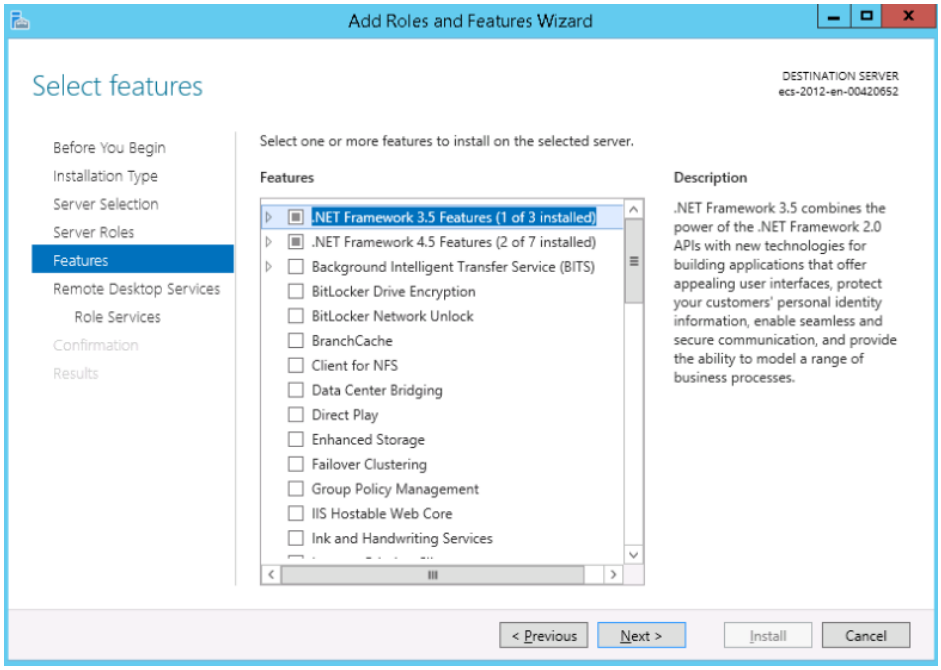
Figure 4-16 Selecting server roles



6. On the **Features** page, retain default settings and click **Next** twice.

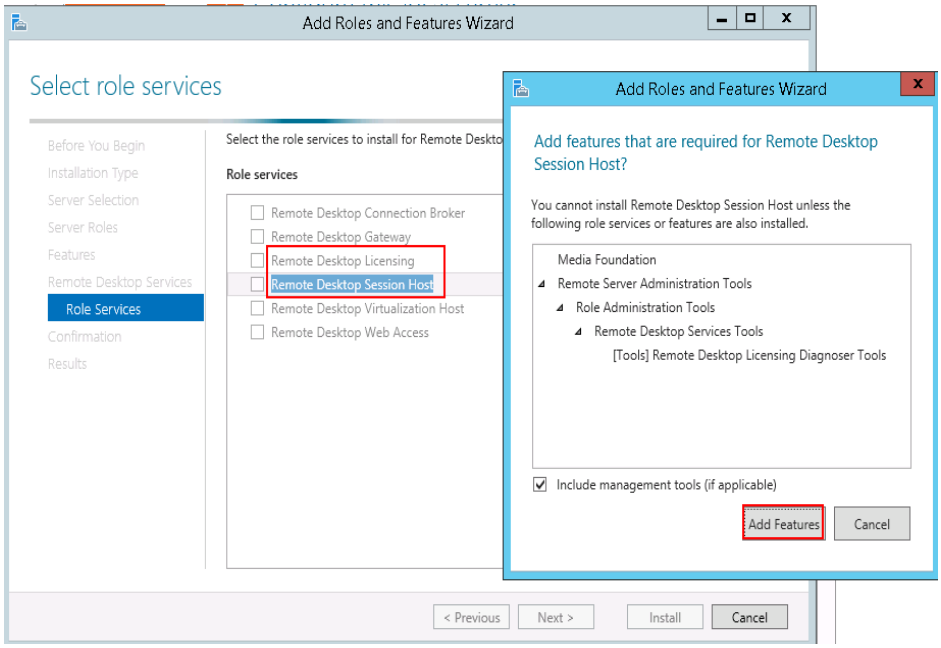
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-17 Features



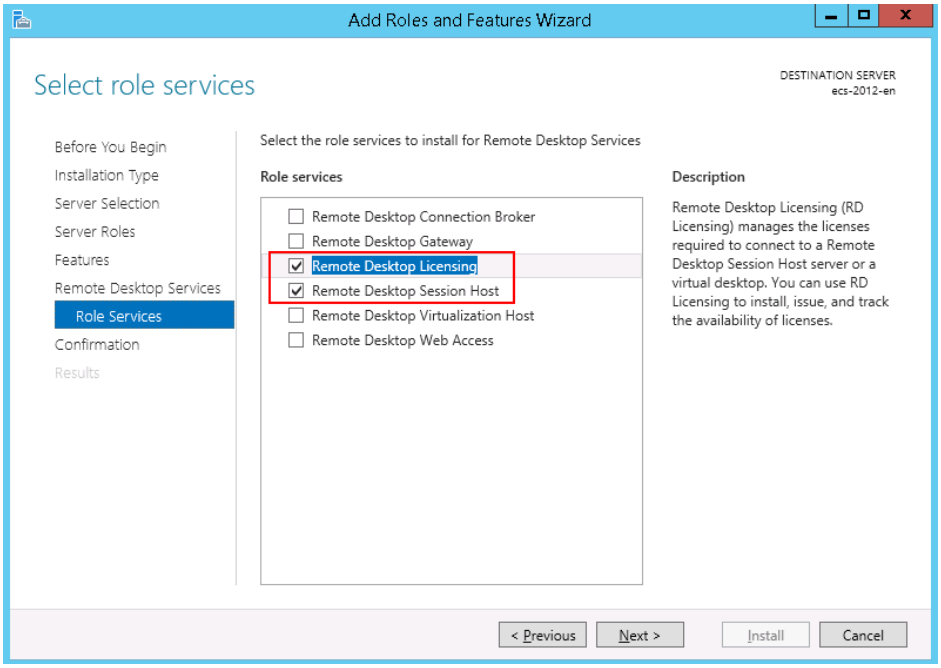
7. On the **Role Services** page, select **Remote Desktop Session Host** and **Remote Desktop Licensing**. In the displayed dialog box, click **Add Features** and then **Next**.

Figure 4-18 Adding features required by the remote desktop session host



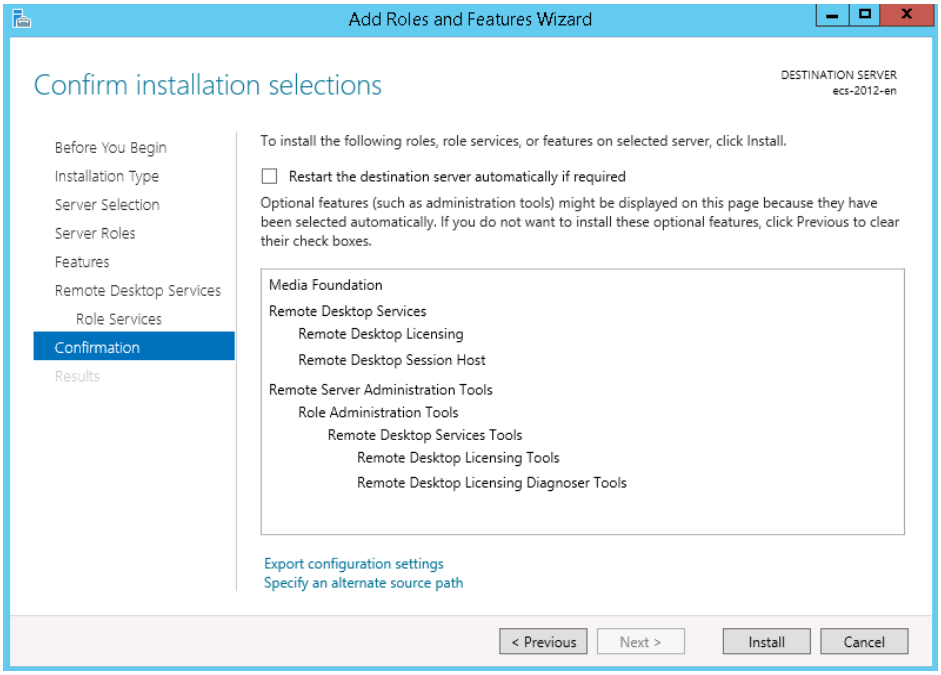
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-19 Selecting Remote Desktop Licensing



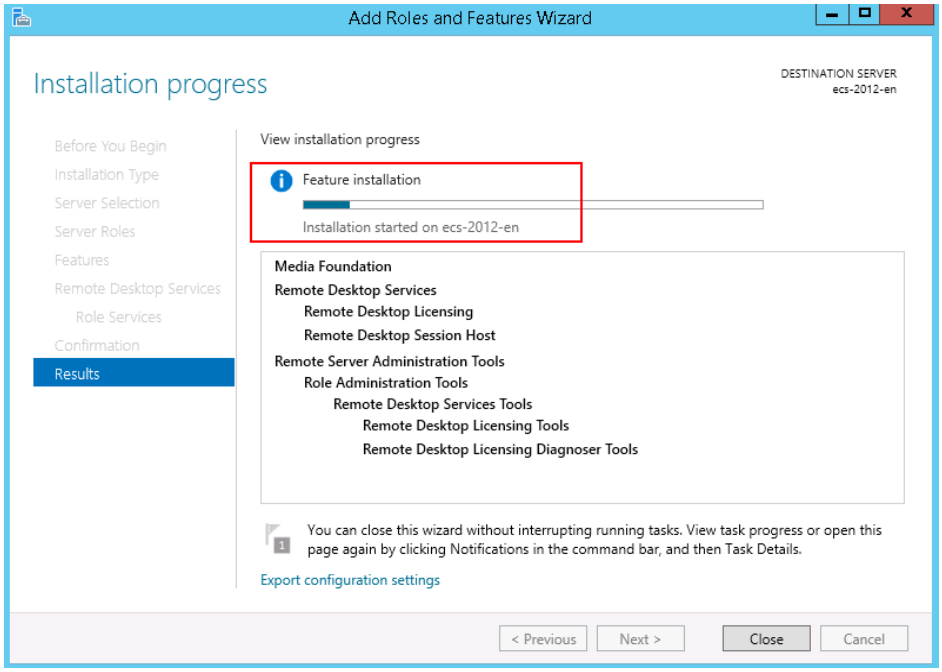
8. Confirm installation selections and click **Install**.

Figure 4-20 Confirming installation selections



9. After the installation is complete, restart the destination server as prompted and click **Close**.

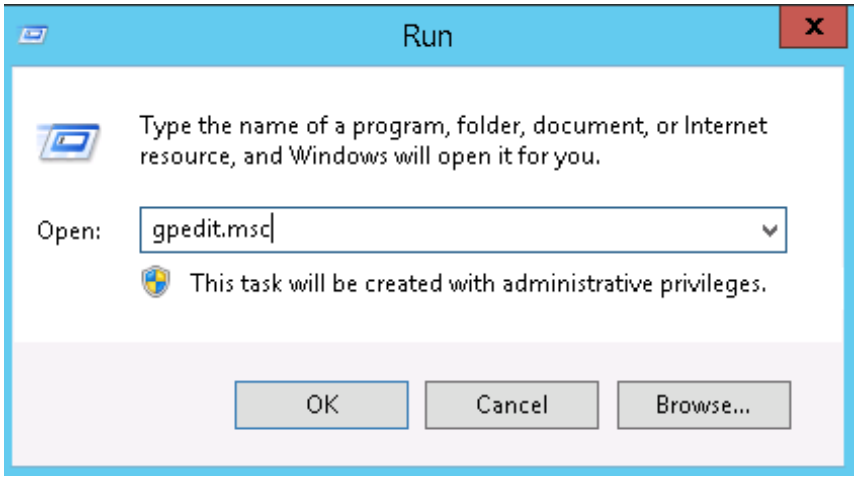
Figure 4-21 Installation progress



Enabling Multi-User Logins

1. In the **Run** dialog box, enter **gpedit.msc** and click **OK** to start Local Group Policy Editor.

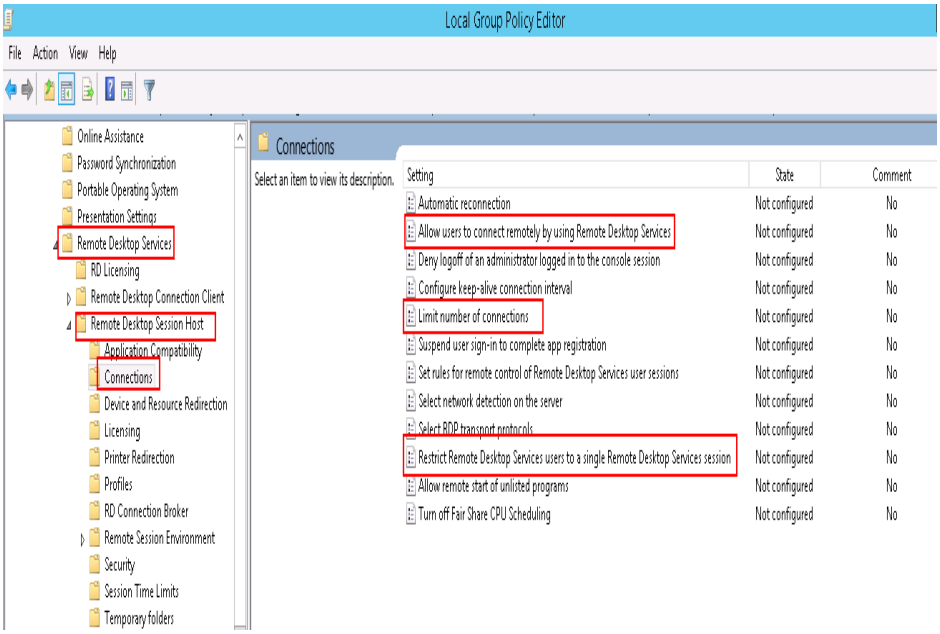
Figure 4-22 gpedit.msc



2. Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**. Configure **Allow user to connect remotely by using Remote Desktop Services**, **Limit number of connections** (based on site requirements), and **Restrict Remote Desktop Services users to a single Remote Desktop Services session**.

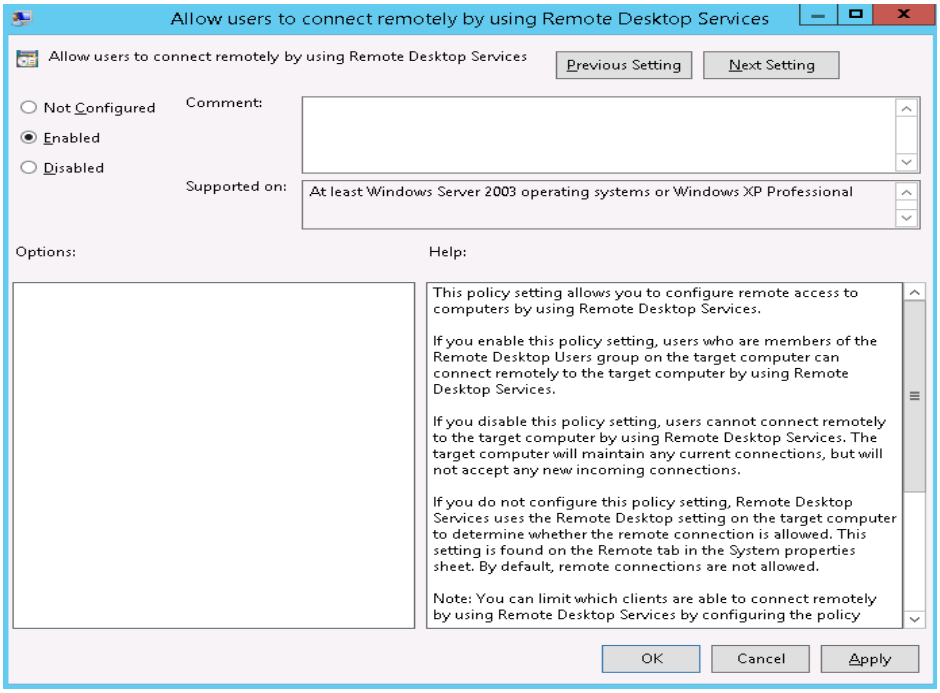
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-23 Configuring Connections



3. Right-click **Allow users to connect remotely by using Remote Desktop Services** and choose **Edit**. Then, set the status to **Enabled**.

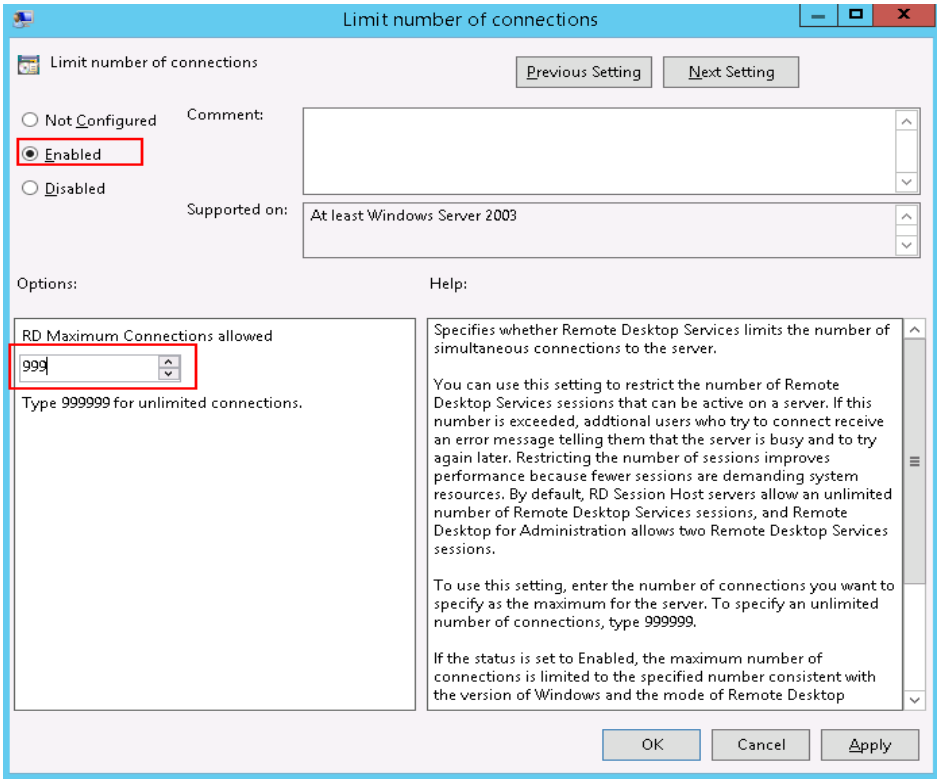
Figure 4-24 Allowing users to connect remotely by using Remote Desktop Services



4. Set **Limit number of connections** to **Enabled** and set the number based on site requirements.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-25 Setting limit number of connections



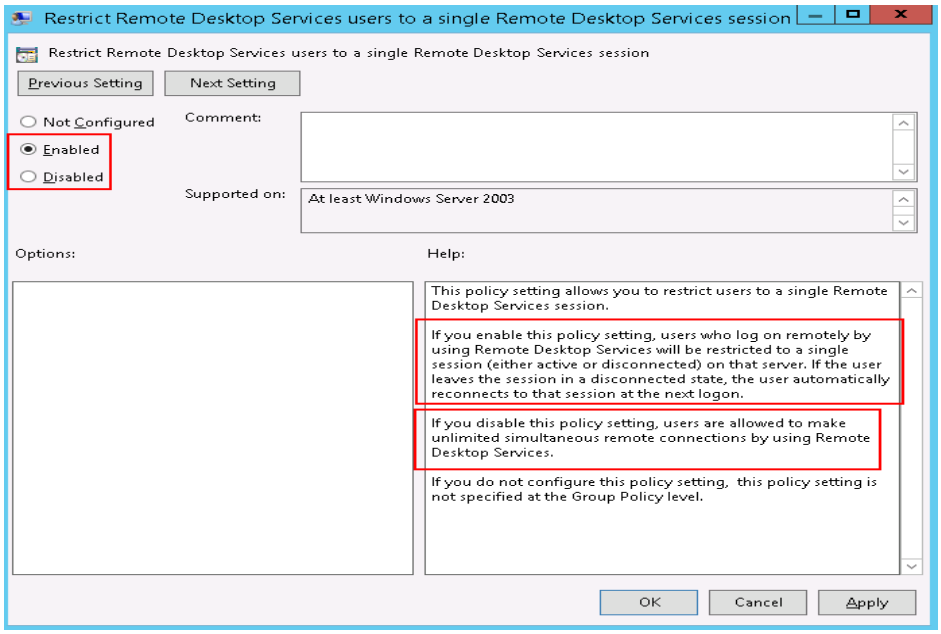
5. Set **Restrict Remote Desktop Services users to a single Remote Desktop Services session** to **Enabled** or **Disabled** as required. In this example, **Enabled** is selected.
   - **Enabled**: allows concurrent logins by multiple users, but does not allow multiple logins using one account.

     For example, users A, B, and C can concurrently log in to an HECS using account A, B, and C, respectively. However, users A, B, and C cannot use the same account to log in to the HECS.
   - **Disabled**: allows multiple users to concurrently log in to an HECS using one account.

     For example, users A, B, and C can use the same account to concurrently log in to an HECS.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-26 Restricting Remote Desktop Services users to a single Remote Desktop Services session



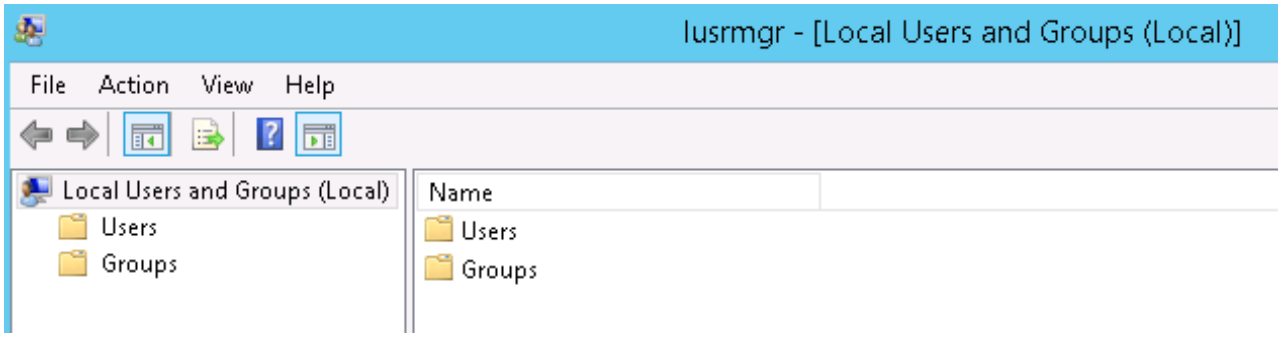
6. Run **cmd** and then **gpupdate /force** to forcibly start Local Group Policy Editor and restart the HECS.

Adding a New User to the Remote Desktop Users Group

After enabling multi-user login, add new users to the remote desktop users group. This section describes how to create a user and add the user to remote desktop users group.

1. Open the **Run** dialog box, enter **lusrmgr.msc**, and click **OK** to open **Local Users and Groups**.

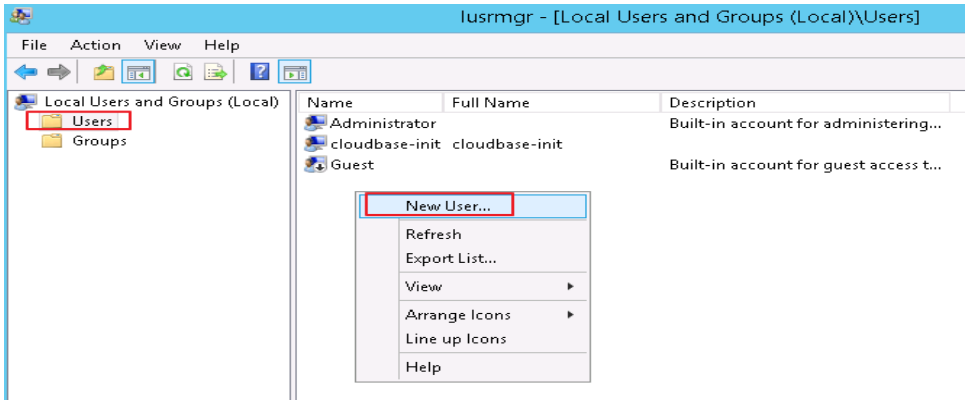
Figure 4-27 Local Users and Groups



2. Select **Users**, right-click the blank area, and choose **New User** from the shortcut menu.

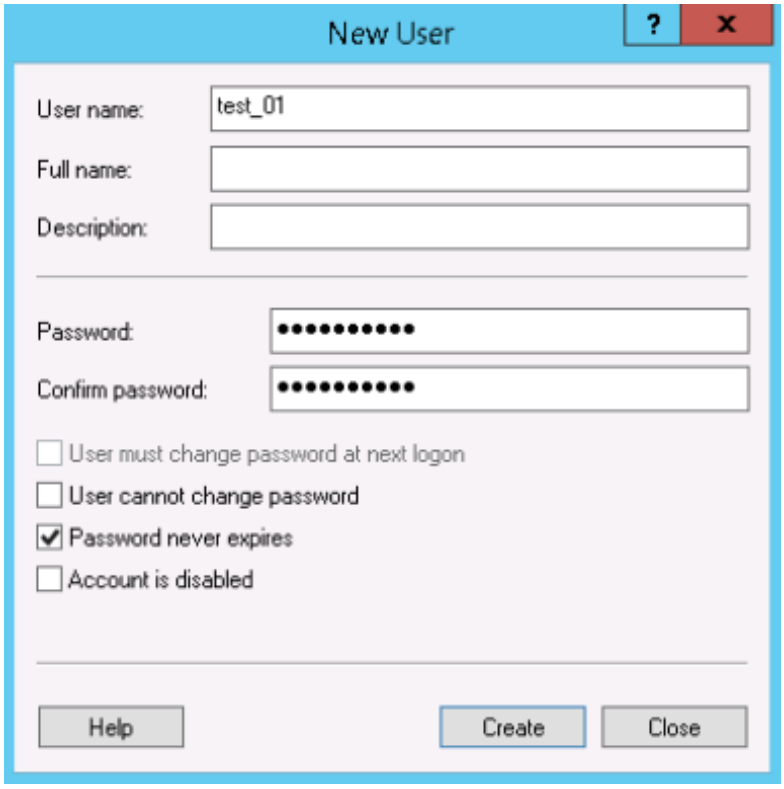
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-28 Adding a new user



3. Set user information and click **Create**.

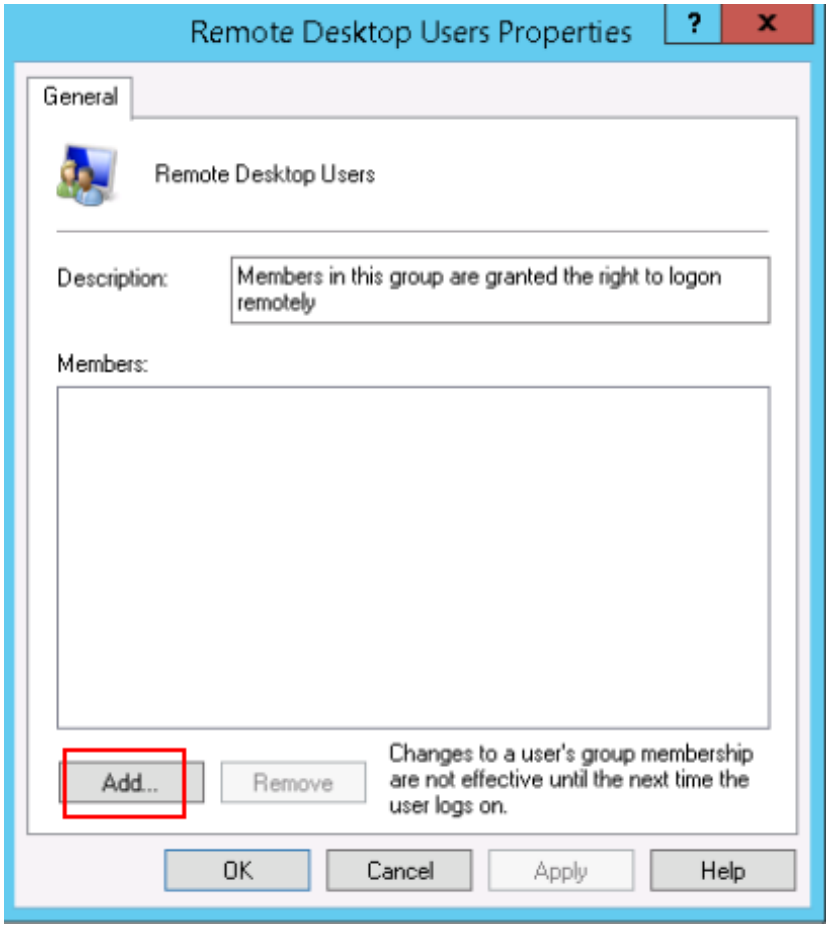
Figure 4-29 Setting user information



4. Select **Groups**, double-click **Remote Desktop Users**, and click **Add**.

 Copyright © Huawei Technologies Co., Ltd.

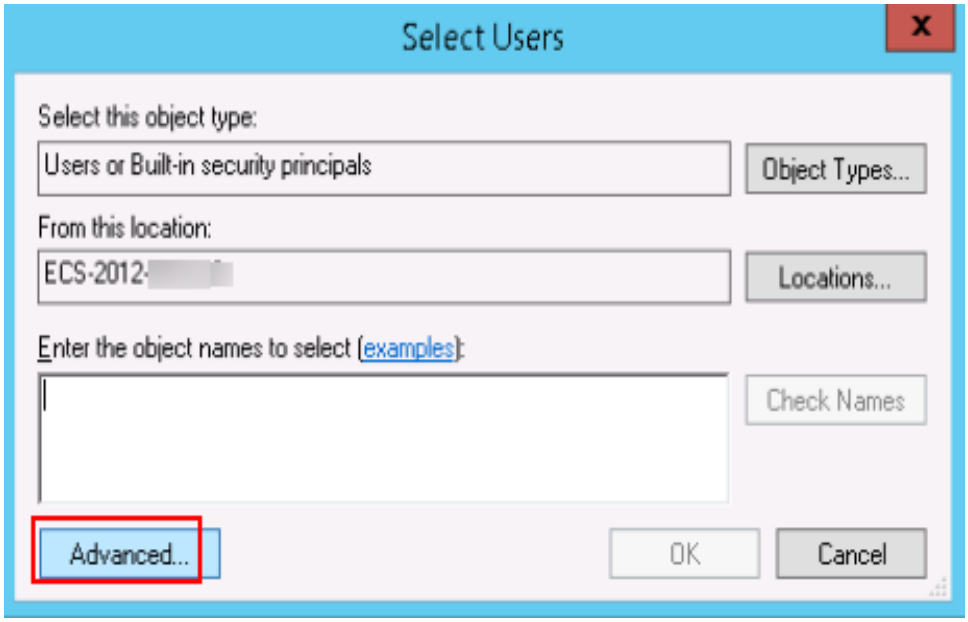
Figure 4-30 Remote Desktop Users Properties



5. In the **Select Users** dialog box, click **Advanced**.

 Copyright © Huawei Technologies Co., Ltd.

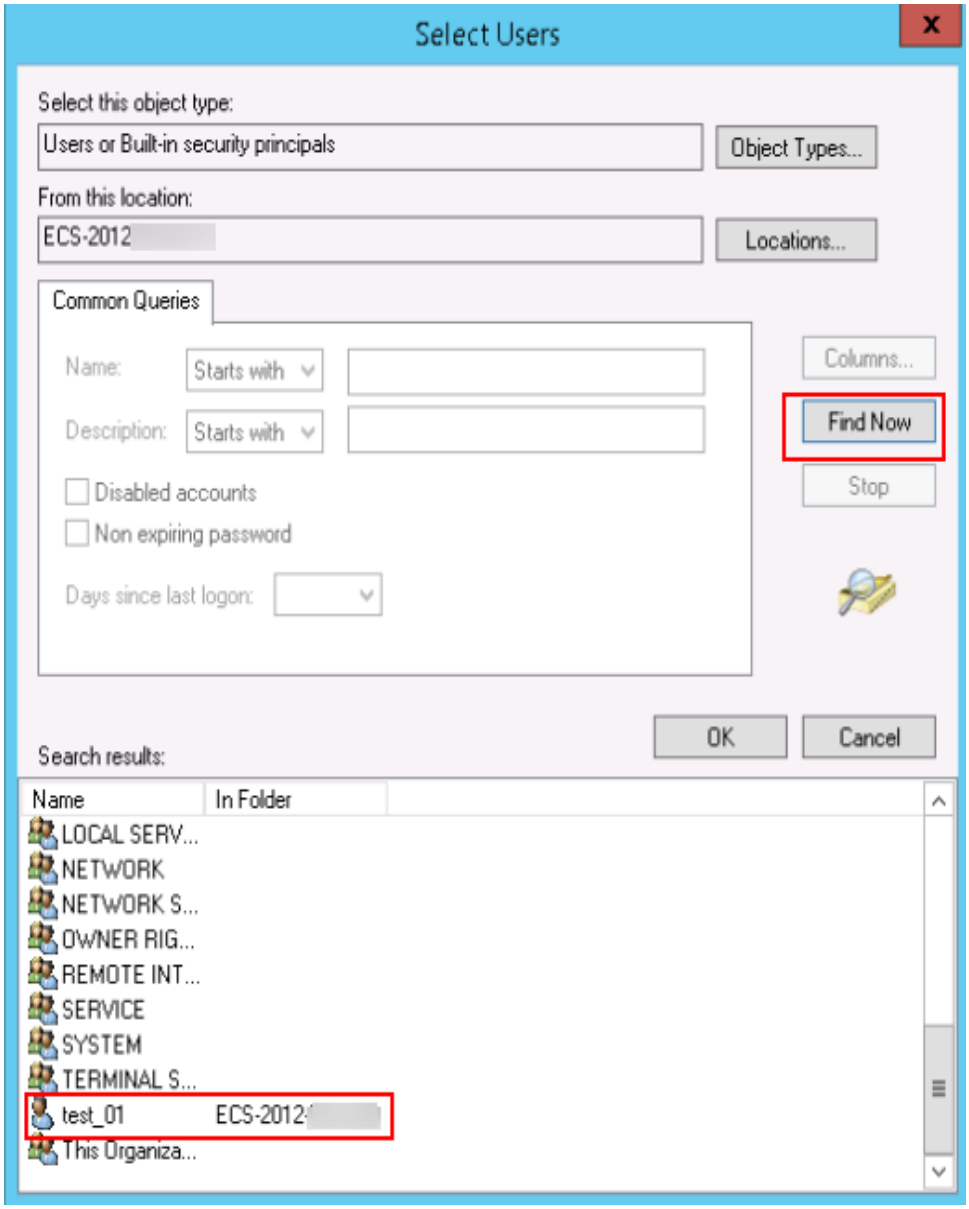
Figure 4-31 Selecting users (Advanced)



6. Click **Find Now**, select the user for remote login in the search results, and click **OK**.

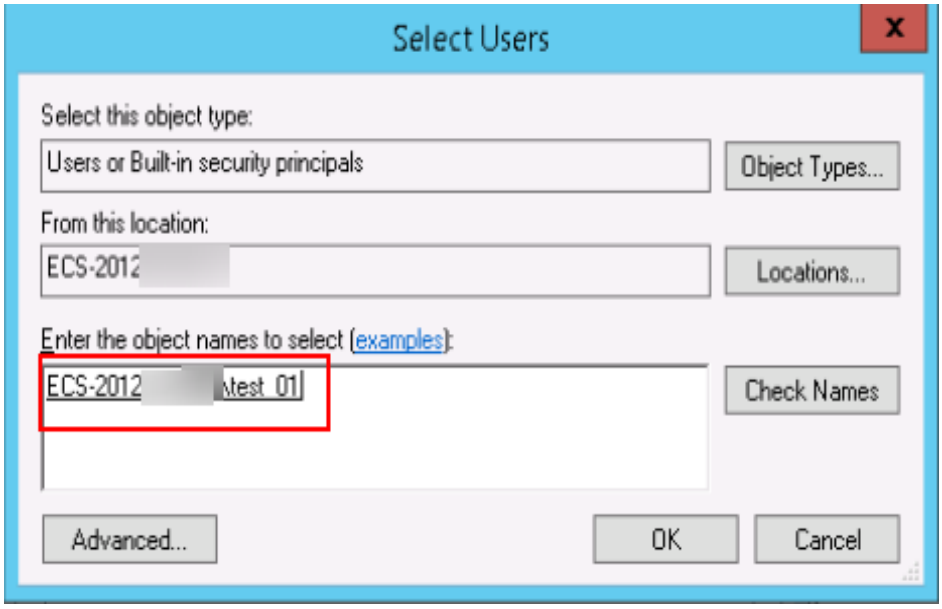
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-32 Selecting users (Find Now)



 Copyright © Huawei Technologies Co., Ltd.

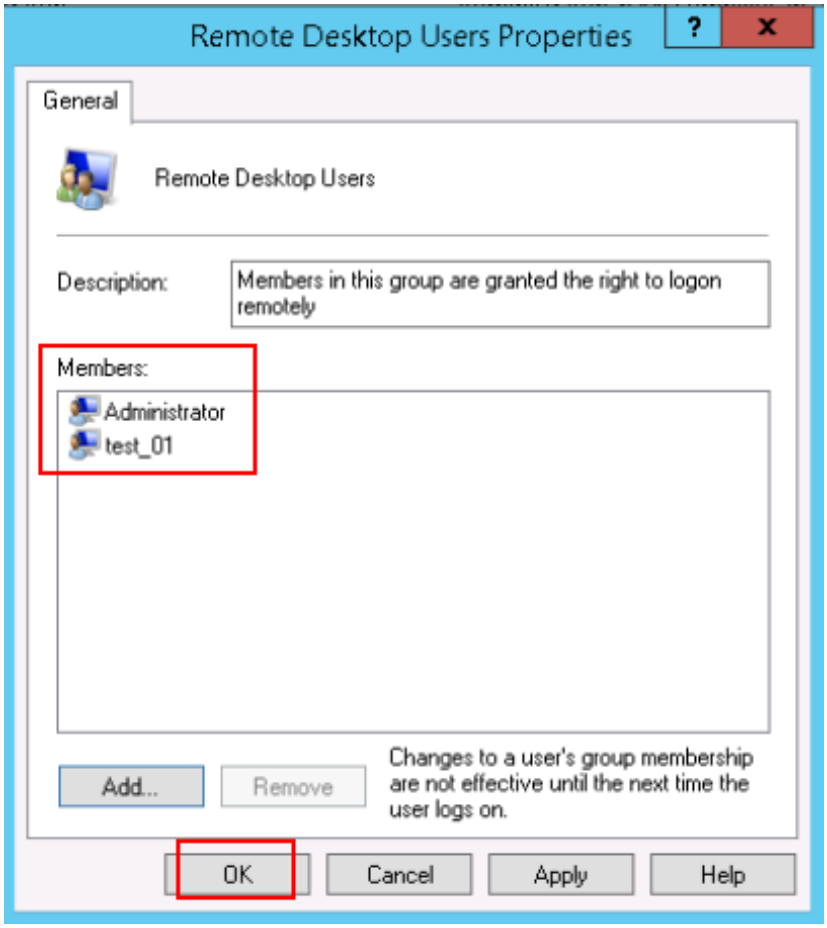
Figure 4-33 Adding a user



7. Click **OK** to add the user to the Remote Desktop Users group.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-34 Confirming user information



Follow-up Operations

For instructions on how to activate Remote Desktop Licensing, see 4.7 Applying for a License for Authenticating Multi-User Sessions and Activating the HECS.

4.7 Applying for a License for Authenticating Multi-User Sessions and Activating the HECS

Scenarios

This section describes how to configure remote desktop services and activate the HECS.

The HECS running Windows Server 2012 is used as an example.

Procedure

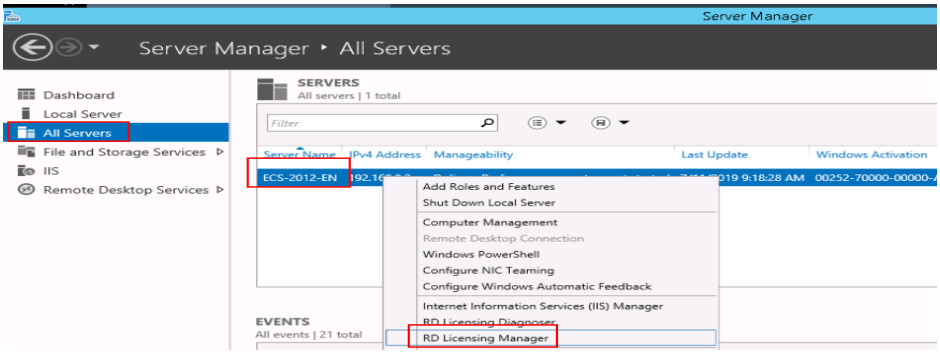
1. Applying for a License for Authenticating Multi-User Sessions
2. Activating the HECS
3. Configuring the Licensing Server for Remote Desktop Session Host

 Copyright © Huawei Technologies Co., Ltd.

Applying for a License for Authenticating Multi-User Sessions

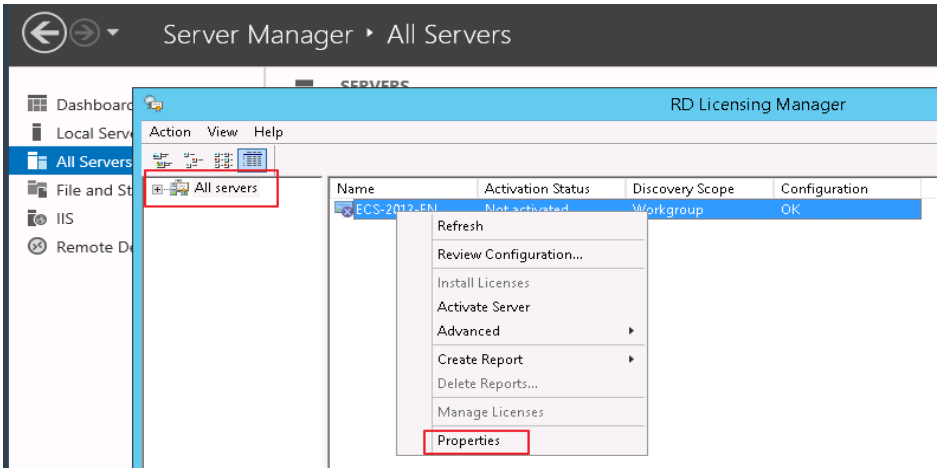
1. Log in to the Windows HECS.
2. On the OS, click  to open **Server Manager**.
3. On the **Server Manager** page, click **All Servers**, right-click the server name, and choose **RD Licensing Manager** from the shortcut menu.

   Figure 4-35 Selecting RD Licensing Manager

4. Right-click the unactivated server and choose **Properties** from the shortcut menu.

   Figure 4-36 Selecting properties of the unactivated server

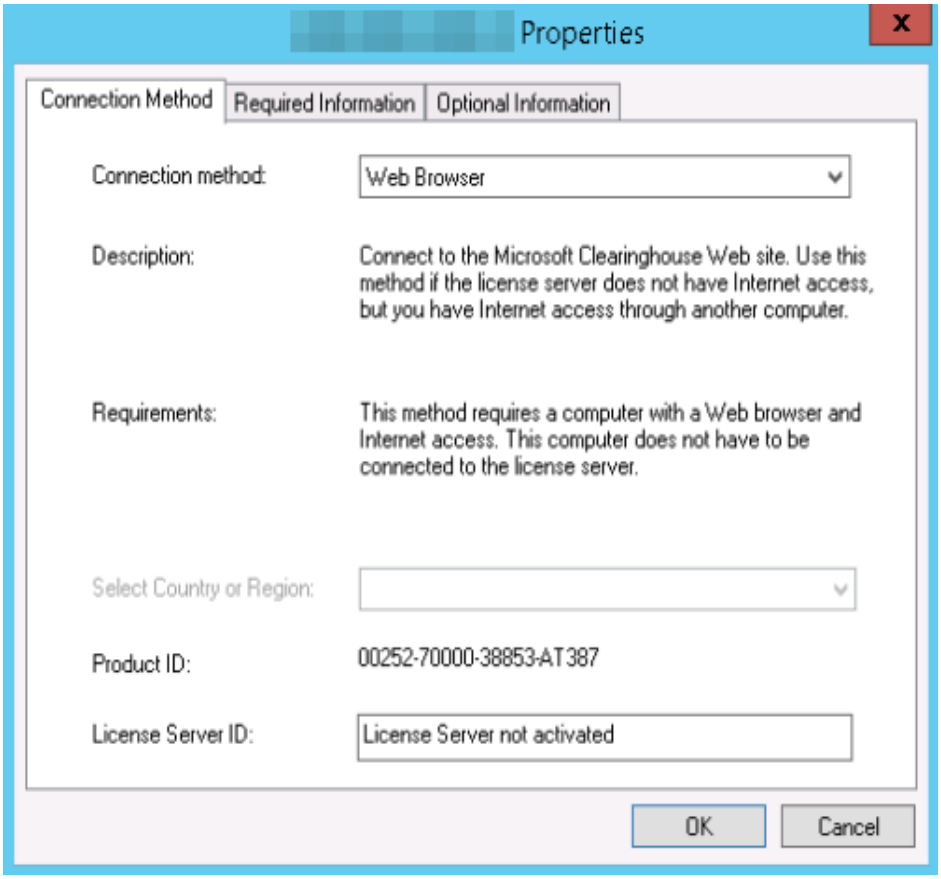
5. In the **Properties** dialog box, set **Connection Method** to **Web Browser**. Record the product ID which will be required for obtaining a server license.

NOTICE

If the destination server is not displayed in **RD Licensing Manager**, choose **Action** > **Connect**, and enter the server IP address.

 Copyright © Huawei Technologies Co., Ltd.

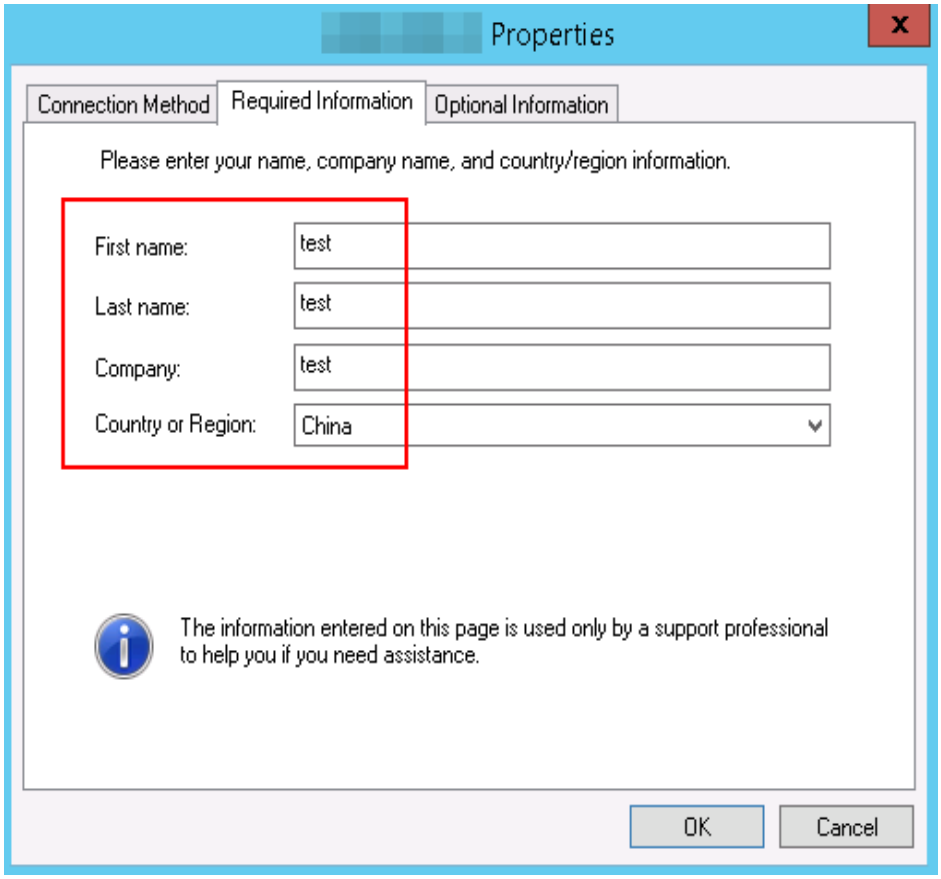
Figure 4-37 Web browser for connection



6. Set parameters and click **OK**.

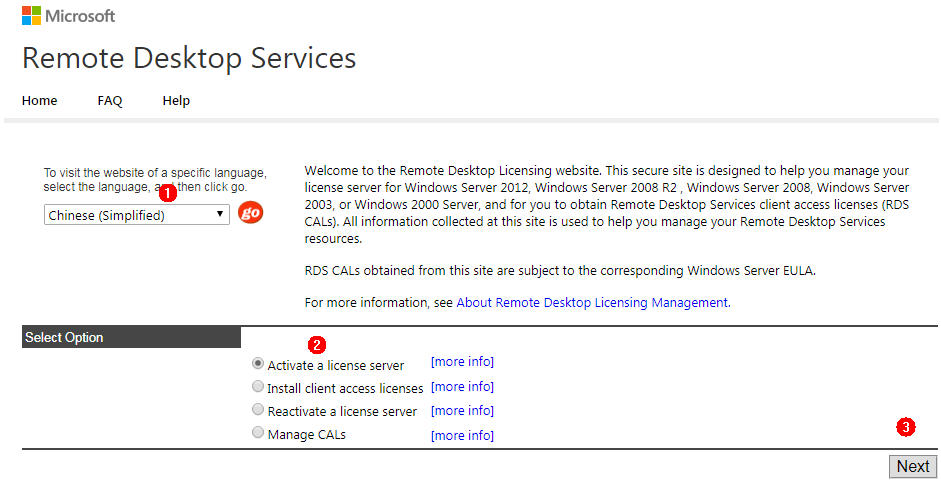
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-38 Setting parameters



7. Access https://activate.microsoft.com using Internet Explorer.
   Select **Activate a license server** and click **Next**.

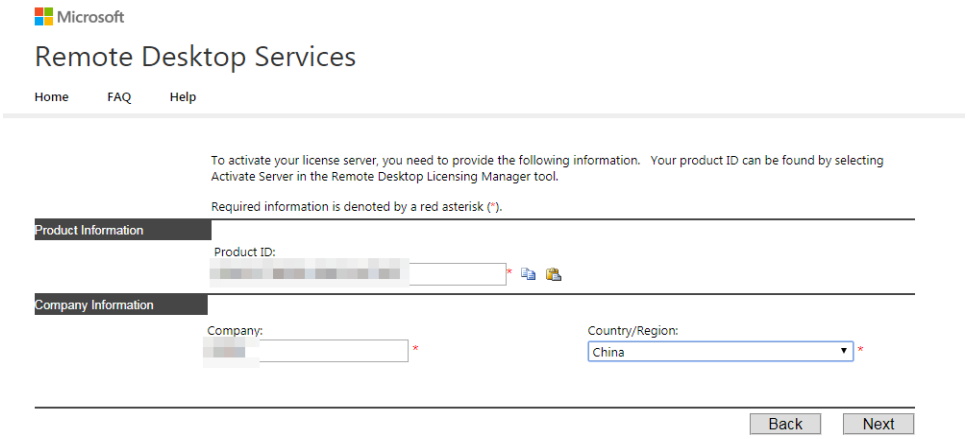
Figure 4-39 Activating the license server



8. Set parameters and click **Next**. Confirm the product information and click **Next**.

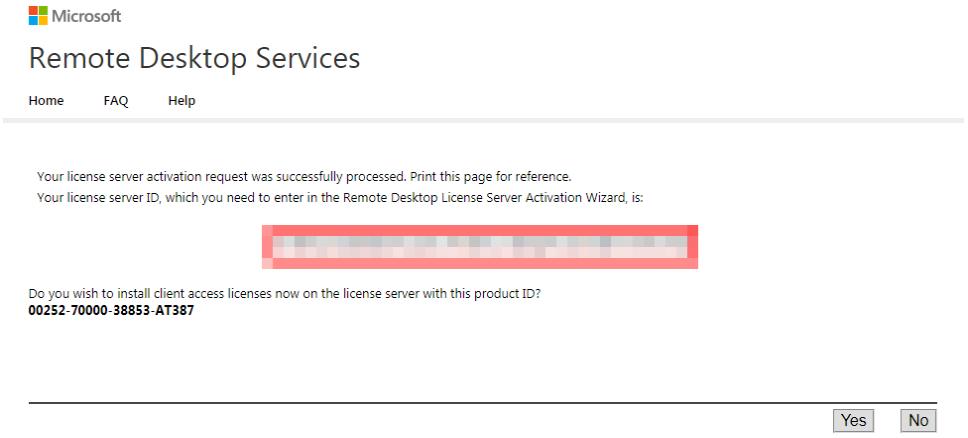
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-40 Configuring the server



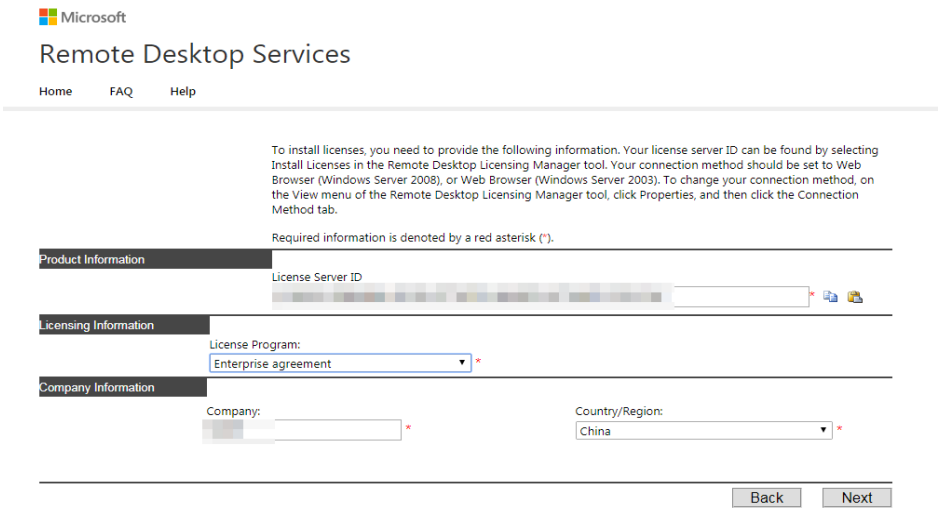
9. Record the license server ID and click **Yes**.

Figure 4-41 Obtaining the license server ID



10. If the license server ID is not available, set **License Program** to **Enterprise agreement** and click **Next**.

Figure 4-42 Enterprise agreement

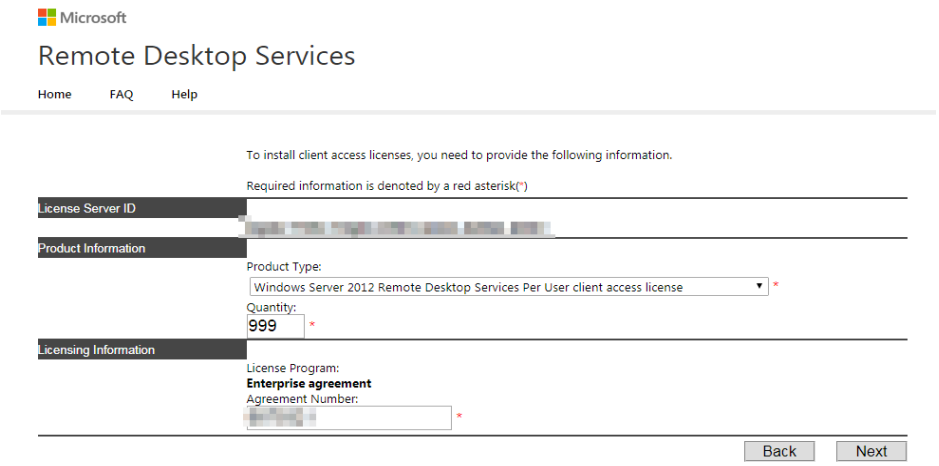


11. Set parameters.
    - **Product Type**: specifies the license server type, for example, **Windows Server 2012 Remote Desktop Services Per User client access license**.
    - **Quantity**: the maximum number of users allowed for remote desktop connections, for example, **999**.
    - **Agreement Number**: a 7-digit license registration number purchased at the official Microsoft website.

NOTE

HUAWEI CLOUD does not provide licenses for remote desktop connections. Purchase this license on the official Microsoft website.

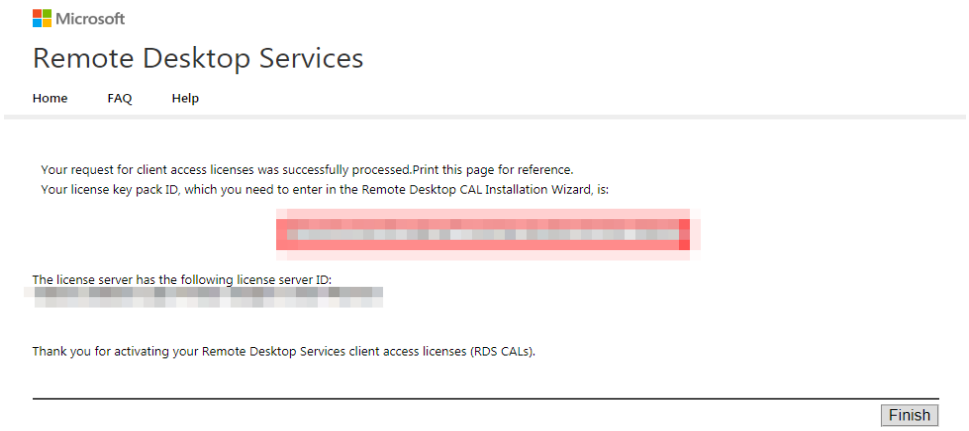
Figure 4-43 Setting license server information



12. Record the license server ID and license key pack ID and click **Finish**.

 Copyright © Huawei Technologies Co., Ltd.

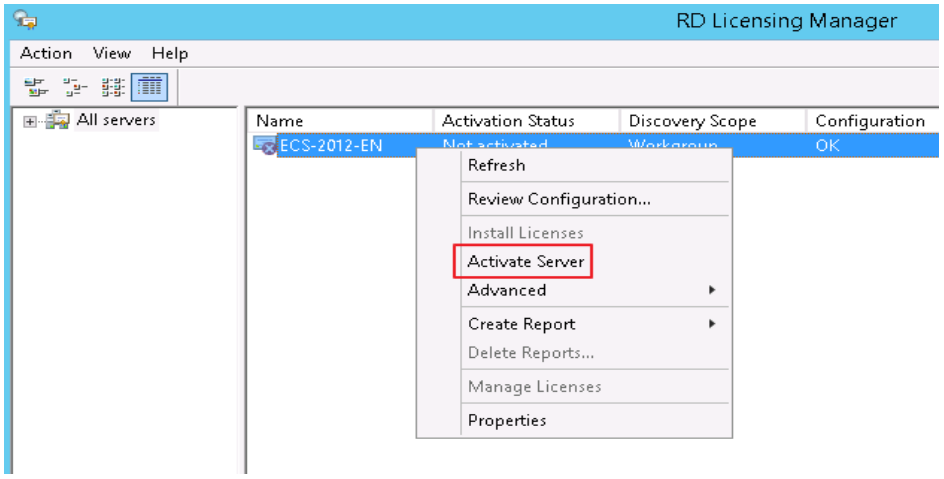
Figure 4-44 Obtaining a license key pack ID



Activating the HECS

1. Log in to the HECS. Open **RD Licensing Manager**, right-click the HECS, and choose **Activate Server**.

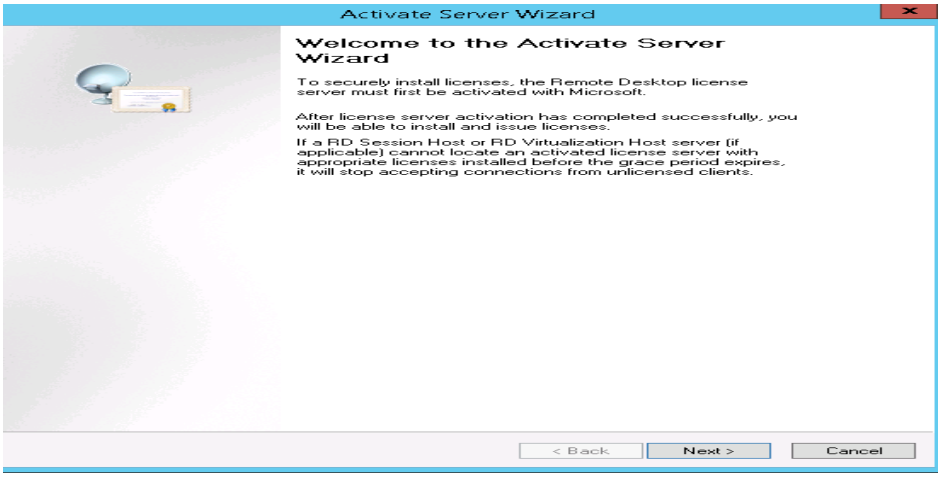
Figure 4-45 Activating the HECS



2. In **Activate Server Wizard**, click **Next**.

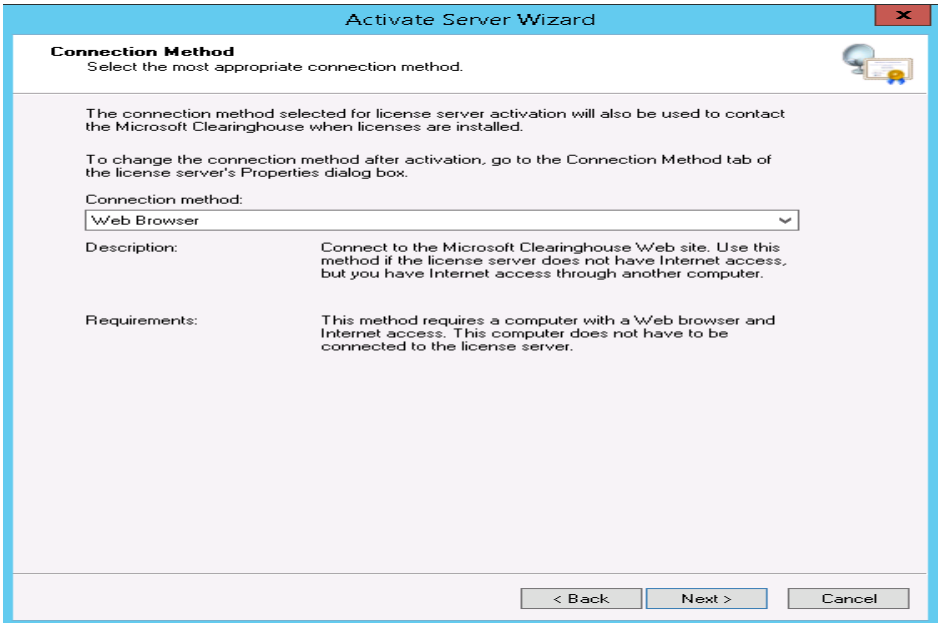
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-46 Activate Server Wizard



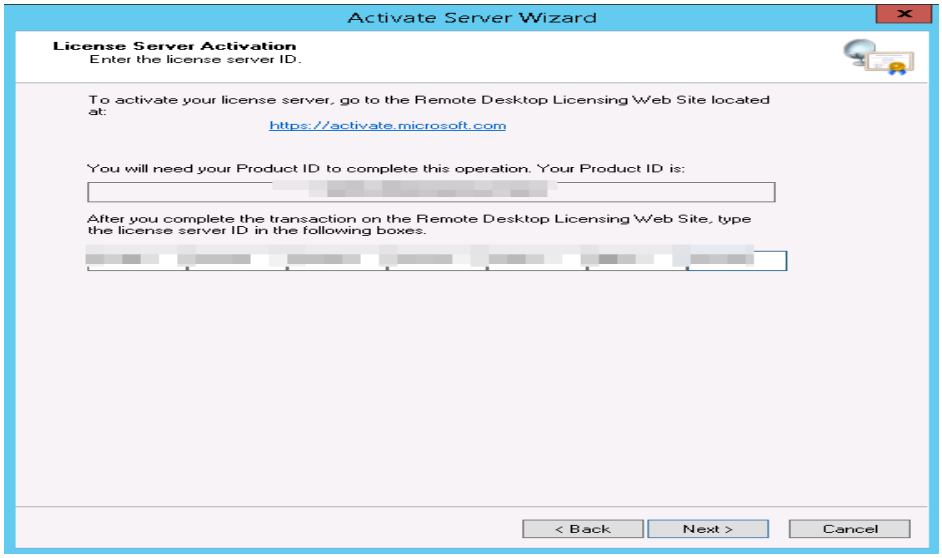
3. Set **Connection method** to **Web Browser** and click **Next**.

Figure 4-47 Web browser for connection



4. Enter the license server ID and click **Next**.
   The license server ID is the ID obtained in step 9.

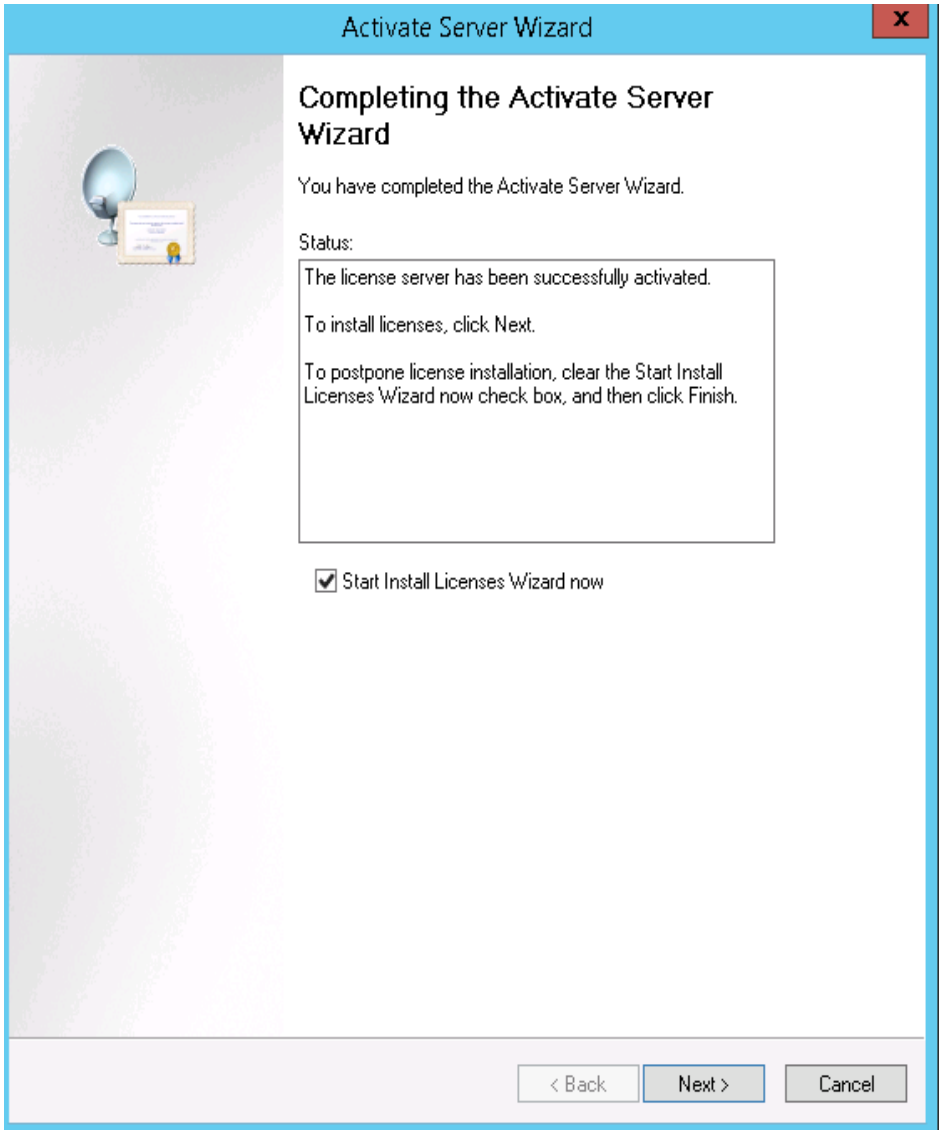
Figure 4-48 Entering the license server ID



5. Select **Start Install Licenses Wizard now** and click **Next**.

 Copyright © Huawei Technologies Co., Ltd.

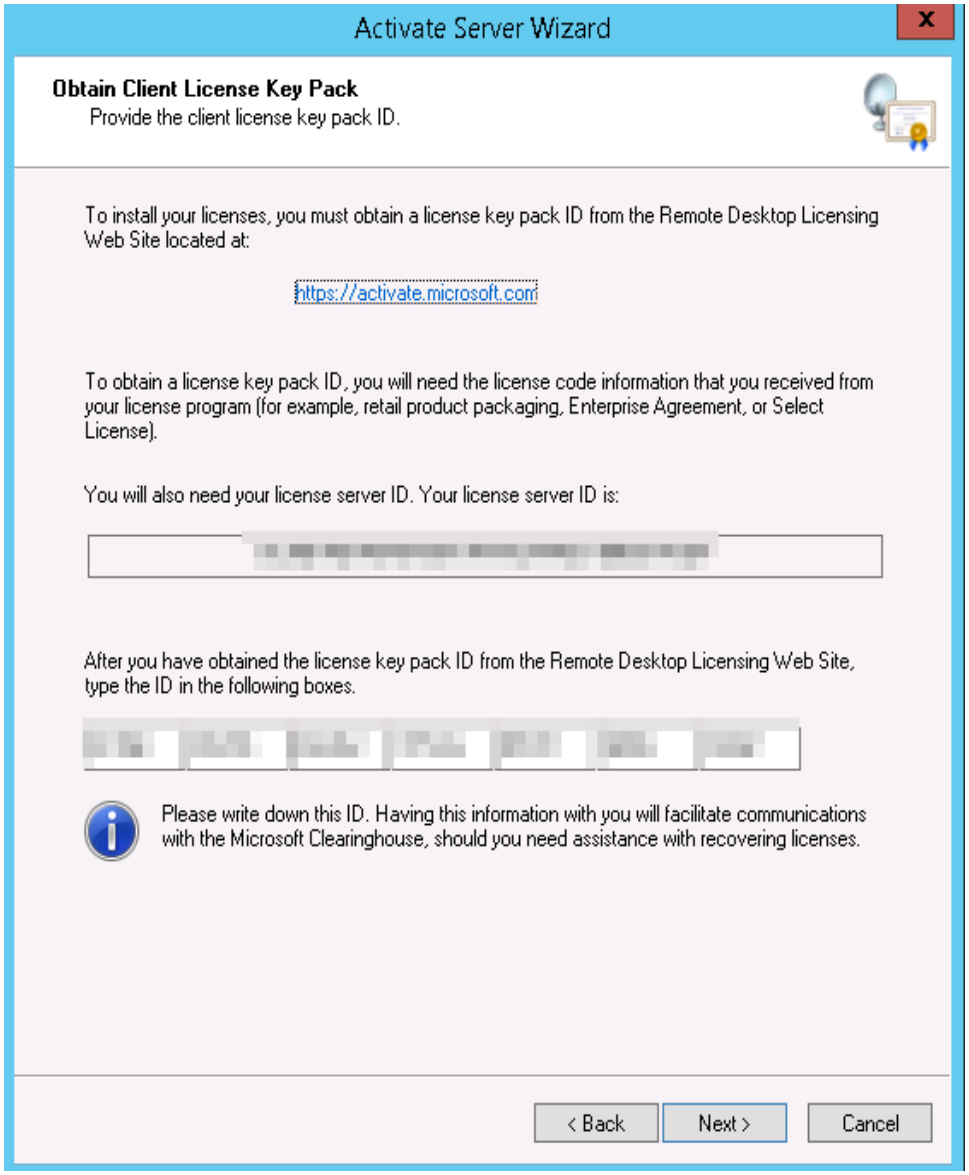
Figure 4-49 Starting license installation wizard



6. Enter the license key pack ID and click **Next**.
   The key pack ID is obtained in step 12.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-50 Entering the key pack ID



7. Click **Finish**.

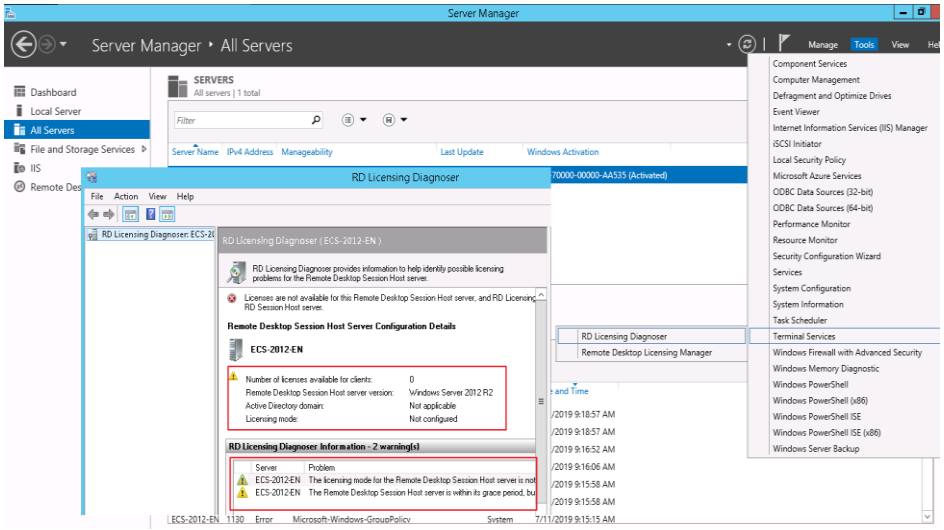
Configuring the Licensing Server for Remote Desktop Session Host

1. Log in to the Windows HECS.
2. On the OS, click  to open **Server Manager**. Click **Tools** > **Terminal Services** > **RD Licensing Diagnoser** and check the HECS licensing status.

   As shown in Figure 4-51, the system displays a message indicating that the licensing mode for the Remote Desktop Session Host Server is not configured.

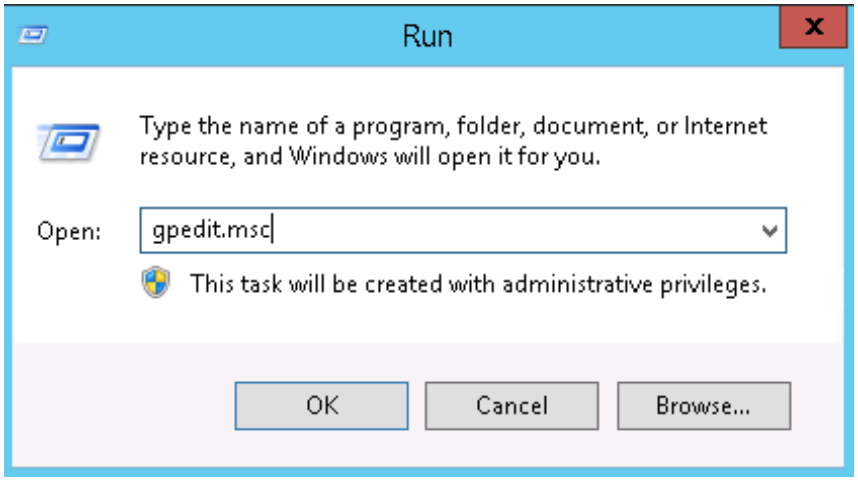
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-51 Checking the HECS licensing status



3. In the **Run** dialog box, enter **gpedit.msc** and click **OK** to start Local Group Policy Editor.

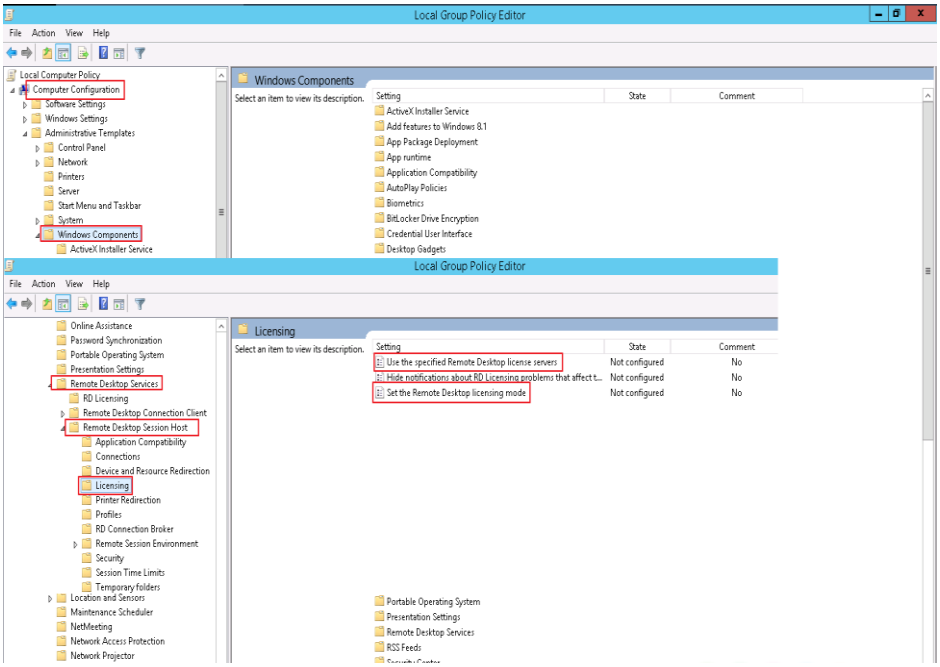
Figure 4-52 gpedit.msc



4. Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Licensing**.

 Copyright © Huawei Technologies Co., Ltd.

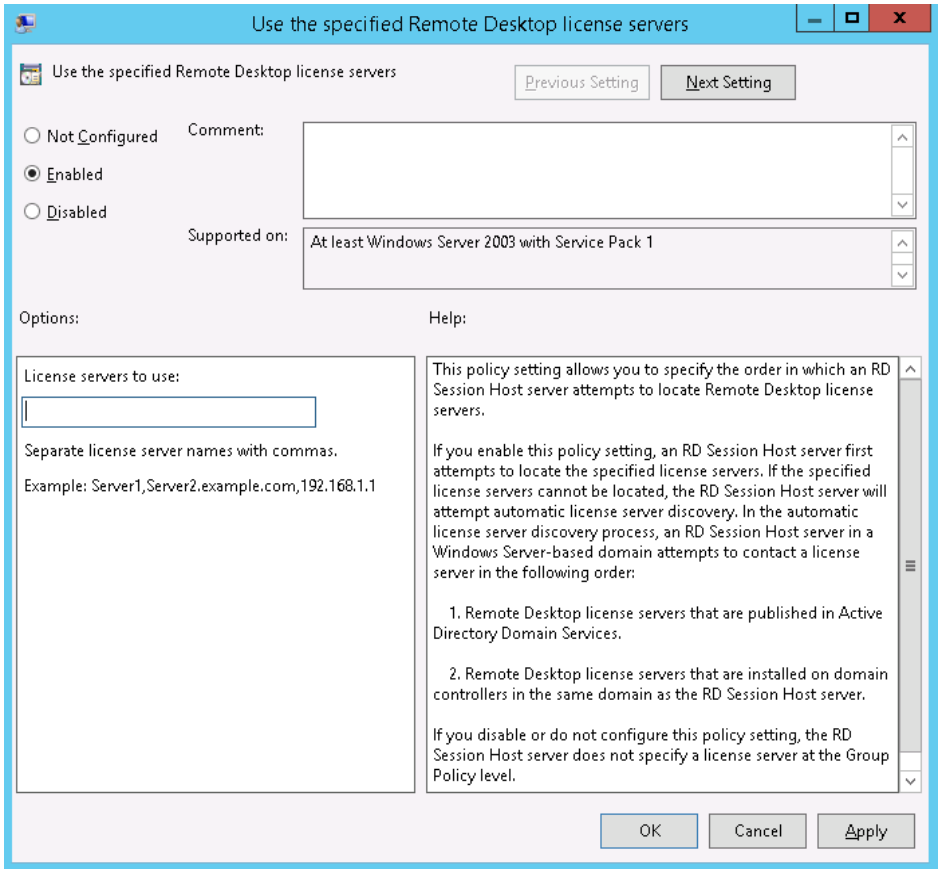
Figure 4-53 Modifying licensing items



5. Set **Use the specified Remote Desktop license servers** to **Enabled**, enter the private IP address or hostname of the HECS under **License servers to use**, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-54 Using the specified remote desktop license servers



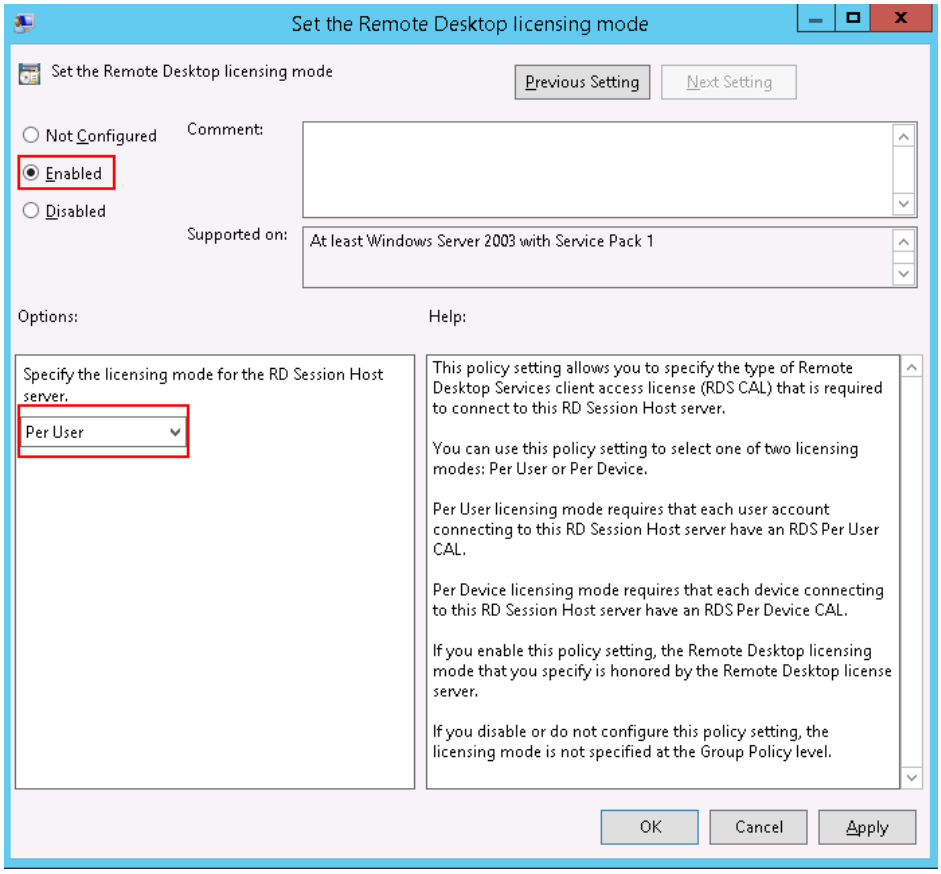
6. **Set the Remote Desktop licensing mode** to **Enabled**, and set the licensing mode to **Per User**.

NOTE

If a message is displayed indicating that there is a problem with your remote desktop license, set the licensing mode to **Per Device**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-55 Setting the remote desktop licensing mode



7. Run **cmd** and then **gpupdate /force** to forcibly start Local Group Policy Editor and restart the HECS.

5 Network Configurations

5.1 Why Can't an EIP Be Pinged?

Symptom

After you purchase an HECS with an EIP bound, you fail to ping the EIP of the HECS, or the HECS cannot ping the Internet.

Troubleshooting

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one in the list.

Figure 5-1 Method of locating the failure to ping an EIP

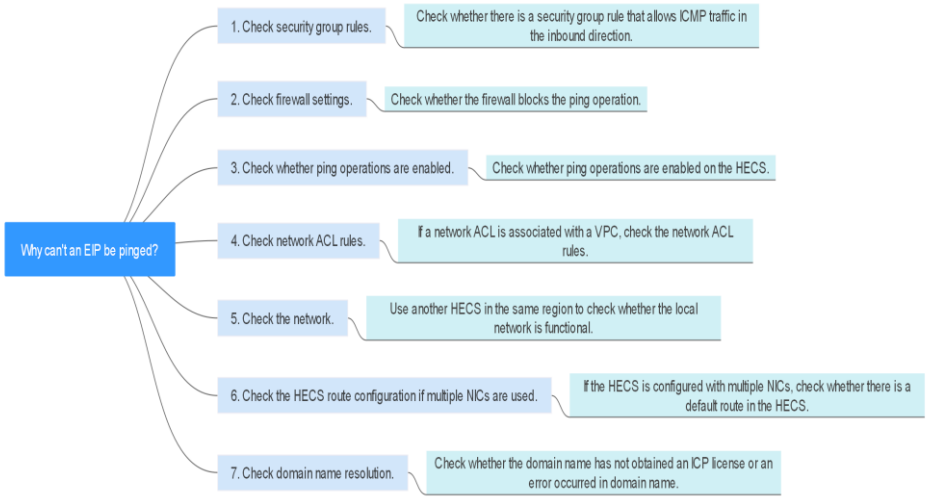


Table 5-1 Method of locating the failure to ping an EIP

Possible Cause	Handling Measure
No security group rule	Add a security group rule to allow ICMP traffic. For details, see

 Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Handling Measure
allows ICMP traffic.	Checking Security Group Rules.
Ping operations are prohibited on the firewall.	Allow ping operations on the firewall. For details, see Checking Firewall Settings.
Ping operations are prohibited on the HECS.	Allow ping operations on the HECS. For details, see Checking Whether Ping Operations Are Prohibited on the HECS.
The associated network ACL denies ICMP traffic.	Check whether the network ACL associated with the VPC denies ICMP traffic. For details, see Checking Network ACL Rules.
A network exception occurred.	Use another HECS in the same region to check whether the local network is functional. For details, see Checking the Network.
Routes are incorrectly configured if multiple NICs are used.	If the network is inaccessible due to an extension NIC, the fault is generally caused by incorrect route configurations. To resolve this issue, see Checking the HECS Route Configuration If Multiple NICs Are Used.
The domain name is not ICP licensed or cannot be resolved.	If the domain name cannot be pinged, the domain name is not ICP licensed or cannot be resolved. To resolve this issue, see Checking Domain Name Resolution If the Domain Name Cannot Be Pinged.

Checking Security Group Rules

The ping operations use the ICMP protocol. Check whether the security group associated with the HECS allows ICMP traffic in the inbound direction.

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Computing**, click **Hyper ECS**.
4. On the **Hyper Elastic Cloud Server** page, click the name of the HECS with security group rules to be modified.

   The HECS details page is displayed.
5. Click the **Security Groups** tab, expand the information of the security group, and view security group rules.
6. Click the security group ID.

   The system automatically switches to the security group console.
7. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-2 Add Inbound Rule

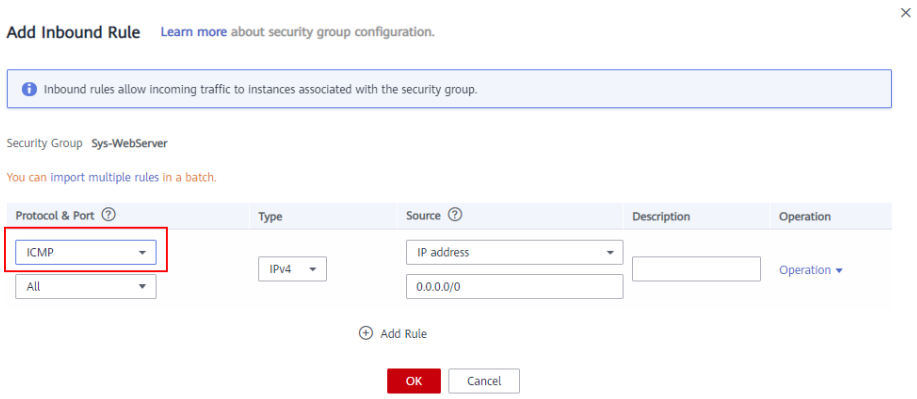


Table 5-2 Security group rules

Direction	Type	Protocol/Port Range	Source
Inbound	IPv4	ICMP/Any	0.0.0.0/0 0.0.0.0/0 indicates all IP addresses.

8. Click **OK** to complete the security rule configuration.

Checking Firewall Settings

If a firewall is enabled on the HECS, check whether the firewall blocks the ping operation.

Linux

1. Run the following command to check the firewall status, taking CentOS 7 as an example:

   firewall-cmd --state

   If **running** is displayed in the command output, the firewall has been enabled.
2. Check whether there is any ICMP rule blocking the ping operation.

   iptables -L

   If the command output shown in Figure 5-3 is displayed, there is no ICMP rule blocking the ping operation.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-3 Checking firewall rules



If the ping operation is blocked by an ICMP rule, run the following commands to modify the rule for unblocking:

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

Windows

1. Log in to the Windows HECS, click the Windows icon in the lower left corner of the desktop, and choose **Control Panel** > **Windows Firewall**.
2. Click **Turn Windows Firewall on or off**.

   View and set the firewall status.
3. If the firewall is **On**, go to 4.
4. Check the ICMP rule statuses in the firewall.
   a. In the navigation pane on the **Windows Firewall** page, click **Advanced settings**.
   b. Enable the following rules:

      Inbound Rules: **File and Printer Sharing (Echo Request - ICMPv4-In)**

      Outbound Rules: **File and Printer Sharing (Echo Request - ICMPv4-Out)**

      If IPv6 is enabled, enable the following rules:

      Inbound Rules: **File and Printer Sharing (Echo Request - ICMPv6-In)**

      Outbound Rules: **File and Printer Sharing (Echo Request - ICMPv6-Out)**

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-4 Inbound Rules

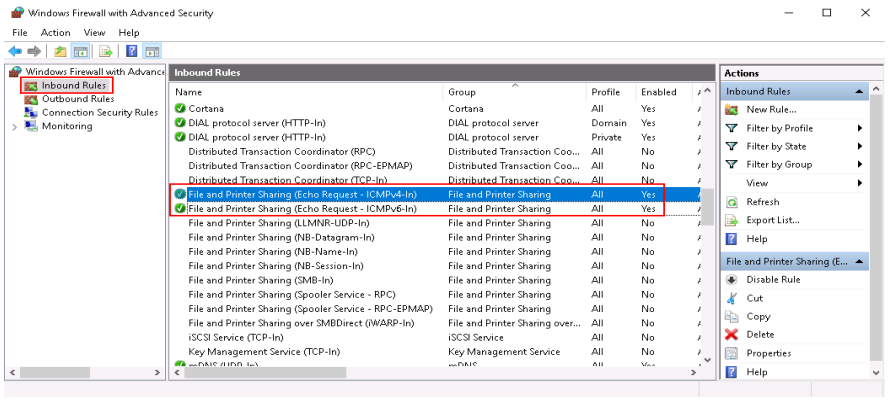
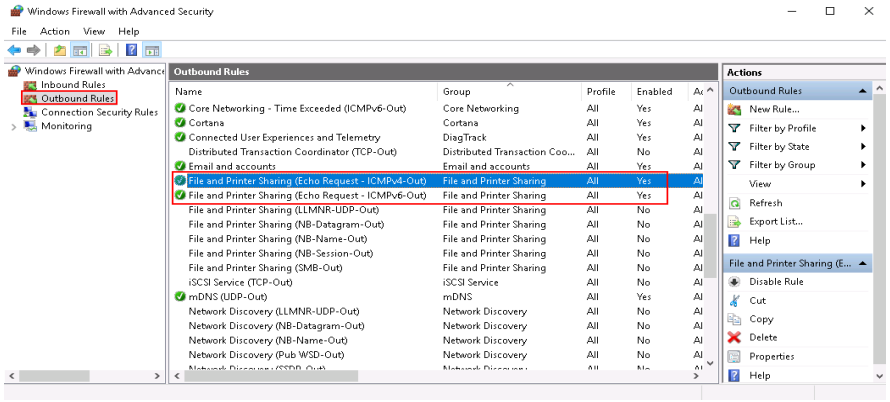


Figure 5-5 Outbound Rules



Checking Whether Ping Operations Are Prohibited on the HECS

Windows

Enable ping operations using the CLI.

1. Start the **Run** dialog box. Enter **cmd** and press **Enter**.
2. Run the following command to enable ping operations:

   netsh firewall set icmpsetting 8

Linux

Check the kernel parameters of the HECS.

1. Check the **net.ipv4.icmp_echo_ignore_all** value in the **/etc/sysctl.conf** file. Value **0** indicates that ping operations are allowed, and value **1** indicates that ping operations are prohibited.
2. Allow ping operations.
   - Run the following command to temporarily allow the ping operations:

     #echo 0 >/proc/sys/net/ipv4/icmp_echo_ignore_all
   - Run the following command to permanently allow the ping operations:

 Copyright © Huawei Technologies Co., Ltd.

net.ipv4.icmp_echo_ignore_all=0

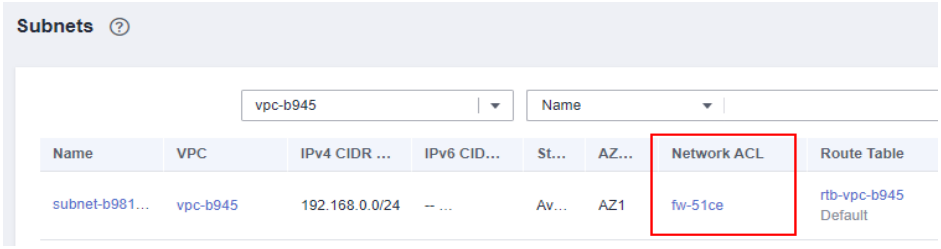
Checking Network ACL Rules

By default, no network ACL is configured for a VPC. If a network ACL is associated with a VPC, check the network ACL rules.

1. Check whether the subnet of the HECS has been associated with a network ACL.

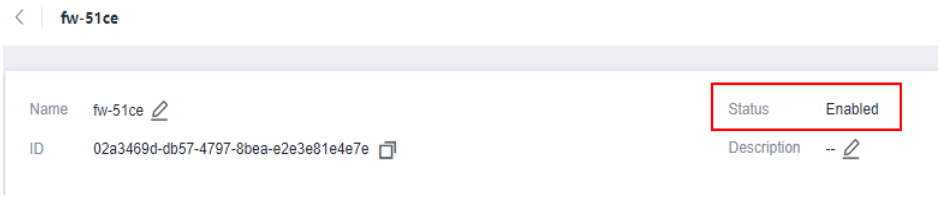
   If a network ACL name is displayed, the subnet of the HECS has been associated with the network ACL.

   Figure 5-6 Network ACL



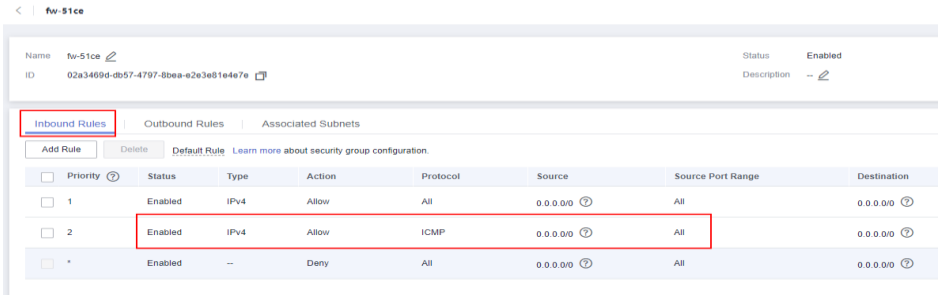
2. Click the network ACL name to view its status.

   Figure 5-7 Enabled network ACL



3. If the network ACL is enabled, add an ICMP rule to allow traffic.

   Figure 5-8 Adding an ICMP rule



NOTE

The default network ACL rule denies all incoming and outgoing packets. After the network ACL is disabled, the default rule still takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Checking the Network

1. Use another HECS in the same region to check whether the local network is functional.

   Use another HECS in the same region to ping the affected EIP. If the EIP can be pinged, the VPC is functional. In such a case, rectify the local network fault and ping the affected EIP again.

2. Check whether the link is accessible.

   A ping failure may be caused by link congestion, link node faults, or heavy load on the HECS.

   For details, see Troubleshooting a Ping Failure or Packet Loss Using a Link Test.

Checking the HECS Route Configuration If Multiple NICs Are Used

The default route of an OS preferentially selects the primary NIC generally. If an extension NIC is selected in a route and the network malfunctions, this issue is generally caused by the incorrect route configuration.

- If the HECS is configured with multiple NICs, check whether there is a default route in the HECS.

  a. Log in to the HECS and run the following command to check whether the default route is available:

  ip route

  Figure 5-9 Default route

  ```
  [root@do-not-del-scy ~]# ip route
  default via 192.168.2.1 dev eth0
  169.254.0.0/16 dev eth0  scope link  metric 1002
  169.254.169.254 via 192.168.2.1 dev eth0  proto static
  192.168.2.0/24 dev eth0  proto kernel  scope link  src 192.168.2.112
  ```

  b. If the route is unavailable, run the following command to add it:

  ip route add default via *XXXX* **dev eth0**

  NOTE

  In the preceding command, *XXXX* specifies a gateway IP address.

- If the HECS has multiple NICs and the EIP is bound to an extension NIC, configure policy routing on the HECS for network communication with the extension NIC.

  For details, see How Do I Configure Policy-Based Routing for ECSs with Multiple NICs?

Checking Domain Name Resolution If the Domain Name Cannot Be Pinged

If the EIP can be pinged but the domain name cannot be pinged, the possible cause is that the domain name has not obtained an ICP license or an error occurred in domain name.

1. Check the ICP license of the domain name.

   According to the *Regulation on Internet Information Service of the People's Republic of China* released by the Ministry of Industry and Information Technology (MIIT), all websites with their own domain name that operate in China are required to obtain a license.

 Copyright © Huawei Technologies Co., Ltd.

- If you want to use a server in the Chinese mainland to provide Internet services, you need to submit an ICP licensing request to the server provider to obtain an ICP license for the domain name.
- If your server is outside the Chinese mainland, no ICP license is required.

2. Check the domain name resolution.

   If your domain name has been licensed but the domain name records are incorrectly configured, the domain name may fail to be resolved.

   Switch to the DNS console to view details about the domain name records.

3. Check the DNS server configuration.

   If the system shows no server found after you ping the domain name, this issue may be caused by slow response from the DNS server. In such a case, see Troubleshooting Slow Access of a Website Outside the Chinese Mainland over an ECS.

5.2 Why Is Outbound Access Through TCP Port 25 Restricted?

Symptom

You cannot access an external address using TCP port 25. For example, you cannot run the **Telnet smtp.***.com 25** command.

Possible Causes

TCP port 25 is prohibited by default in the outbound direction for security purposes.

You do not need to enable TCP port 25, unless you want to deploy an email service on the cloud.

Solution

- If you want to use an HECS on HUAWEI CLOUD to send emails, you are advised to use Cloud Speedy Mail.
- Use port 465 supported by the third-party email service provider.
- Apply for enabling TCP port 25 in the outbound direction.

  If you must enable TCP port 25 on the HECS for external communications, submit an application.

NOTICE

Before sending the application, you must agree and guarantee that TCP port 25 is only used to connect to third-party Simple Mail Transfer Protocol (SMTP) servers and that emails are sent using the third-party SMTP servers. If you use the EIP specified in the service ticket to directly send emails over SMTP, we will permanently disable TCP port 25 and you will no longer be able to use it or request for it to be enabled.

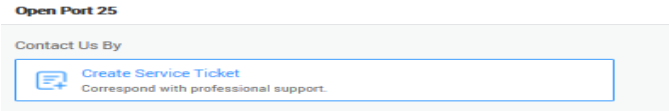
a. On the **Create Service Ticket** page, in the **Products** area, choose **Computing** > **Hyper Elastic Cloud Server**.

 Copyright © Huawei Technologies Co., Ltd.

For details about how to submit a service ticket, see Submitting a Service Ticket.

b. Click **Open Port 25** under **Select Subtype** and click **Create Service Ticket**.

Figure 5-10 Creating a service ticket



c. On the displayed page, enter the required information as prompted.

5.3 What Should I Do If My Windows HECS Cannot Access the Internet?

If you failed to access the Internet on a Windows HECS, following the operations provided in this section for troubleshooting.

Possible Causes

- The HECS has not had an EIP bound.
- The EIP exceeds the bandwidth limit.
- The access is blocked by the Internet service provider (ISP).
- The abnormal operation performed on the HECS triggers the security rule that denies the Internet access.
- The security group is incorrectly configured.
- The HECS performance cannot meet service requirements.
- The Internet access request is blocked by the firewall rule configured for the HECS.
- Third-party antivirus software installed on the HECS blocked the Internet access.
- The HECS has been attacked by viruses or Trojan horses.
- The network configuration on the HECS is incorrect.

Solution

Perform the following operations for troubleshooting:

1. Check whether the HECS has an EIP bound. If not, bind an EIP to it and check whether the fault is rectified.

   For instructions about how to bind an EIP, see Binding an EIP.

2. Check whether the HECS can access the Internet with the EIP bandwidth.

   If accessing the Internet failed, check whether the EIP bandwidth exceeds the bandwidth limit.

   For details, see How Do I Check Whether the Bandwidth Exceeds the Limit?

3. Check whether the fault occurs on specific IP addresses. If so, these IP addresses may be blocked by the ISP.

 Copyright © Huawei Technologies Co., Ltd.

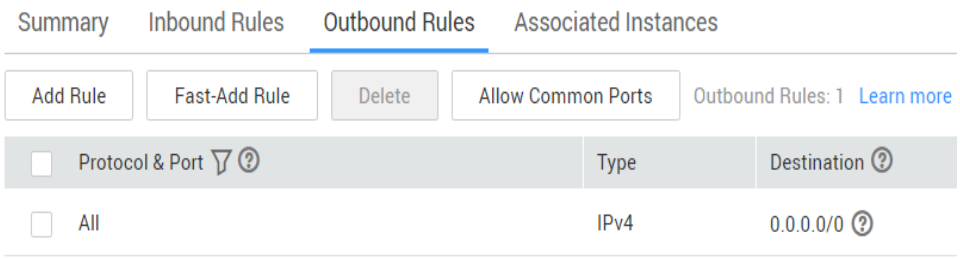
4. On the CLI of the HECS, run the **ipconfig /all** command to check whether the NIC configuration is correct. Run the **ncpa.cpl** command to start Network and Sharing Center and check whether the NIC is functional.
5. Run the **route print** command to obtain the routing table of the HECS and check whether the default route of 0.0.0.0 designates to the default gateway.
6. Run the **ping** command to check whether data can be exchanged between the HECS and the gateway.
7. Run the **ping** command to obtain the IP address of the DNS server.

   Compare the time required for pinging the DNS server and the time for pinging a specific IP address, and determine whether the DNS server is running properly.
8. Run the **netstat** command to detect SYN-SENT, CLOSE_WAIT, or FIN_WAIT.

   If such information is detected, port resources are exhausted. This issue is generally caused by a software bug. To handle this issue, rectify the fault and restart the HECS.
9. Check whether the security group of the HECS is correctly configured. If a whitelist is configured for the outbound rules of the security group, the network traffic in the outbound direction is permitted. As shown in Figure 5-11, all network traffic in the outbound direction is permitted.

   For instructions about how to permit a protocol or port, see Adding a Security Group Rule.

   Figure 5-11 Permitting all network traffic in the outbound direction



10. Disable firewall rules for the HECS and check whether the fault is rectified.

    If the fault is rectified, check the firewall rules.
11. Disable or uninstall the third-party antivirus software on the HECS, and check whether the fault is rectified.

5.4 Why Can't the Website Deployed on an HECS Be Accessed?

Symptom

Whether a website can be accessed depends on the network, port, firewall, and security group configurations of cloud servers. If any problem occurs, the website cannot be accessed.

 Copyright © Huawei Technologies Co., Ltd.

Troubleshooting

If an error is displayed when you access a website, identify possible causes based on the error message.

Identify possible causes based on error code descriptions in Returned Values for General Requests in the *Elastic Cloud Server API Reference*.

Possible causes are listed here in order of their probability.

If the fault persists after you have ruled out one cause, move on to the next one.

Figure 5-12 Possible causes and solutions



Table 5-3 Possible causes and solutions

Possible Cause	Handling Measure
Port communication	Check whether the port used by the website is listened to on the HECS. For details, see Checking Port Communication.
Security group rules	Check whether access to the port is allowed in the security group that contains the HECS. For details, see Checking Security Group Rules.
Firewall configuration	Disable the firewall and try again. For details, see Checking the Firewall Configuration.
HECS routes	Check whether the gateway configuration in the HECS route table is correct. For details, see Checking the HECS Routes.
Local network	Check whether you can use another hotspot or network to access the website. For details, see Checking the Local Network.
vCPU usage	Identify and optimize the processes that cause high vCPU usage. For details, see Checking the vCPU Usage.
Domain name	Check whether the domain name can be resolved. For details,

 Copyright © Huawei Technologies Co., Ltd.

Possible Cause	Handling Measure
resolution (applicable to scenarios where a domain name is used to access the website)	see Checking the ICP Filing and Domain Name Resolution.
ICP license (applicable to scenarios where a domain name is used to access the website)	Check whether the domain name of the website and the EIP of the HECS have been licensed. For details, see Checking the ICP Filing and Domain Name Resolution.

Checking Port Communication

Ensure that service processes and ports are in **LISTEN** state. Table 5-4 lists common TCP connection statuses.

- Linux

  Run the **netstat -antp** command to check whether the port used by the website is in **LISTEN** or **LISTENING** state.

  Example command: **netstat -ntulp |grep 80**

  Figure 5-13 Checking port status

  ```
  [root@elb-mq02 ~]# netstat -antpu | grep sshd
  tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      7178/sshd
  ```

  - If the port is in **LISTEN** state, go to Checking Security Group Rules.
  - If the port is not in **LISTEN** state, check whether the web service process is correctly configured and started.

- Windows

  Perform the following operations to check port communication:

  a. Run **cmd.exe**.

  b. Run the **netstat -ano | findstr "***PID***"** command to obtain the PID used by the process.

  Example command: **netstat -ano | findstr "80"**

  Figure 5-14 Checking port listening status

  ```
  C:\Users\Administrator>netstat -ano |findstr "80"
    TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
    TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       880
    TCP    [::]:80                [::]:0                 LISTENING       4
    TCP    [::]:49155             [::]:0                 LISTENING       880
    UDP    0.0.0.0:123            *:*                                    808
    UDP    [::]:123               *:*                                    808
  ```

  - If the port is in **LISTENING** state, go to Checking Security Group Rules.
  - If the port is not in **LISTENING** state, check whether the web service process is correctly configured and started.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-4 Common TCP connection statuses

TCP Connection Status	Description	Application Scenario
LISTEN	Listens for network connection requests from a remote TCP port.	The TCP server is running properly.
ESTABLISHED	Indicates that a connection has been set up.	A TCP connection is properly set up.
TIME-WAIT	Waits until the remote TCP server receives the acknowledgement after sending a disconnection request.	The TCP connection is disconnected, and this state is cleared in 1 minute.
CLOSE-WAIT	Waits for a disconnection request sent by a local user.	An application program fault leads to an open socket. This state is displayed after the network is disconnected, indicating that a process is in a dead cycle or waiting for certain requirements to be met. To resolve this issue, restart the affected process.
FIN-WAIT-2	Waits for the network disconnection request from a remote TCP server.	The network has been disconnected and requires 12 minutes to automatically recover.
SYN-SENT	Waits for the matched network connection request after a network connection request is sent.	The TCP connection request failed, which is generally caused by delayed handling of high CPU usage on the server or by a DDoS attack.
FIN-WAIT-1	Waits for the remote TCP disconnection request, or the acknowledgement for previous disconnection request.	If the network has been disconnected, this state may not automatically recover after 15 minutes. If the port has been used for a long period of time, restart the OS to resolve this issue.

Checking Security Group Rules

If the port used by the website is denied in the security group, add a rule to the security group to allow access to the port.

1. Log in to the management console.
2. Under **Computing**, click **Hyper ECS**.
3. On the **Hyper Elastic Cloud Server** page, click the name of the HECS with security group rules to be modified.
4. Click the **Security Groups** tab and view security group rules.
5. Click **Modify Security Group Rule**.
6. Configure the rule to allow access to the port used by the website.

 Copyright © Huawei Technologies Co., Ltd.

Checking the Firewall Configuration

- Linux

  The following uses port 80 and CentOS 6.8 as an example.

  a. Run the **iptables -nvL --line-number** command to obtain the firewall policies.

  b. Run the following commands to allow access to the default SSH port 80:

  iptables -A INPUT -p tcp --dport 80 -j ACCEPT

  iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

  c. Run the **service iptables save** command to save the added rules.

  d. Run the **service iptables restart** command to restart iptables.

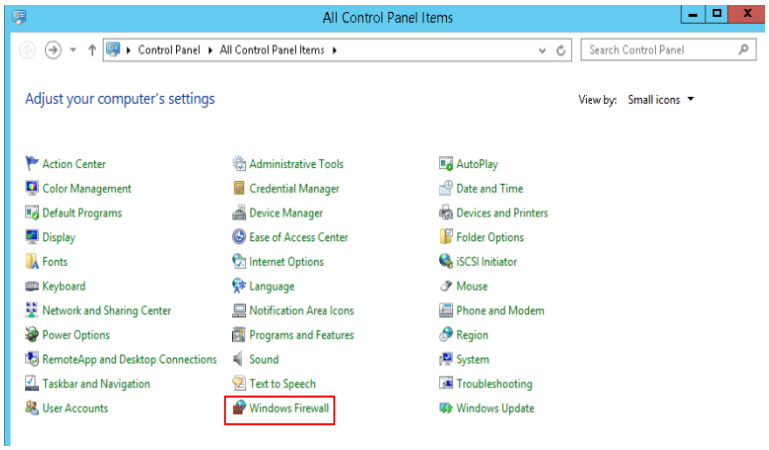
  e. Run the **iptables -nvL --line-number** command to check whether the added rules have taken effect.

  f. Disable the firewall and try again.

- Windows

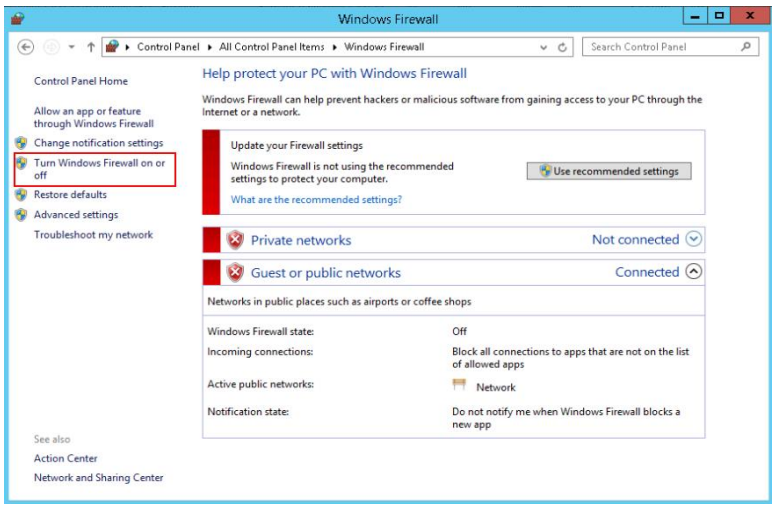
  a. Log in to the Windows HECS.

  b. Click the Windows icon in the lower left corner of the desktop and choose **Control Panel** > **Windows Firewall**.



  c. Click **Turn Windows Firewall on or off**.

  View and set the firewall status.



  d. Disable the firewall and try again.

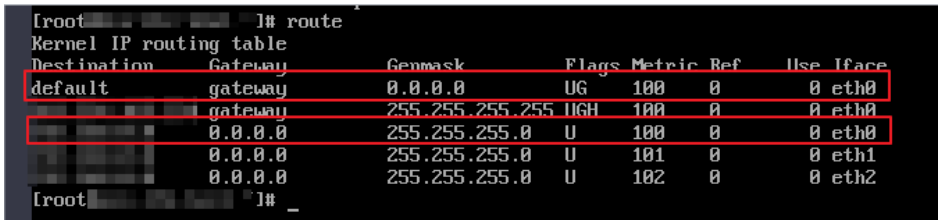
 Copyright © Huawei Technologies Co., Ltd.

Checking the HECS Routes

- Linux

a. Run the **route** command to check the routing policy. Ensure that the default route 0.0.0.0 is destined for the gateway and that the IP address and the gateway are in the same network segment, as shown in the first and third lines in Figure 5-15.

Figure 5-15 Viewing the routing policy



b. Run the **ifconfig** or **ip addr** command to obtain the HECS IP address.

Figure 5-16 ifconfig command output

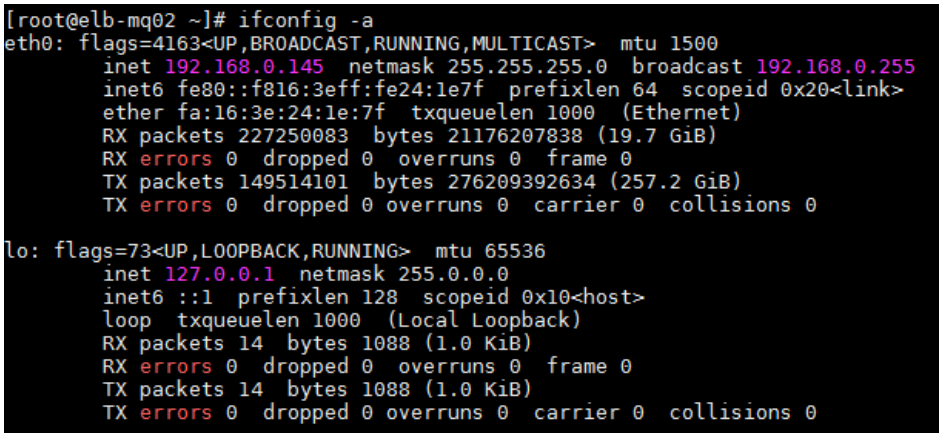
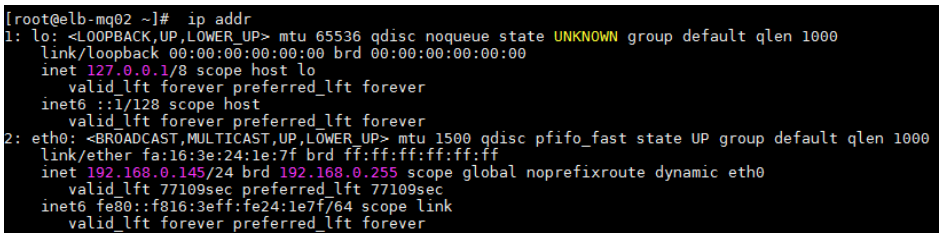


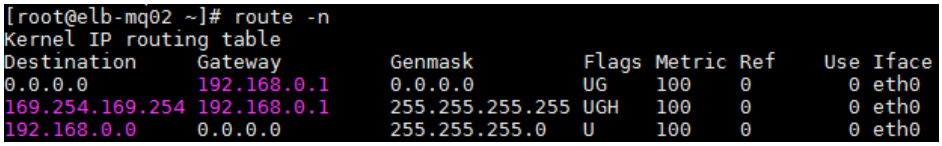
Figure 5-17 ip addr command output



c. Run the **route -n** command to obtain the gateway in the routing table.

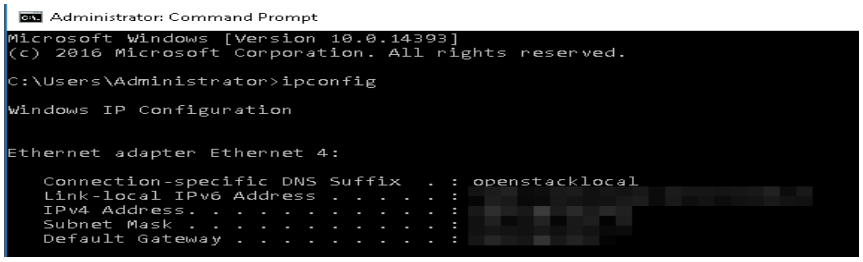
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-18 route -n command output



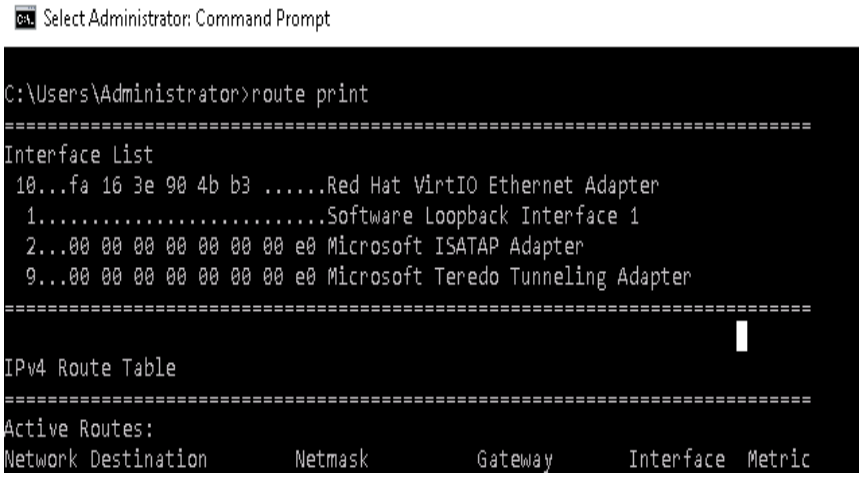
- Windows
  a. Run **cmd.exe**.
  b. Run the **ipconfig** command to obtain the HECS IP address.

  Figure 5-19 ipconfig command output



  c. Run the **route print** command to obtain the gateway in the routing table.

  Figure 5-20 route print command output



Checking the Local Network

Try another hotspot or network to access the website.

If the website can be accessed, the fault may occur on the local network. In such a case, rectify the fault and try again.

 Copyright © Huawei Technologies Co., Ltd.

Checking the vCPU Usage

If the bandwidth or vCPU usage of an HECS is too high, website access failures may occur. If you have created an alarm rule using Cloud Eye, the system automatically generates an alarm when the bandwidth or CPU usage reaches the threshold specified in the rule.

1. Identify the processes leading to high bandwidth or vCPU usage.
   - Windows offer multiple tools to locate faults, including Task Manager, Performance Monitor, Resource Monitor, Process Explorer, Xperf (supported by versions later than Windows Server 2008), and obtained full memory dump.
   - Linux: Run the **tcp** command to check the OS running status.
2. Check whether the processes are malicious and handle the issue accordingly.
   - If the processes are desired, optimize them or modify HECS configurations.
   - If the processes are malicious, stop these processes manually or use a third-party tool to stop them.

Checking the ICP Filing and Domain Name Resolution

Use the EIP bound to the HECS to access the website. If the website can be accessed using the EIP but not its domain name, the domain name cannot be resolved.

Whether a website can be accessed is related to the status and real-name authentication of the domain name, website licensing, domain name records, and website network environment. If any of the preceding is abnormal, the website cannot be accessed.

1. Check the ICP license of the domain name.

   According to the *Regulation on Internet Information Service of the People's Republic of China* released by the Ministry of Industry and Information Technology (MIIT), all websites with their own domain name that operate inside China are required to obtain a license.
   - If your server is in the Chinese mainland, submit an ICP filing request to the server provider to obtain an ICP license for the domain name.
   - If your server is outside the Chinese mainland, no ICP license is required.
   - If your domain name has been licensed, transfer it to HUAWEI CLOUD DNS for resolution or host a level-2 subdomain of the domain name on HUAWEI CLOUD DNS if you do not transfer the domain name.

   NOTE
   - Ensure that the ICP filing information is authentic and valid and that the website content is consistent with the ICP filing information.
   - After the application is approved, it takes one working day for the website to be accessible.
2. Check the domain name resolution.

   If your domain name has been licensed but the domain name records are incorrectly configured, the domain name may fail to be resolved.

   Switch to the DNS console to view details about the domain name records.
3. Check the DNS server configuration.

   If the system shows no server found after you ping the domain name, this issue may be caused by slow response from the DNS server. In such a case, see What Can I Do If Accessing a Website Outside the Chinese Mainland Is Slow on an HECS?

 Copyright © Huawei Technologies Co., Ltd.

5.5 Why Accessing a Website Outside the Chinese Mainland Is Slow on an HECS?

Symptom

Accessing a website outside the Chinese mainland may be slow on an HECS.

Generally, an international line is used for accessing a website outside the Chinese mainland. However, the international line may inevitably pass through network nodes distributed around the world, resulting in high latency.

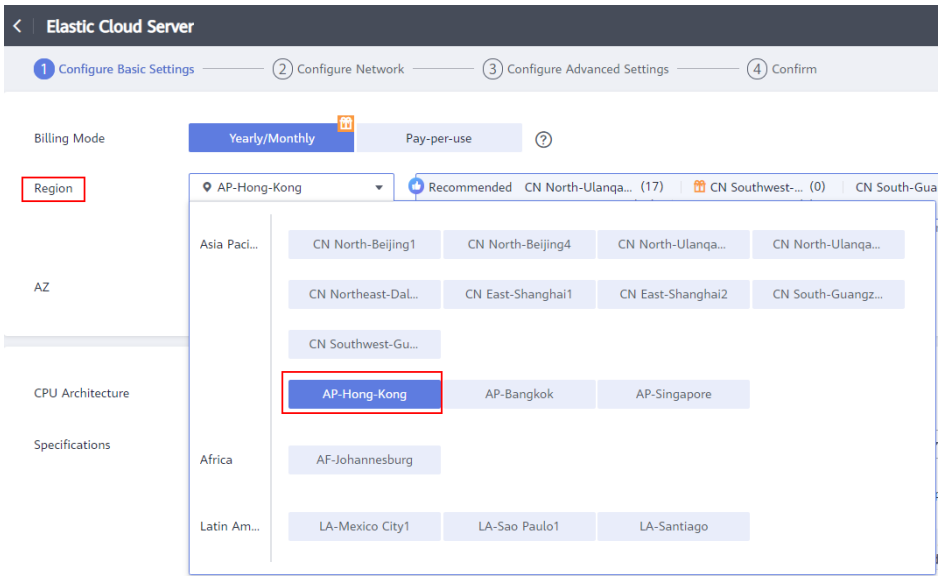
Handling Methods

- **Purchase HECSs in a region outside the Chinese mainland.**

  Considering the physical distance and network infrastructure, you can purchase HECSs in a region outside the Chinese mainland if you need to access websites outside the Chinese mainland.

  The following uses AP-Hong Kong as an example.

  Figure 5-21 Buying HECSs in AP-Hong Kong



- **Improve the access speed.**

  Alternatively, perform the following operations to speed up the access.

  – Modifying the DNS Configuration

  – Modifying the hosts File

  After that, run the **ping -t** *Website address* command to check the packet loss. For details, see Checking Whether the Request Is Responded.

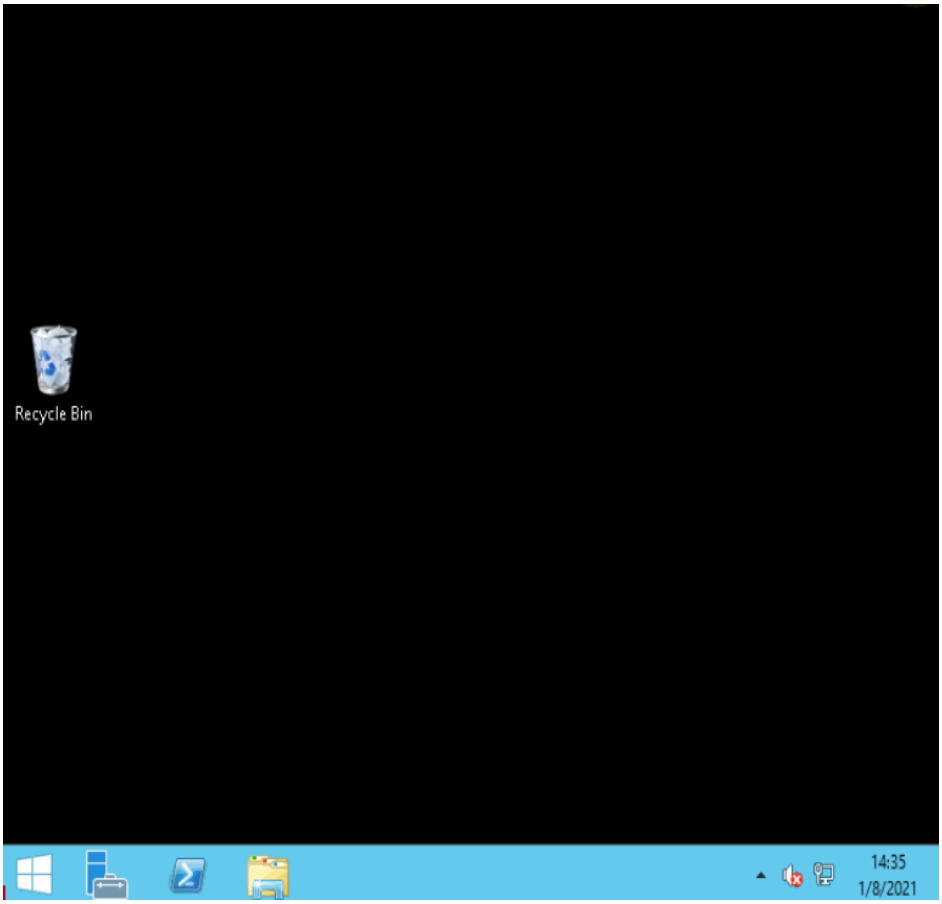
Modifying the DNS Configuration

Change the DNS server addresses to public DNS server addresses, for example, 114.114.114.114 and 8.8.8.8.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-22 demonstrates how you can modify the DNS configuration on Windows Server 2012.

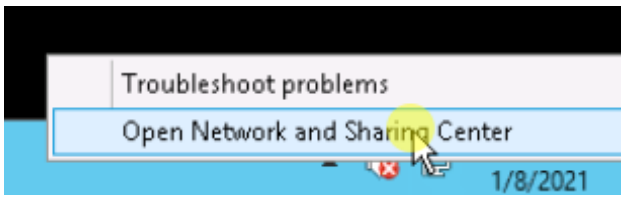
Figure 5-22 Modifying the DNS configuration



The following are detailed operations:

1. Log in to the HECS as user **Administrator**.
2. Enable the local area connection.
   a. In the lower right corner of the taskbar, right-click the network connection icon.
   b. Click **Open Network and Sharing Center**.

      Figure 5-23 Open Network and Sharing Center

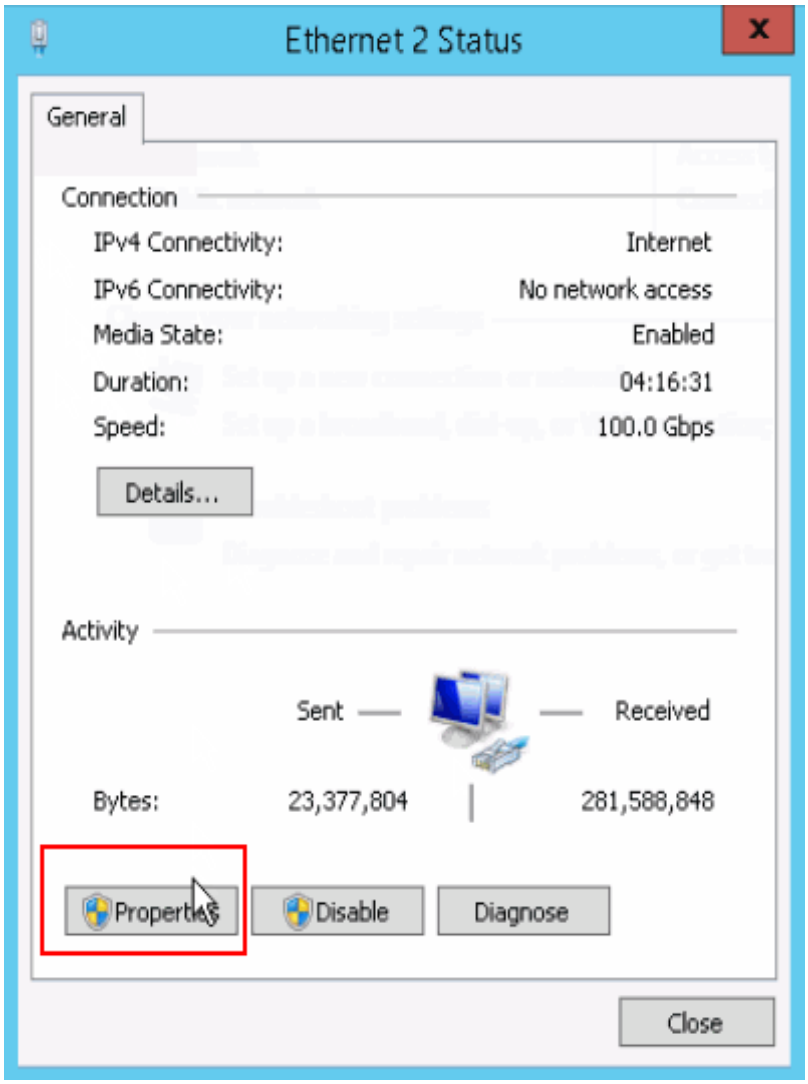
   c. In the navigation pane on the left, click **Change adapter settings**.
3. Configure the DNS server addresses of the HECS.

 Copyright © Huawei Technologies Co., Ltd.

a. Double-click network connections.

b. Click **Properties** in the lower left corner.

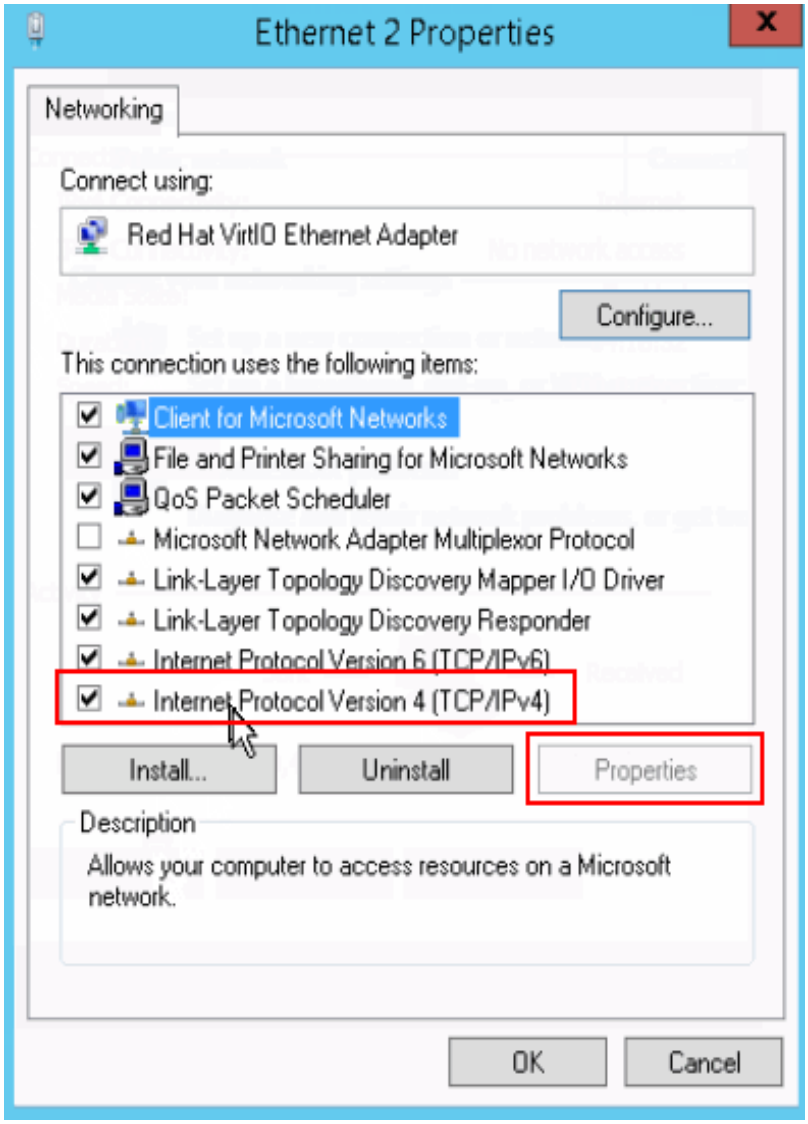
Figure 5-24 Local area connection



c. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

 Copyright © Huawei Technologies Co., Ltd.

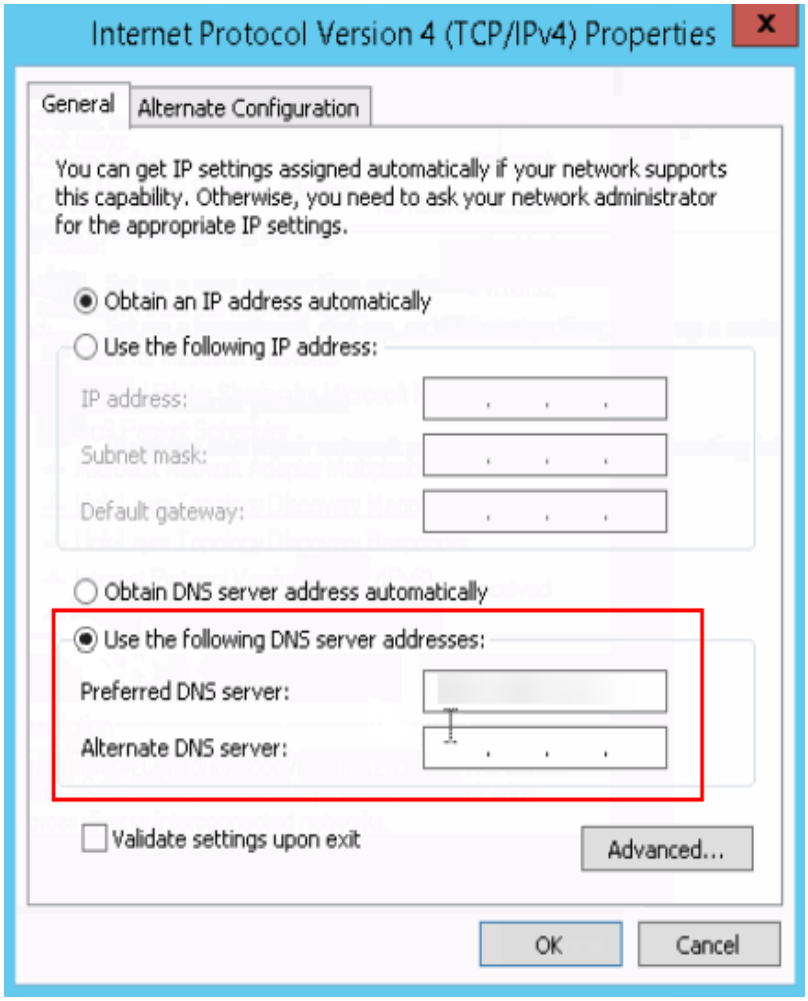
Figure 5-25 Selecting a protocol type



d. Select **Use the following DNS server addresses** and set the DNS server addresses.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-26 Setting the DNS server addresses



Modifying the hosts File

Select a server that allows you to access the website at the fastest speed and add its IP address and the domain name of the website to the **hosts** file.

Use either of the following methods to obtain the IP address of the server that allows you to access the website at the fastest speed:

- Ping the domain name.

  For details, see Method 1: Pinging the Domain Name.
- Use a ping tool and PingInfoView.

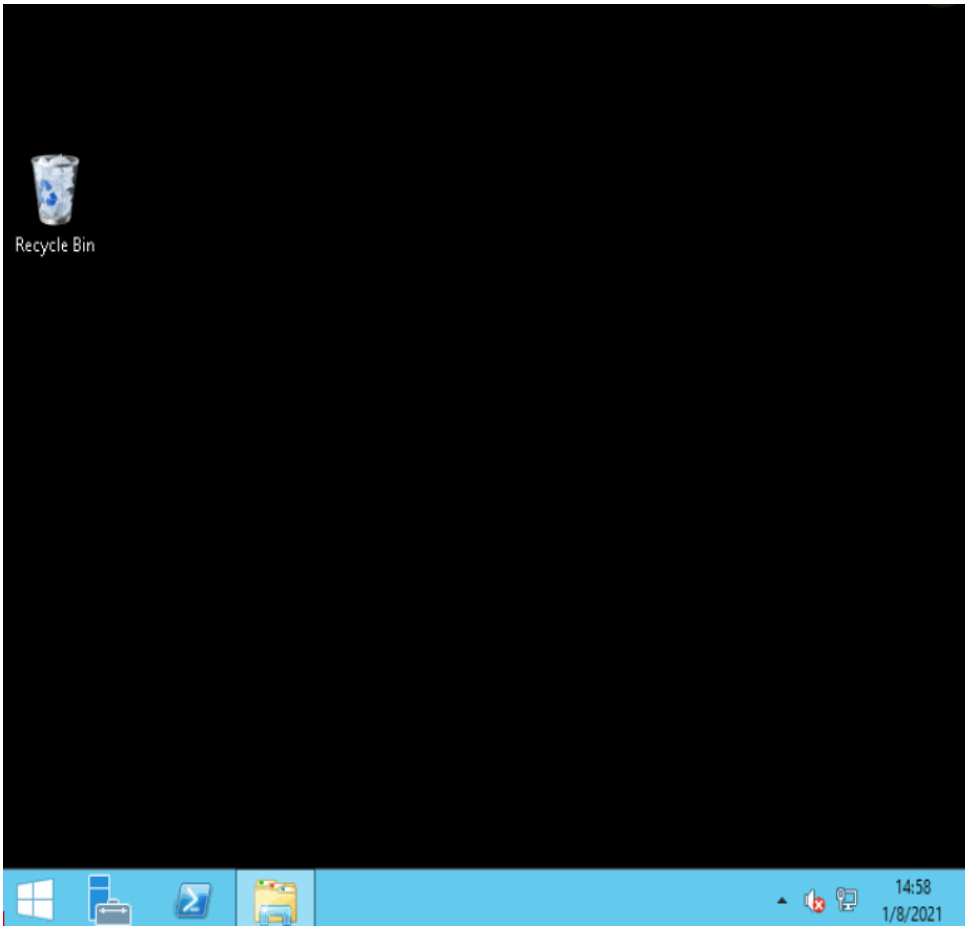
  For details, see Method 2: Using a Ping Tool and PingInfoView.

Method 1: Pinging the Domain Name

Figure 5-27 demonstrates how you can ping the domain name on Windows Server 2012 to obtain the IP address of the server with the fastest access speed. (www.example.com is used as the example domain name.)

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-27 Modifying the **hosts** file

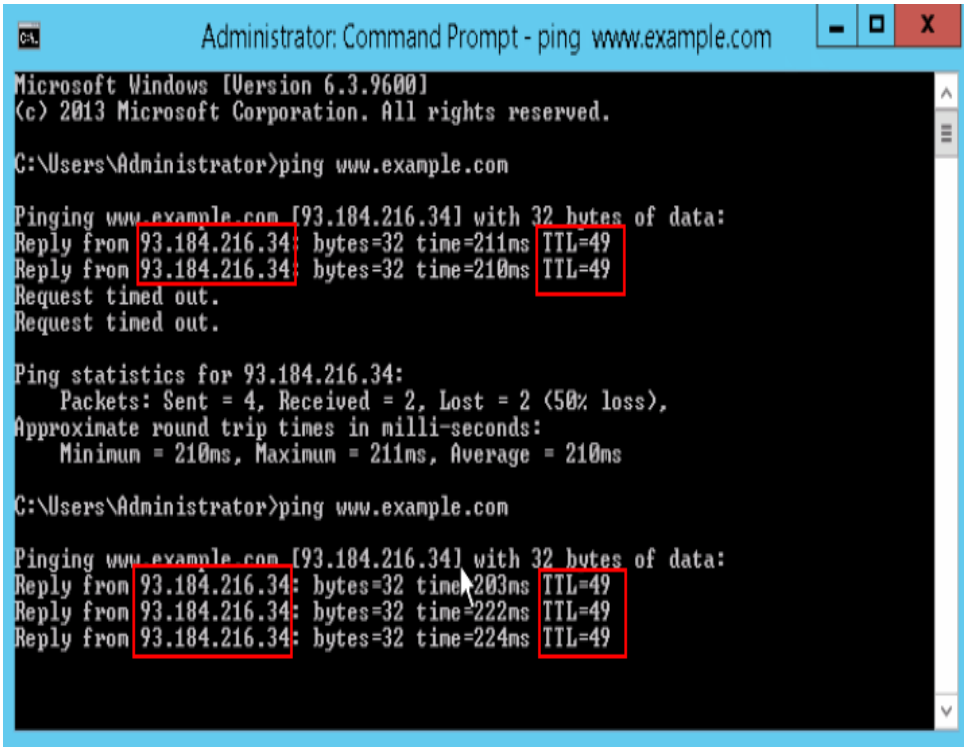


The following are detailed operations:

1. Ping www.example.com and wait for the result.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-28 Command output



2. Ping the domain name repeatedly and record a stable IP address with the smallest TTL value.

CAUTION

During the operation, run the **ipconfig /flushdns** command to refresh the DNS resolution cache. If you do not run the command, the same IP address will be returned.

In this example, IP address 93.184.216.34 has the smallest TTL value (**TTL=44**).

3. Modify the **hosts** file.

   Open the **C:\Windows\System32\drivers\etc\hosts** file, add the mapping between the IP address and the domain name (**99.84.178.238 www.example.com**) in the end of the file, save and exit the file.

CAUTION

- The **hosts** file is one of core OS files. Back up the **hosts** file before modifying it.
- Only the IP address you have configured in the **hosts** file will be returned when the domain name is used to access the website.
- If access is slow and you want to replace the IP address, delete the existing mapping from the **hosts** file and repeat the proceeding operations to obtain a new IP address.

4. Access the website again.

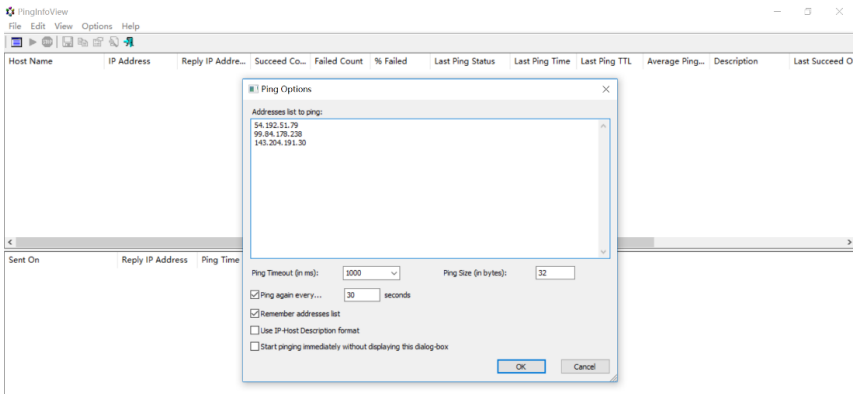
 Copyright © Huawei Technologies Co., Ltd.

Modifying the **hosts** file can only improve the access speed. If the problem persists, purchase HECSs in a region outside the Chinese mainland, for example, AP-Hong Kong.

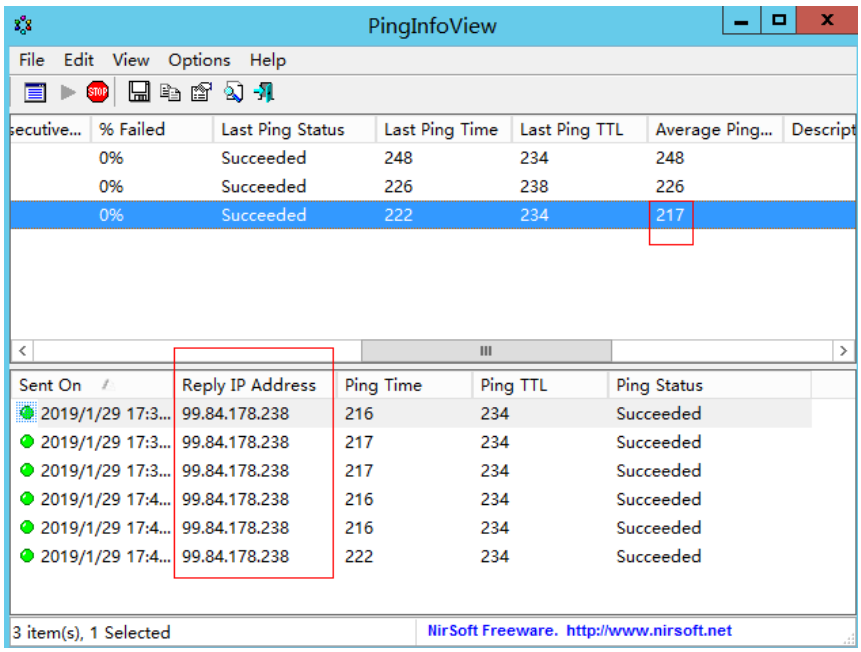
Method 2: Using a Ping Tool and PingInfoView

You can also try to speed up website access by modifying the **hosts** file. To do so, perform the following operations:

1. Log in to the HECS as user **Administrator**.
2. Use a browser to access the ping tool.
3. Enter the domain name of the website and record the IP addresses with the lowest response time. (www.example.com is used as an example.)
4. Download PingInfoView, decompress it, and run **PingInfoView.exe**.
5. Open **PingInfoView**, copy the IP addresses obtained in step 3 to the text box, and click **OK**.



6. Copy one IP address in the search result.



7. Open the **C:\Windows\System32\drivers\etc\hosts** file and add the mapping between the IP address and the domain name in the end of the file.

 Copyright © Huawei Technologies Co., Ltd.

CAUTION

- The **hosts** file is one of core OS files. Back up the **hosts** file before modifying it.
- Only the IP address you have configured in the **hosts** file will be returned when the domain name is used to access the website.
- If access is slow and you want to replace the IP address, delete the existing mapping from the **hosts** file and repeat the proceeding operations to obtain a new IP address.

For example, if the obtained IP address is 99.84.178.238, enter **99.84.178.238 www.example.com** in the end of the **hosts** file, save and exit the file.

8. Access the website again.

   If the fault persists, use an HECS purchased in a region outside the Chinese mainland to access the website.

Checking Whether the Request Is Responded

Try to access the website. If the website can be accessed but it is loaded slowly, packet loss may occur. In such a case, run the **ping -t** *Website address* command to check the packet loss. For details, see Troubleshooting a Ping Failure or Packet Loss Using a Link Test.

Example command: **ping -t www.example.com**

NOTE

In Windows, you can also download the curl client, decompress it, open the **bin** folder, copy the path, and configure the environment variables.

If a response status code is displayed, the request has been sent and received. Slow website access may be caused by loss of packets sent to the destination server.

Contact customer service to check for packet loss. You can also use Cloud Connect to speed up website access. For details, see Communication Among Multiple VPCs Across Regions.

 Copyright © Huawei Technologies Co., Ltd.

6 File Uploading

6.1 How Can I Upload a File to a Windows HECS?

Files are generally uploaded to Windows HECSs through MSTSC-based remote desktop connection. This section describes how to upload a file from a local Windows computer to a Windows HECS through remote desktop connection.

Prerequisites

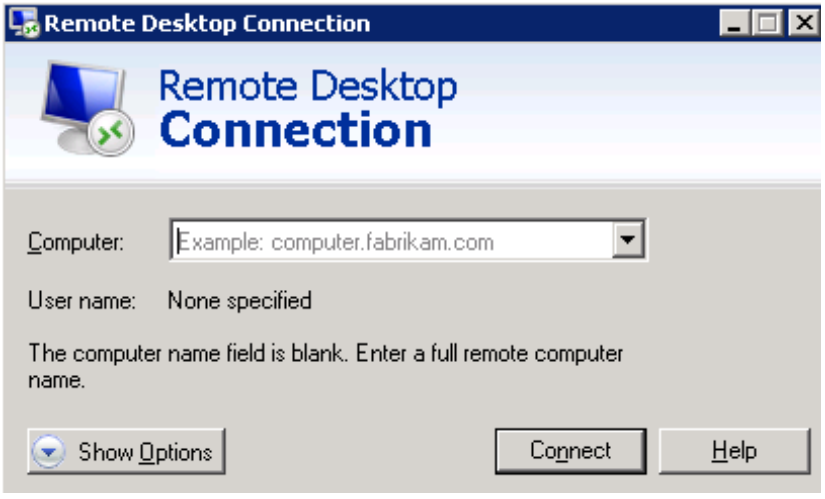
The Windows HECS can access the Internet.

Solution

1. On the local Windows computer, click **Start**. In the **Search programs and files** text box, enter **mstsc**.

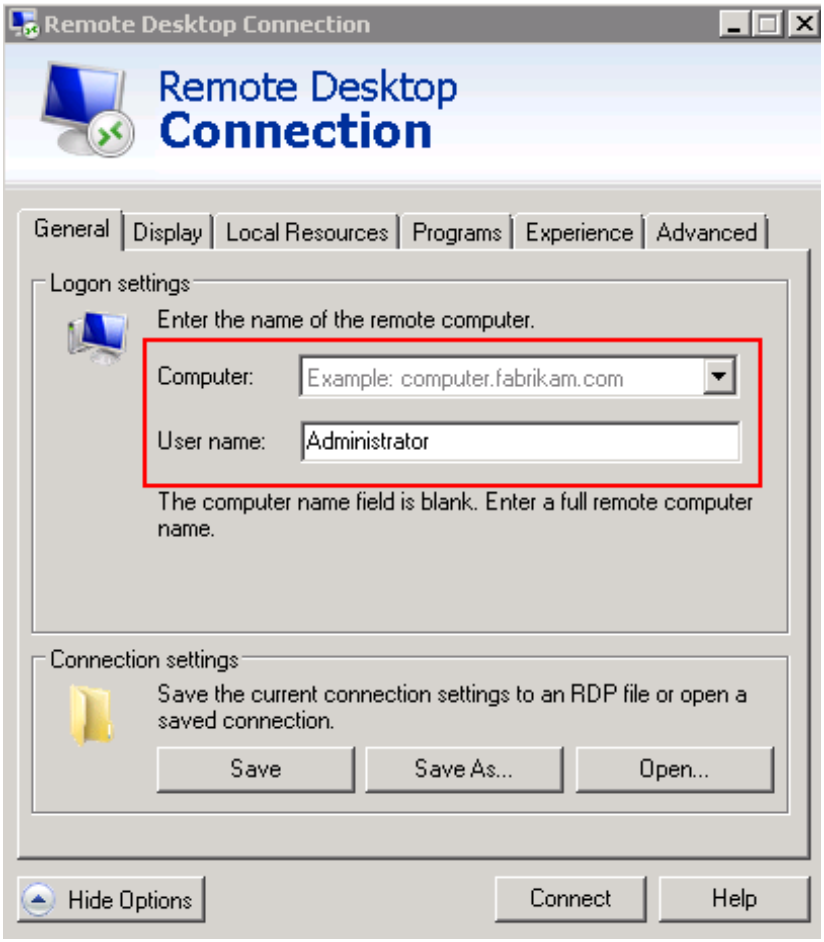
   The **Remote Desktop Connection** window is displayed.

2. Click **Options**.



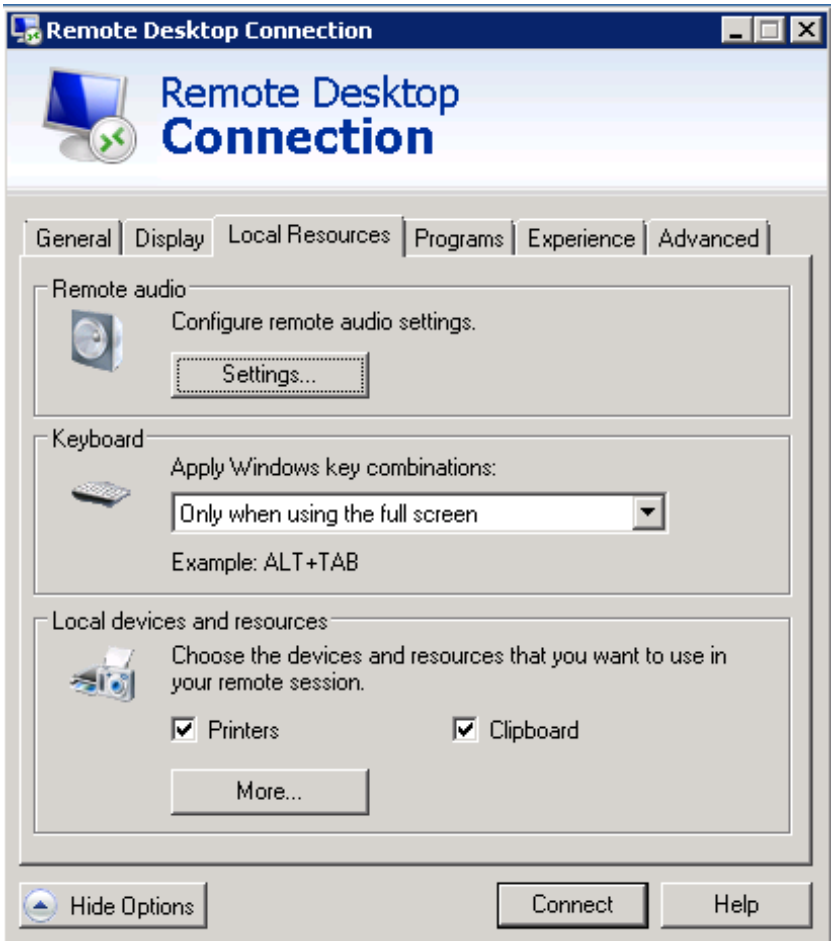
3. On the **General** tab, enter the EIP bound to the HECS and username **Administrator** for logging in to the HECS.

 Copyright © Huawei Technologies Co., Ltd.



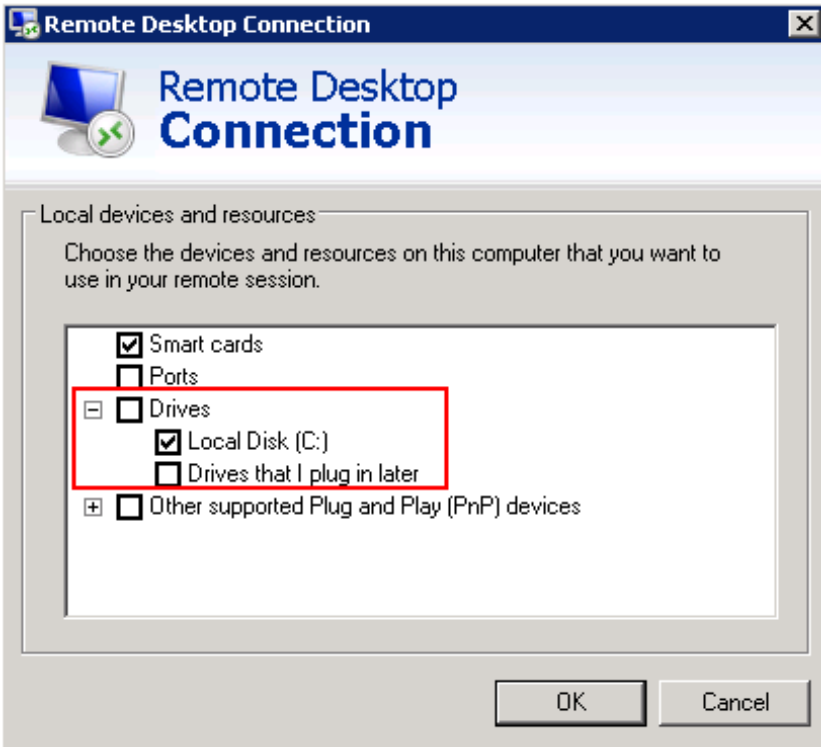
4. Click the **Local Resources** tab and verify that **Clipboard** is selected in the **Local devices and resources** pane.

 Copyright © Huawei Technologies Co., Ltd.



5. Click **More**.
6. In the **Drives** pane, select the local disk where the file to be uploaded to the Windows HECS is located.

 Copyright © Huawei Technologies Co., Ltd.



7. Click **OK** and log in to the Windows HECS.
8. Choose **Start** > **Computer**.

   The local disk is displayed on the Windows HECS.
9. Double-click the local disk to access it and copy the file to be uploaded to the Windows HECS.

6.2 How Can I Transfer Data Between a Local Host and a Windows HECS?

Method 1: Install a Data Transfer Tool

Install a data transfer tool, such as **QQ.exe** on both the local host and the Windows HECS to transmit data.

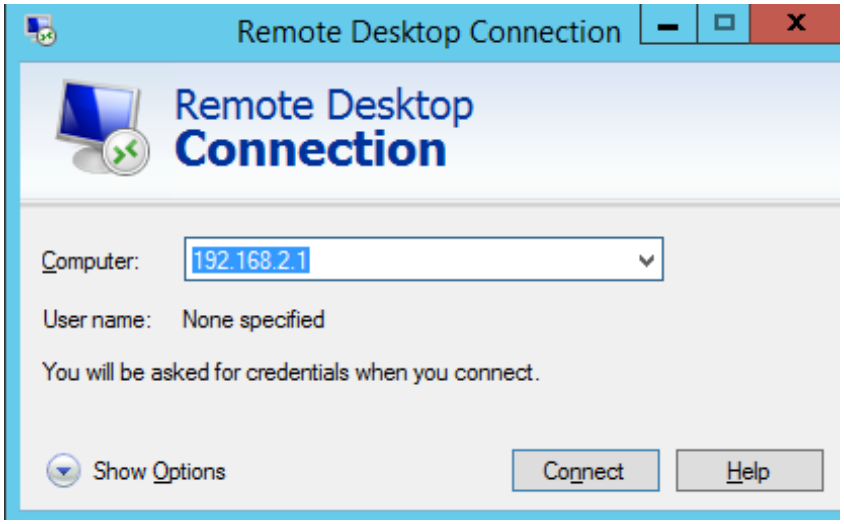
Method 2: Configure Local Disk Mapping

Use MSTSC to transfer data. This method does not support resumable transmission. Therefore, you are not recommended to use this method to transfer large files. If you need to transfer a large file, use FTP.

1. Log in to the local host.
2. Press **Win+R** to open the **Open** text box.
3. Enter **mstsc** to start the remote desktop connection.

 Copyright © Huawei Technologies Co., Ltd.

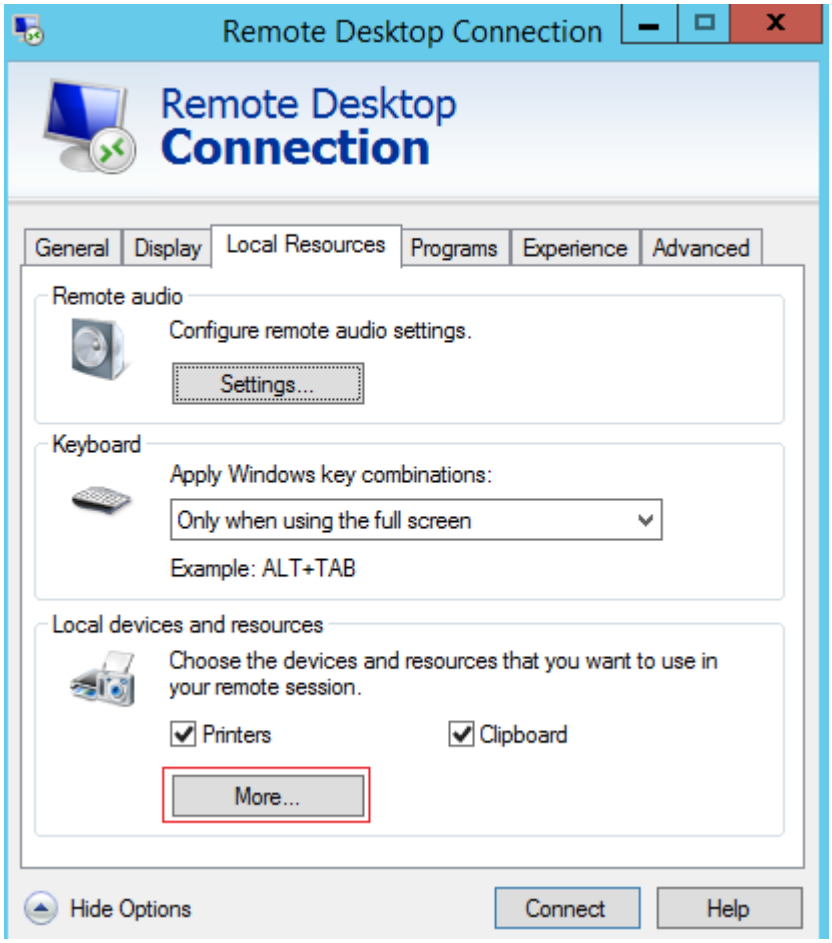
Figure 6-1 Remote Desktop Connection



4. In the **Remote Desktop Connection** window, click in the lower left corner.
5. Click the **Local Resources** tab and then **More** in the **Local devices and resources** pane.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-2 Local Resources

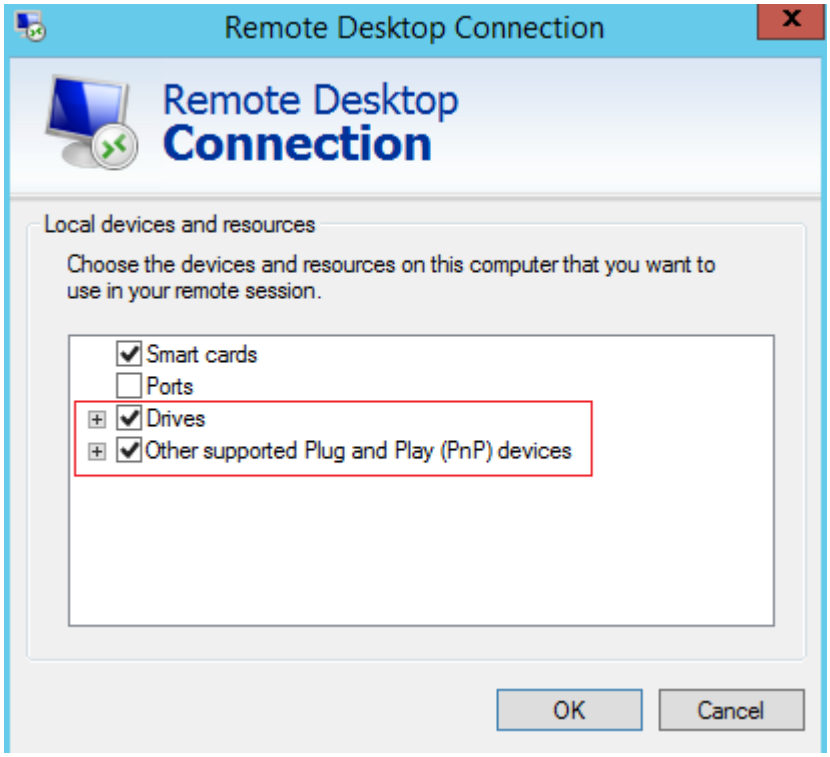


6. Select **Drives** and **Other supported Plug and Play (PnP) devices** and click **OK** to map all disks on the local host to the Windows HECS.

   If only certain disks on the local host need to be mapped to the Windows HECS, expand **Drives** and select the desired ones.

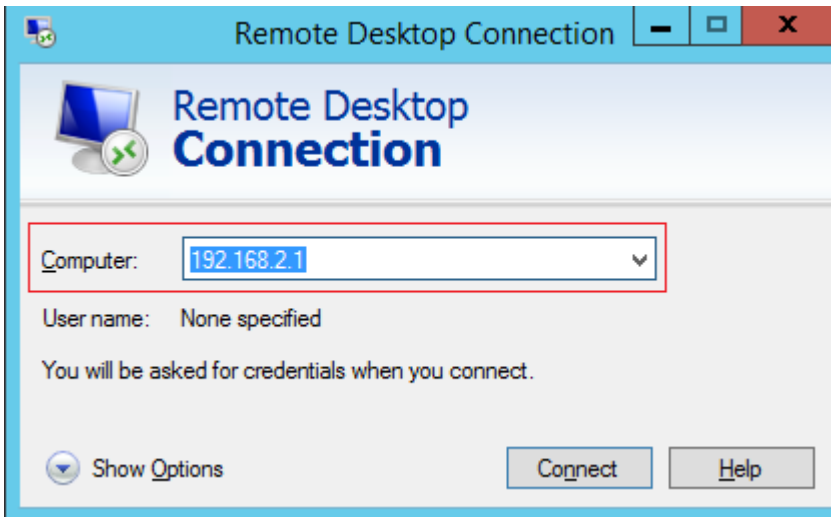
 Copyright © Huawei Technologies Co., Ltd.

Figure 6-3 Local devices and resources



7. Open the **Remote Desktop Connection** window again and enter the EIP bound to the Windows HECS in the **Computer** text box.

Figure 6-4 Connecting a remote desktop to the Windows HECS



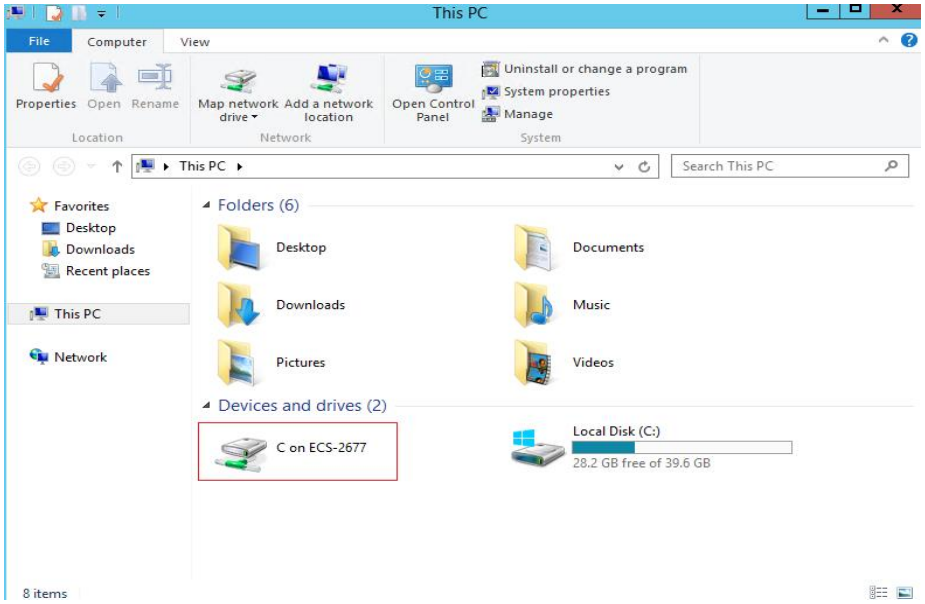
8. Click **Connect**.

   Log in to the Windows HECS.

9. Check the disks of the Windows HECS. If the disk information of the local host is displayed, data can be transmitted between your local host and the Windows HECS.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-5 Viewing disks



Method 3: Set Up an FTP Site

Set up an FTP site and transfer files to the HECS.

6.3 How Can I Use WinSCP to Upload a File to a Linux HECS?

WinSCP is generally used to upload files to Linux HECSs. This section describes how to upload a file from a local Windows computer to a Linux HECS using WinSCP.

The operations described in this section are performed in CentOS 7.2 as an example.

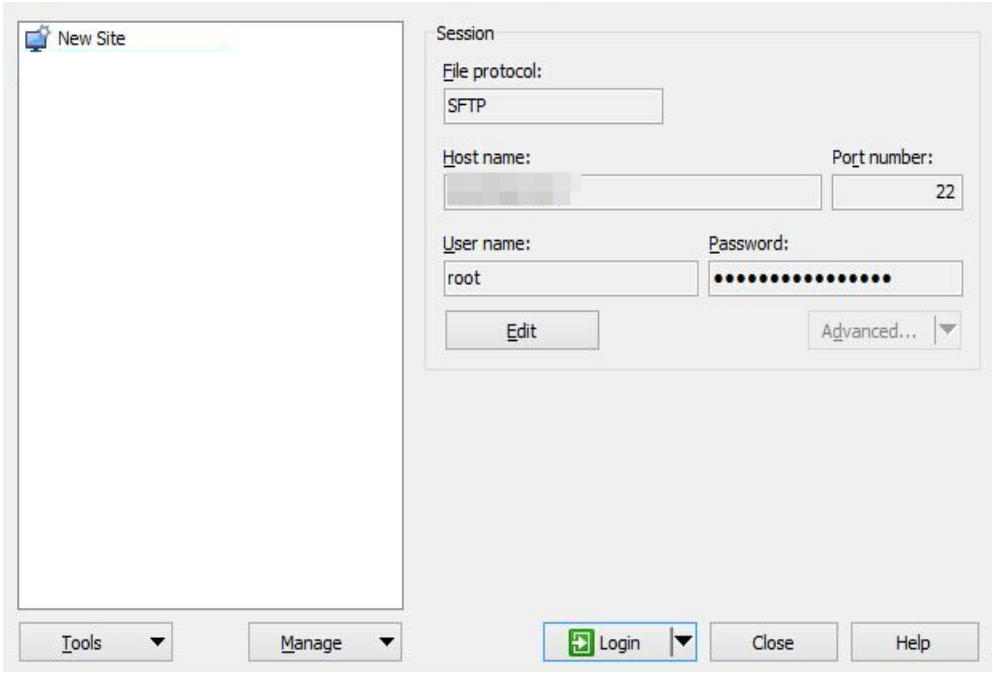
Prerequisites

The Linux HECS can access the Internet.

Solution

1. Download WinSCP and install it. To download WinSCP, log in at https://winscp.net/eng/docs/start.
2. Install WinSCP.
3. Start WinSCP.

 Copyright © Huawei Technologies Co., Ltd.



Set parameters as follows:

- **File protocol**: Select **SFTP** or **SCP**.
- **Host name**: Enter the EIP bound to the HECS. Log in to the management console to obtain the EIP.
- **Port number**: **22** by default.
- **User name**: Enter the username for logging in to the HECS.
- **Password**: Enter the password you set when purchasing the HECS or the password you set after purchasing the HECS.

4. Click **Login**.
5. After the login, drag a file from the local computer on the left to the remotely logged in HECS on the right for uploading.

 Copyright © Huawei Technologies Co., Ltd.

7 Disk Management

7.1 What Is the Mapping Between Device Names and Disks?

Scenarios

After I logged in to a Linux HECS and viewed disk information, I found that the disk device names were different from those displayed on the management console and could not identify the HECS to which a specified disk was attached. This section describes how to obtain the device name used on an HECS according to the disk information displayed on the management console.

Obtaining the Disk ID of an HECS on the Management Console

1. Log in to the management console.
2. Under **Computing**, click **Halo ECS**.
3. On the **Hyper Elastic Cloud Server** page, click the name of the target HECS.
   The page providing details about the HECS is displayed.
4. Click the **Disks** tab and then to expand the disk information.
5. Check the disk **Device Identifier**.

NOTE

If **Device Identifier** is not displayed on the web page, stop the HECS and restart it.

- If **Device Type** is **VBD**, use a serial number or BDF to obtain the disk device name.
  To use a serial number, see Using a Serial Number to Obtain a Disk Device Name.
  To use a BDF, see Using a VBD to Obtain a Disk Device Name.
- If **Device Type** is **SCSI**, use a WWN to obtain the disk device name. For details, see Using a WWN to Obtain a Disk Device Name.

Using a Serial Number to Obtain a Disk Device Name

If a serial number is displayed on the management console, run either of the following commands to obtain the device name.

 Copyright © Huawei Technologies Co., Ltd.

For example, if the serial number of the VBD disk is 62f0d06b-808d-480d-8, run either of the following commands:

 # udevadm info --query=all --name=/dev/xxx | grep ID_SERIAL

 # ll /dev/disk/by-id/*

Or:

 # udevadm info --query=all --name=/dev/vdb | grep ID_SERIAL

 # ll /dev/disk/by-id/*

The following information is displayed:

```
[root@ecs-ab63 ~]# udevadm info --query=all --name=/dev/vdb | grep ID SERIAL
E: ID_SERIAL=62f0d06b-808d-480d-8
[root@ecs-ab63 ~]# ll /dev/disk/by-id/*
lrwxrwxrwx 1 root root  9 Dec 30 15:56 /dev/disk/by-id/virtio-128d5bfd-f215-487f-9
-> ../../vda
lrwxrwxrwx 1 root root 10 Dec 30 15:56
/dev/disk/by-id/virtio-128d5bfd-f215-487f-9-part1 -> ../../vda1
lrwxrwxrwx 1 root root  9 Dec 30 15:56 /dev/disk/by-id/virtio-62f0d06b-808d-480d-8
-> ../../vdb
```

The displayed information is the disk device name, **/dev/vdb** in the preceding terminal display.

Using a VBD to Obtain a Disk Device Name

1. Run the following command to use a BDF to obtain the device name:

   ll /sys/bus/pci/devices/*BDF disk ID***/virtio*/block**

   For example, if the BDF disk ID of the VBD disk is 0000:02:02.0, run the following command to obtain the device name:

   ll /sys/bus/pci/devices/0000:02:02.0/virtio*/block

   The following information is displayed:

   ```
   [root@ecs-ab63 ~]# ll /sys/bus/pci/devices/0000:02:02.0/virtio*/block
   total 0
   drwxr-xr-x 8 root root 0 Dec 30 15:56 vdb
   ```

   The displayed information is the disk device name, **/dev/vdb** in the preceding terminal display.

Using a WWN to Obtain a Disk Device Name

1. Log in to the HECS as user **root**.
2. Run the following command to view the disk device name:

   ll /dev/disk/by-id |grep *WWN***|grep scsi-3**

   For example, if the WWN obtained on the management console is 6888603000008b32fa16688d09368506, run the following command:

   ll /dev/disk/by-id |grep 6888603000008b32fa16688d09368506|grep scsi-3

   The following information is displayed:

   ```
   [root@host-192-168-133-148 block]# ll /dev/disk/by-id/ |grep
   6888603000008b32fa16688d09368506 |grep scsi-3
   ```

 Copyright © Huawei Technologies Co., Ltd.

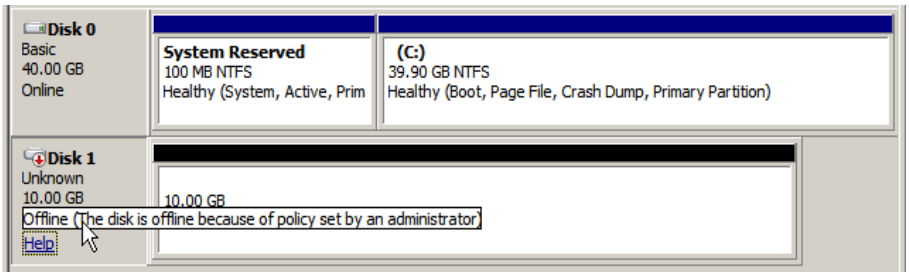
```
lrwxrwxrwx 1 root root  9 May 21 20:22 scsi-36888603000008b32fa16688d09368506
-> ../../sda
```

7.2 What Should I Do If a Disk Is Offline?

Symptom

A disk attached to a Windows HECS is offline, and the system displays the message "The disk is offline because of policy set by an administrator."

Figure 7-1 Offline disk



Possible Causes

Windows has three types of SAN policies: **OnlineAll**, **OfflineShared**, and **OfflineInternal**.

Table 7-1 SAN policies

SAN Policy	Description
OnlineAll	Indicates that all newly detected disks are automatically brought online.
OfflineShared	Indicates that all newly detected disks on sharable buses, such as FC or iSCSI, are left offline by default, while disks on non-shareable buses are kept online.
OfflineInternal	Indicates that all newly detected disks are left offline.

The SAN policy of certain Windows OSs, such as Windows Server 2008/2012 Enterprise Edition and Data Center Edition, is **OfflineShared** by default.

Solution

Use the disk partition management tool DiskPart to obtain and set the SAN policy on the HECS to **OnlineAll**.

1. Log in to the Windows HECS.
2. Press **Win+R** to run **cmd.exe**.
3. Run the following command to access DiskPart:

 Copyright © Huawei Technologies Co., Ltd.

diskpart

4. Run the following command to view the SAN policy on the HECS:

   san

   - If the SAN policy is **OnlineAll**, run the **exit** command to exit DiskPart.
   - If the SAN policy is not **OnlineAll**, go to step 5.

5. Run the following command to change the SAN policy to **OnlineAll**:

   san policy=onlineall

6. (Optional) Use the HECS with the SAN policy changed to create a private image to make the configuration take effect permanently. After an HECS is created using this private image, the disks attached to the HECS are online by default. You only need to initialize them.

7.3 What Should I Do If the Data Disk of a Windows HECS Becomes Offline After the HECS Specifications Are Modified?

Scenarios

After the specifications of a Windows HECS are modified, disk attachment may fail. Therefore, check disk attachment after specification modification. This section describes how to check disk attachment after HECS specifications are modified.

Procedure

1. Check whether the number of disks displayed on the **Computer** page after specification modification is the same as that before specifications modification.

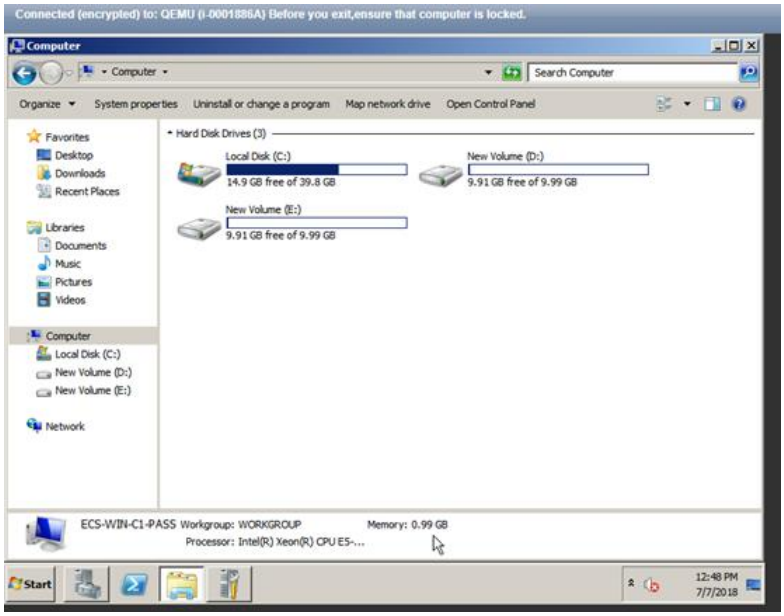
   - If yes, the disks are properly attached. No further action is required.
   - If no, an error has occurred in disk attachment. In this case, go to step 2.

   For example:

   An HECS running Windows Server 2008 has one system disk and two data disks attached before specification modification.

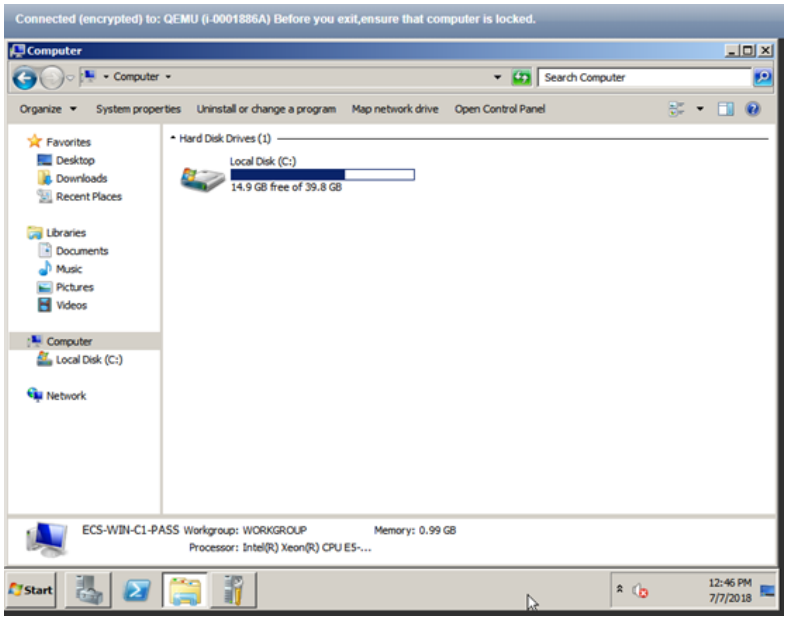
 Copyright © Huawei Technologies Co., Ltd.

Figure 7-2 Disk attachment before specification modification



After the specifications are modified, check disk attachment.

Figure 7-3 Disk attachment after specification modification



Only one system disk is displayed. Data disks failed to attach after the specification modification.

2. Set the affected disks to be online.
   a. Click **Start** in the task bar. In the displayed **Start** menu, right-click **Computer** and choose **Manage** from the shortcut menu.

      The **Server Manager** page is displayed.

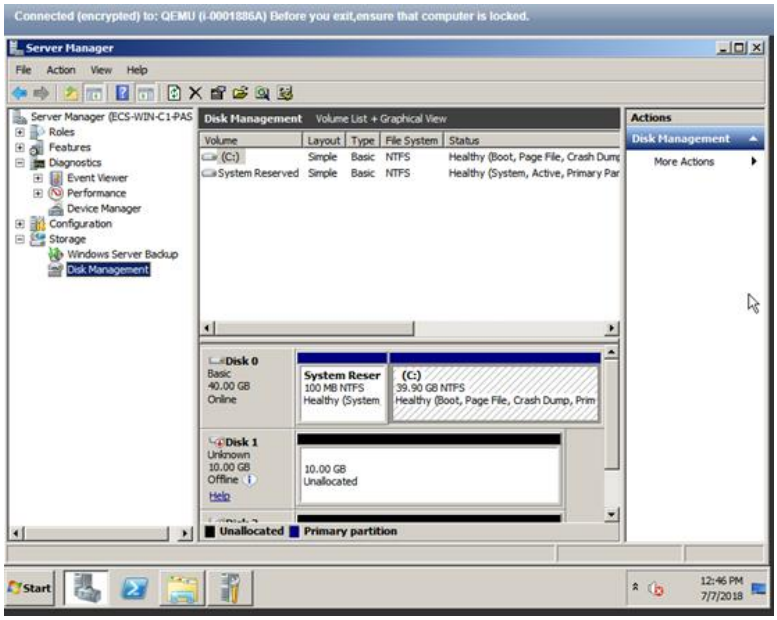
 Copyright © Huawei Technologies Co., Ltd.

b. In the navigation pane on the left, choose **Storage** > **Disk Management**.

   The **Disk Management** page is displayed.

c. In the left pane, the disk list is displayed. Right-click the affected disk and choose **Online** from the shortcut menu to set it to be online.

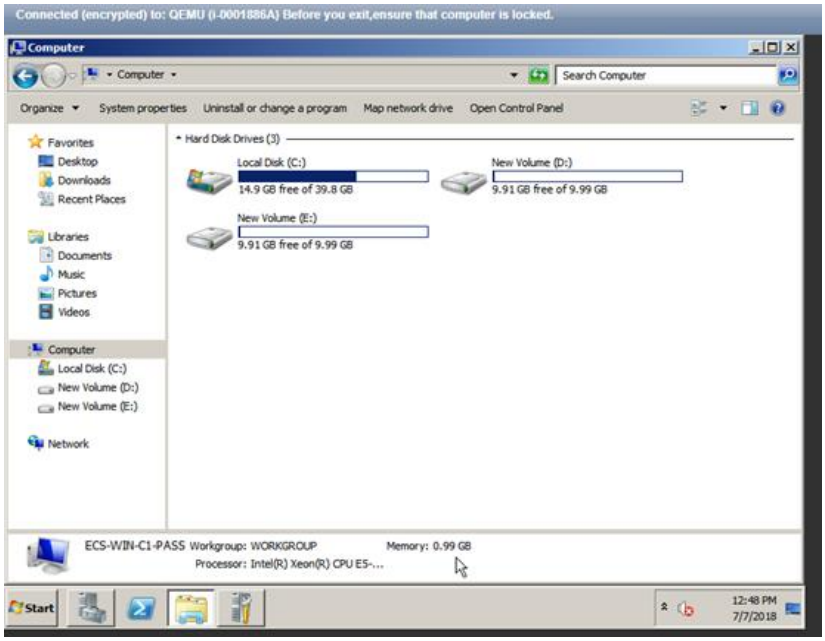
Figure 7-4 Setting the disk to be online



3. On the **Computer** page, check whether the number of disks is the same as that before the specification modification.
   - If the numbers are the same, no further action is required.
   - If the numbers are different, contact customer service.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-5 Disk attachment after disk online



7.4 What Should I Do If the Disk of a Linux HECS Becomes Offline After the HECS Specifications Are Modified?

Scenarios

After Linux HECS specifications are modified, disk mounting may fail. Therefore, check disk mounting after specification modification. This section describes how to check disk mounting after HECS specifications are modified.

Procedure

1. Log in to the HECS as user **root**.
2. Run the following command to view the disks mounted before specification modification:

   fdisk -l | grep 'Disk /dev/'

   Figure 7-6 Viewing disk information before specification modification

   ```
   [root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# fdisk -l |grep 'Disk /dev/'
   Disk /dev/vda: 42.9 GB, 42949672960 bytes, 83886080 sectors
   Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
   Disk /dev/vdc: 10.7 GB, 10737418240 bytes, 20971520 sectors
   [root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]#
   ```

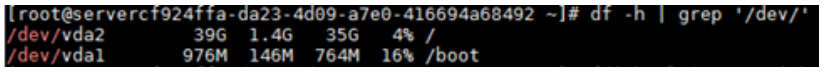
   As shown in Figure 7-6, the HECS has three disks attached: **/dev/vda**, **/dev/vdb**, and **/dev/vdc**.

 Copyright © Huawei Technologies Co., Ltd.

3. Run the following command to view disks mounted after specification modification:

   df -h| grep '/dev/'

   Figure 7-7 Viewing disk information after specification modification

   As shown in Figure 7-7, only one disk **/dev/vda** is mounted to the HECS.

4. Check whether the number of disks obtained in step 3 is the same as that obtained in step 2.
   - If the numbers are the same, the disk mounting is successful. No further action is required.
   - If the numbers are different, the disk mounting failed. In such a case, go to step 5.

5. Run the **mount** command to mount the affected disks.

   For example, run the following command:

   mount /dev/vbd1 /mnt/vbd1

   In the preceding command, **/dev/vbd1** is a disk partition, and **/mnt/vbd1** is the mount point to mount the partition.

NOTICE

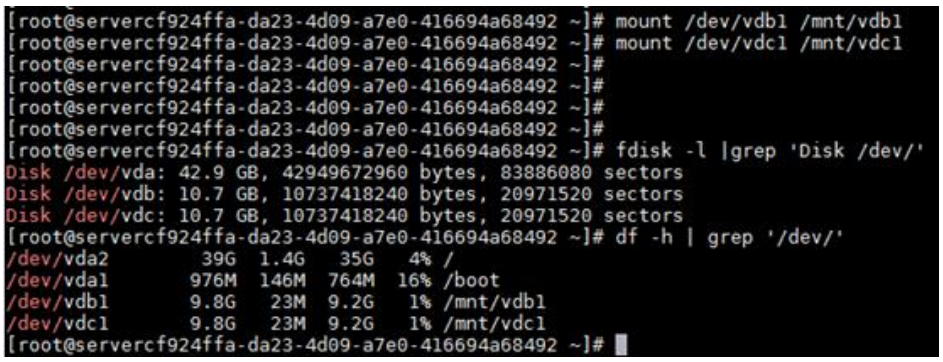
Ensure that **/mnt/vbd1** is empty. Otherwise, the mounting will fail.

6. Run the following commands to check whether the numbers of disks before and after specification modification are the same:

   fdisk -l | grep 'Disk /dev/'

   df -h| grep '/dev/'
   - If the numbers are the same, no further action is required.
   - If the numbers are different, contact customer service.

   Figure 7-8 Checking the number of disks mounted

   As shown in Figure 7-8, the numbers of disks before and after specification modification are the same. The disks are **/dev/vda**, **/dev/vdb**, and **/dev/vdc**.

 Copyright © Huawei Technologies Co., Ltd.

7.5 What Are the Restrictions on Attaching an EVS Disk to an HECS?

- The EVS disk and the target ECS must be located in the same AZ.
- For a non-shared disk, the EVS disk must be in **Available** state.

  For a shared disk, the target EVS disk must be in **In-use** or **Available** state.
- The target HECS must be in **Running** or **Stopped** state.
- A frozen EVS disk cannot be attached to an HECS.
- A SCSI EVS disk cannot be used as an HECS system disk.
- If you detach the system disk purchased when creating an HECS and want to continue using it as a system disk, you can only attach it to the original HECS. If you want to use it as a data disk, you can attach it to any HECS.

  If you detach the non-shared data disk purchased when you create an HECS and want to attach it again, you can only attach it to the original HECS as a data disk.

 Copyright © Huawei Technologies Co., Ltd.

8 Password Management

8.1 Resetting the Password for Logging In to a Windows HECS Without Password Reset Plug-ins Installed

Scenarios

If your Windows HECS has not had password reset plug-ins installed, follow the instructions provided in this section to reset the password.

The method described in this section can only be used to change the password of a local Windows account, but not the password of a domain account.

For details about the operations performed on Linux HECS, see 8.2 Resetting the Password for Logging In to a Linux HECS Without Password Reset Plug-ins Installed.

NOTE

HECSs created using a public image have one-click password reset plug-ins installed by default. To reset the password, see Resetting an HECS Password on the Management Console.

Prerequisites

- A temporary Linux HECS which runs Ubuntu 14.04 or later and locates in the same AZ as the target HECS is available.
- An EIP has been bound to the temporary HECS, and the apt-get source has been configured.
- You have used either of the following methods to install ntfs-3g and chntpw software packages on the temporary HECS:

  Method 1:

  Run the following command to install the **ntfs-3g** and **chntpw** software packages:

  sudo apt-get install ntfs-3g chntpw

  Method 2:

  Download the ntfs-3g and chntpw software packages of the version required by the temporary HECS OS.

  Log in at www.tuxera.com/community/open-source-ntfs-3g/ to obtain the **ntfs-3g** software package.

  Log in at https://pkgs.org/download/chntpw to obtain the **chntpw** software package.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Stop the original HECS, detach the system disk from it, and attach the system disk to the temporary HECS.
   a. Log in to the management console.
   b. Click  in the upper left corner and select your region and project.
   c. Under **Computing**, click **Hyper ECS**.
   d. Stop the original Windows HECS, switch to the page providing details about the HECS, and click the **Disks** tab.

   NOTE

   Do not forcibly stop the Windows HECS. Otherwise, password reset may fail.

   e. Locate the row containing the system disk and click **Detach** to detach the system disk from the HECS.
   f. On the page providing details about the temporary HECS, click the **Disks** tab.
   g. Click **Attach Disk**. In the displayed dialog box, select the system disk detached in step 1.e and attach it to the temporary HECS.
2. Log in to the temporary HECS remotely and attach the system disk to it.
   a. Run the following command to view the directory of the system disk detached from the original Windows HECS and now attached to the temporary HECS:

      fdisk -l
   b. Run the following command to mount the file system of the detached system disk to the temporary HECS:

      mount -t ntfs-3g /dev/*Result obtained in step 2.a* **/mnt/**

      For example, if the result obtained in step 2.a is **xvde2**, run the following command:

      mount -t ntfs-3g /dev/xvde2 /mnt/

      If the following error information is displayed after the preceding command is executed, the NTFS file systems may be inconsistent. In such a case, rectify the file system inconsistency.

      ```
      The disk contains an unclean file system (0, 0).
      Metadata kept in Windows cache, refused to mount.
      Failed to mount '/dev/xvde2': Operation not permitted
      The NTFS partition is in an unsafe state. Please resume and shutdown
      Windows fully (no hibernation or fast restarting), or mount the volume
      read-only with the 'ro' mount option.
      ```

      Back up the disk data, run the following command to rectify the NTFS file system inconsistency, and attach the system disk:

      ntfsfix /dev/*Result obtained in step 2.a*

      For example, if the result obtained in step 2.a is **xvde2**, run the following command:

      ntfsfix /dev/xvde2
3. Change the password and clear the original password.
   a. Run the following command to back up the SAM file:

      cp /mnt/Windows/System32/config/SAM /mnt/Windows/System32/config/SAM.bak
   b. Run the following command to change the password of a specified user:

      chntpw -u Administrator /mnt/Windows/System32/config/SAM

 Copyright © Huawei Technologies Co., Ltd.

c. Enter **1**, **q**, and **y** as prompted, and press **Enter**.

The password has been reset if the following information is displayed:

```
Select: [q] > 1
Password cleared!
Select: [q] > q
Hives that have changed:
#Name
0<SAM>
Write hive files? (y/n) [n] : y
0<SAM> - OK
```

4. Stop the temporary HECS, detach the system disk from it, and attach the system disk to the original HECS.
   a. Stop the temporary HECS, switch to the page providing details about the HECS, and click the **Disks** tab.
   b. Click **Detach** to detach the data disk temporarily attached in step 1.g.
   c. On the page providing details about the original Windows HECS, click the **Disks** tab.
   d. Click **Attach Disk**. In the displayed dialog box, select the data disk detached in step 4.b and device name **/dev/sda**.
5. Start the original HECS and set a new login password.
   a. Click **Start** to start the original Windows HECS. After the status becomes **Running**, click **Remote Login** in the **Operation** column.
   b. Click **Start**. Enter **CMD** in the search box and press **Enter**.
   c. Run the following command to change the password (the new password must meet the requirements described in Table 8-1):

      net user Administrator *New password*

Table 8-1 Password complexity requirements

Parameter	Requirement	Example Value
Password	• Consists of 8 characters to 26 characters. • Contains at least three of the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters for Windows: $!@%-_=+[]:./,? – Special characters for Linux: !@%-_=+[]:./^,{}? • Cannot contain the username or the username spelled backwards. • Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)	YNbUwp!dUc9M Clnv **NOTE** The example password is generated randomly. Do not copy this example password.

 Copyright © Huawei Technologies Co., Ltd.

8.2 Resetting the Password for Logging In to a Linux HECS Without Password Reset Plug-ins Installed

Scenarios

If your Linux HECS has not had password reset plug-ins installed, follow the instructions provided in this section to reset the password.

This section describes how to reset the password of user **root**. After resetting the password, you can log in to the HECS, and change the private key or reset the password of a non-**root** user.

For details about the operations performed on Windows HECSs, see 8.1 Resetting the Password for Logging In to a Windows HECS Without Password Reset Plug-ins Installed.

NOTE

HECSs created using a public image have one-click password reset plug-ins installed by default. To reset the password, see Resetting an HECS Password on the Management Console.

Prerequisites

- A temporary Linux HECS which locates in the same AZ as the target HECS is available.
- The temporary HECS has an EIP bound.

Procedure

1. Download the script for resetting the password and upload the script to the temporary HECS.

   Download the password reset script. Use a connection tool, such as WinSCP, to upload the obtained **changepasswd.sh** script to the temporary HECS.

   To download WinSCP, log in at https://winscp.net/.

2. Stop the original HECS, detach the system disk from it, and attach the system disk to the temporary HECS.

   a. Stop the original Linux HECS, switch to the page providing details about the HECS, and click the **Disks** tab.

   NOTE

   Do not forcibly stop the original HECS. Otherwise, password reset may fail.

   b. Locate the row containing the system disk to be detached and click **Detach** to detach the system disk from the HECS.

   c. On the page providing details about the temporary HECS, click the **Disks** tab.

   d. Click **Attach Disk**. In the displayed dialog box, select the system disk detached in step 2.b and attach it to the temporary HECS.

3. Log in to the temporary HECS remotely and reset the password.

   a. Locate the row containing the temporary HECS and click **Remote Login** in the **Operation** column.

   b. Run the following command to view the directory of the system disk detached from the original Linux HECS and now attached to the temporary HECS:

      fdisk -l

 Copyright © Huawei Technologies Co., Ltd.

c. Run the following commands in the directory where the script is stored to run the script for resetting the password:

chmod +x changepasswd.sh

./changepasswd.sh

When you run the password reset script, if the system displays a message indicating that there is no command related to logical volume manager (LVM), such as the message "no lvs command", install an LVM tool on the temporary HECS. The LVM2 tool is recommended, which can be installed by running the **yum install lvm2** command.

NOTE

If the original HECS and the temporary HECS both run CentOS 7, a mount failure may occur during script execution. To resolve this issue, replace **mount $dev $mountPath** with **mount -o nouuid $dev $mountPath** in the script.

d. Enter the new password and the directory obtained in step 3.b as prompted.

If the following information is displayed, the password has been changed:

```
set password success.
```

4. For a non-**root** user, perform the following operations to enable the login permission of user **root**:

vi /etc/ssh/sshd_config

Modify the following parameters:

- Change **PasswordAuthentication no** to **PasswordAuthentication yes**.

  Alternatively, delete the comment tag (#) before **PasswordAuthentication yes**.
- Change **PermitRootLogin no** to **PermitRootLogin yes**.

  Alternatively, delete the comment tag (#) before **PermitRootLogin yes**.
- Change the **AllowUsers** value to **AllowUsers root**.

  Search for **AllowUsers** in the file. If **AllowUsers** is unavailable, add it at the end of the file.

5. Stop the temporary HECS, detach the system disk from it, attach the system disk to the original HECS, and restart the original HECS.
   a. Stop the temporary HECS, switch to the page providing details about the HECS, and click the **Disks** tab.
   b. Click **Detach** to detach the data disk attached in step 2.
   c. On the page providing details about the original Linux HECS, click the **Disks** tab.
   d. Click **Attach Disk**. In the displayed dialog box, select the data disk detached in step 5.b and device name **/dev/sda**.
   e. Restart the original Linux HECS.

 Copyright © Huawei Technologies Co., Ltd.

9 Resource Monitoring

9.1 Why Is My Windows HECS Running Slowly?

If your Windows HECS runs slowly or is inaccessible unexpectedly, the bandwidth or CPU usage of the HECS may be excessively high. If you have created an alarm rule using Cloud Eye, the system automatically sends you an alarm when the bandwidth or CPU usage reaches the threshold specified in the rule.

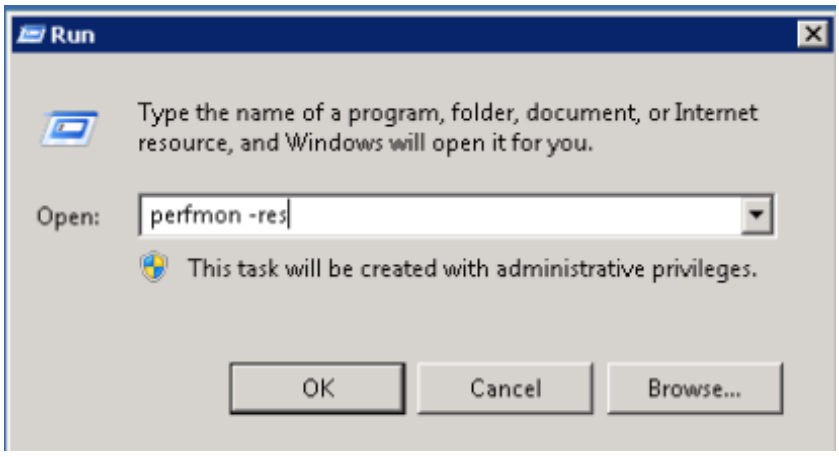
To resolve this issue, perform the following operations:

1. Fault locating: identifies the processes leading to high bandwidth or CPU usage.

   Windows OSs offer multiple tools to locate faults, including Task Manager, Performance Monitor, Resource Monitor, Process Explorer, Xperf (supported by versions later than Windows Server 2008), and obtained full memory dump. When traffic is heavy, you can also use Wireshark to obtain network packets for a period of time for traffic analysis.
2. Troubleshooting: Check whether the processes are malicious and resolve the issue accordingly.
   - If the processes are desired, optimize them or modify HECS configurations.
   - If the processes are malicious, use a third-party tool to automatically stop the processes.

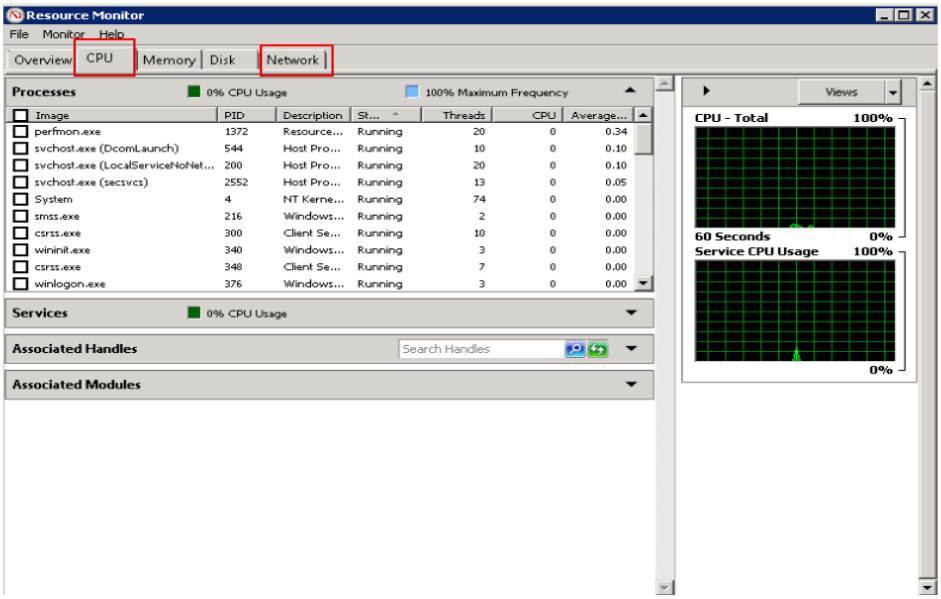
Locating the Fault

1. In the lower left corner of the HECS desktop, choose **Start** > **Run**.
2. In the **Open** dialog box, enter **perfmon -res**.



 Copyright © Huawei Technologies Co., Ltd.

3. On the **Resource Monitor** page, click the **CPU** or **Network** tab to view the CPU or bandwidth usage.



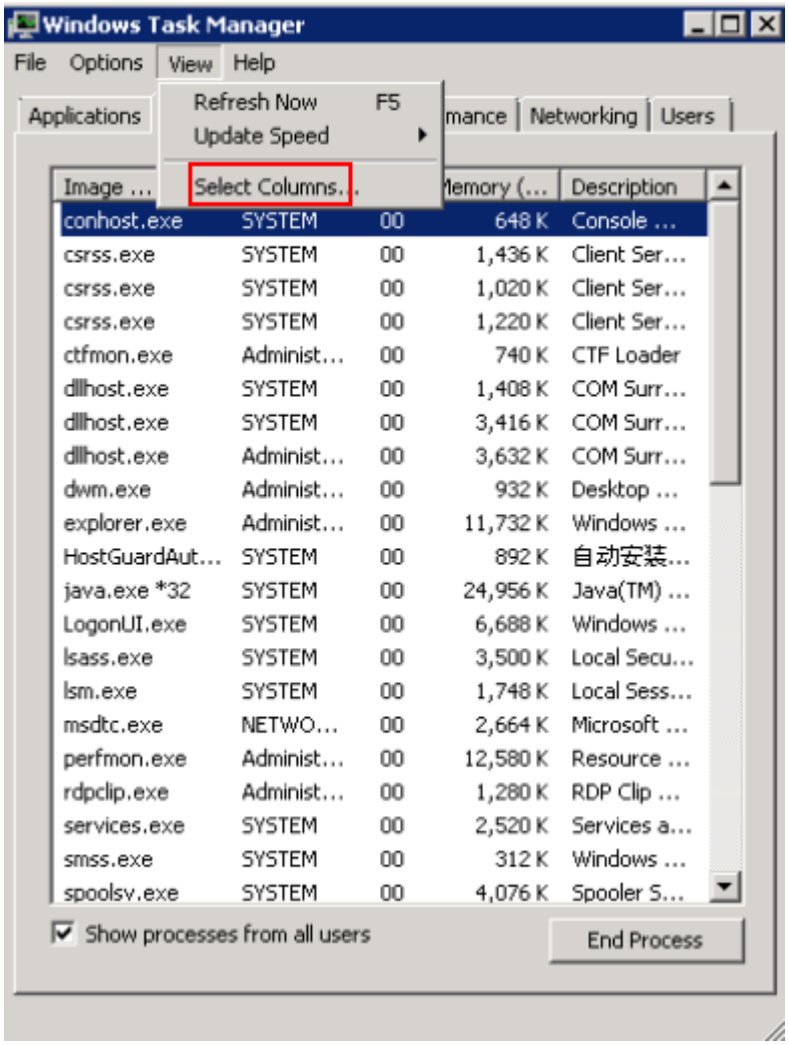
4. Obtain the IDs and names of the processes with high CPU or bandwidth usage.
5. Press **Ctrl+Alt+Delete** to start Windows Task Manager.

   The following describes how to display PIDs in Task Manager, locate a process, and check whether it is malicious.

   a. Click the **Processes** tab.

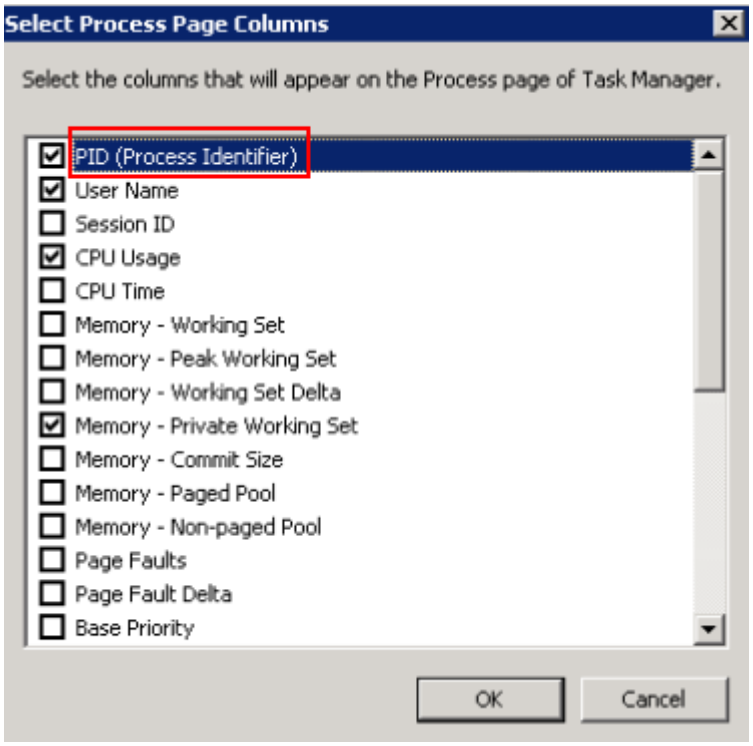
   b. Choose **View** > **Select Columns**.

 Copyright © Huawei Technologies Co., Ltd.



c. Select **PID (Process Identifier)**.

 Copyright © Huawei Technologies Co., Ltd.



d. Click **OK**.

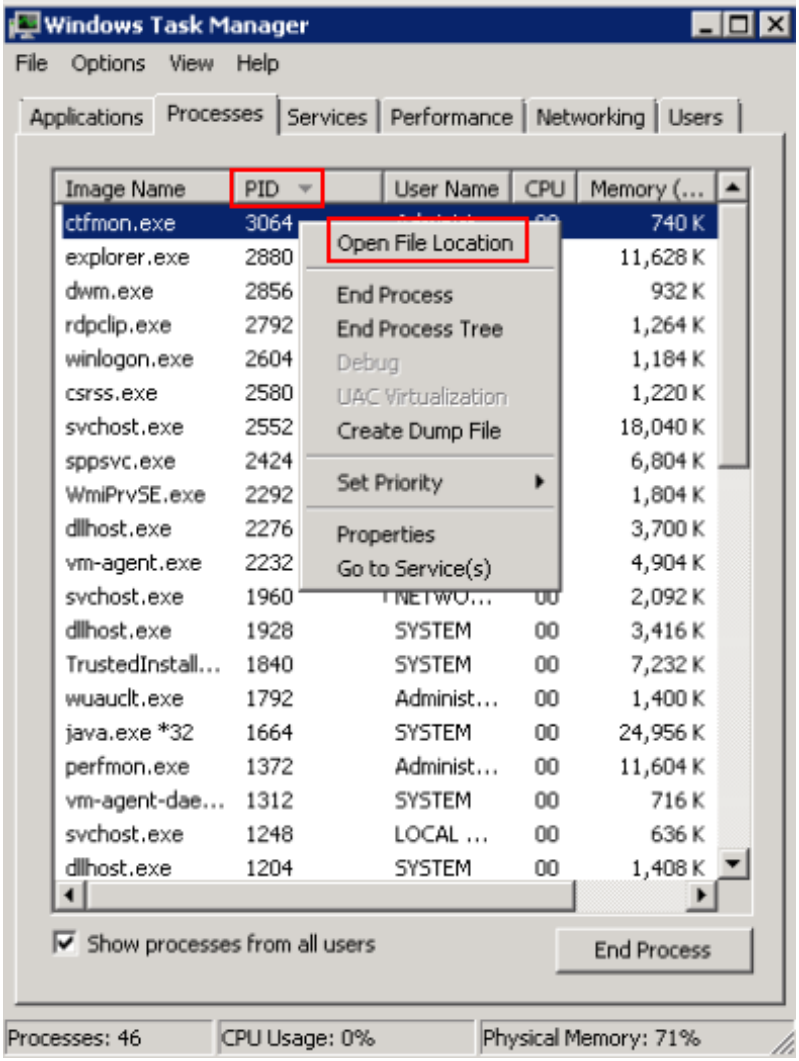
   On the **Processes** tab, the **PID** column is displayed.

e. Click **PID** to sort the data.

f. Right-click a process with high CPU or bandwidth usage and choose **Open File Location** from the shortcut menu.

g. Check whether the process is malicious.

 Copyright © Huawei Technologies Co., Ltd.



Solution

Before troubleshooting, determine whether the process causing high CPU or bandwidth usage is malicious, and take measures accordingly.

Suggestions for non-malicious processes

1. If your HECS runs Windows Server 2008 or 2012, ensure that the available memory capacity is 2 GB or higher.
2. Check whether Windows Update is running on the backend.
3. Check whether antivirus software is scanning on the backend.
4. Check whether applications running on the HECS have high requirements on the network and CPU. If yes, change the bandwidth.
5. If the HECS configuration meets application requirements, deploy applications separately. For example, deploy the database and applications separately.

Suggestions for malicious processes

If the high CPU or bandwidth usage is due to viruses or Trojan horses, manually stop the affected processes. The recommended processing sequence is as follows:

 Copyright © Huawei Technologies Co., Ltd.

1. Use commercial-edition antivirus software or install Microsoft Safety Scanner to scan for viruses in security mode.
2. Install the latest patches for Windows.
3. Run **MSconfig** to disable all drivers that are not delivered with Microsoft and check whether the fault is rectified. For details, see How to perform a clean boot in Windows.
4. If the HECS or site encounters a DDoS or CC attack, which causes a large number of access requests within in a short period of time, log in to the management console and perform the following operations:
   - Check whether Anti-DDoS has been enabled and whether the protection rules are appropriate. To configure a protection rule, see Enabling Anti-DDoS.
   - Check whether CC attack protection has been enabled and whether the protection rules are appropriate. To configure a protection rule, see Configuring CC Attack Protection Rules.

9.2 Why Is My Linux HECS Running Slowly?

If your Linux HECS runs slowly or is unexpectedly inaccessible, the bandwidth or CPU usage of the HECS may be excessively high. If you have created an alarm rule using Cloud Eye, the system automatically sends you an alarm when the bandwidth or CPU usage reaches the threshold specified in the rule.

To resolve this issue, perform the following operations:

1. Fault locating: identifies the processes leading to high bandwidth or CPU usage.
2. Troubleshooting: Check whether the processes are malicious and resolve the issue accordingly.
   - If the processes are desired, optimize them or modify HECS configurations.
   - If the processes are malicious, use a third-party tool to automatically stop the processes or manually stop them.

Common Commands

The following uses the CentOS 7.2 64bit OS as an example to describe common commands. The commands may vary depending on Linux OS editions. For details, see the official documentation for the specific OS edition.

The common commands for checking Linux HECS performance metrics, such as CPU usage, are as follows:

- **ps -aux**
- **ps -ef**
- **top**

Locating High CPU Usage

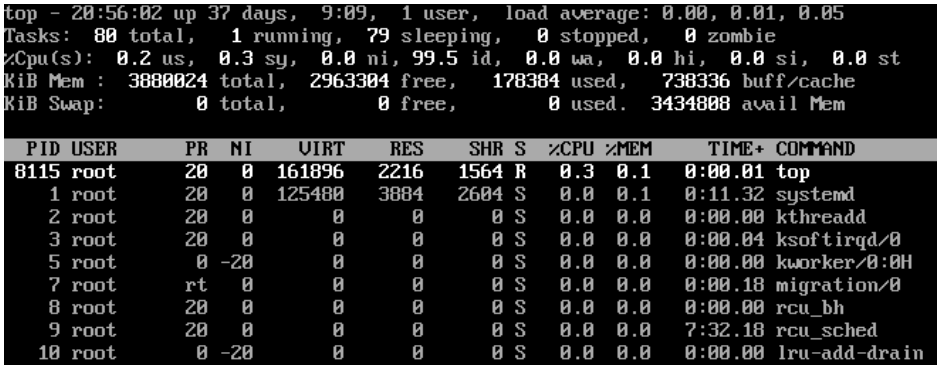
1. Remotely log in to the HECS.
2. Run the following command to check the OS running status:

   top

   Information similar to the following is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-1 Command output



3. View the command output.
   - The first line in the command output is "20:56:02 up 37 days, 1 user, load average: 0.00, 0.01, 0.05", indicating that:

     The current system time is 20:56:02; the HECS has been running for 37 days; there is one login user; the last three values indicate the average CPU load in the last 1 minute, 5 minutes, and 15 minutes, respectively.
   - The third line in the command output shows the overall CPU usage.
   - The fourth line in the command output shows the overall memory usage.
   - The lower part of the command output shows the resource usage of each process.

NOTE

1. On the **top** page, enter **q** or press **Ctrl+C** to exit.
2. Alternatively, click **Input Command** in the upper right corner of the VNC login page, paste or enter commands in the displayed dialog box, and click **Send**.
3. Common parameters in top commands are as follows:

   s: Change the image update frequency.

   l: Show or hide the first line for the top information.

   t: Show or hide the second line for tasks and the third line for CPUs.

   m: Show or hide the fourth line for Mem and the fifth line for Swap.

   N: Sort processes by PID in ascending or descending order.

   P: Sort processes by CPU usage in ascending or descending order.

   M: Sort processes by memory usage in ascending or descending order.

   h: Show help for commands.

   n: Set the number of processes displayed in the process list.

4. Run the **ll /proc/***PID*/**exe** command to obtain the program file specified by a progress ID.



Troubleshooting High CPU Usage

If the processes leading to high CPU usage are malicious, run the **top** command to stop them. If the **kswapd0** process leads to high CPU usage, optimize the program for the process or upgrade the HECS specifications for a larger memory capacity.

kswapd0 is a virtual memory management process. When the physical memory becomes insufficient, **kswapd0** runs to allocate disk swap capacity for caching. This uses a large number of CPU resources.

 Copyright © Huawei Technologies Co., Ltd.

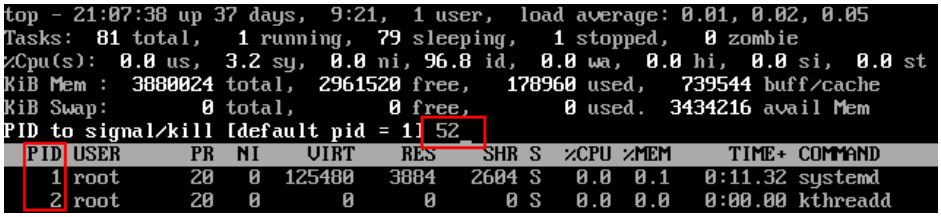
- For detected malicious processes

  Quickly stop such processes on the top page. To do so, perform the following operations:

  a. Press the **k** key during the execution of the **top** command.

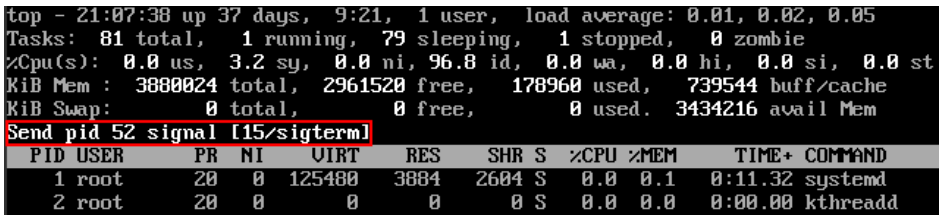
  b. Enter the PID of the process to be stopped.

     The PID of the process is the value in the first column of the **top** command output. For example, to stop the process with PID 52, enter **52** and press **Enter**.



  c. After the operation is successful, information similar to the following is displayed. Press **Enter**.

     Figure 9-2 Example of a successful operation

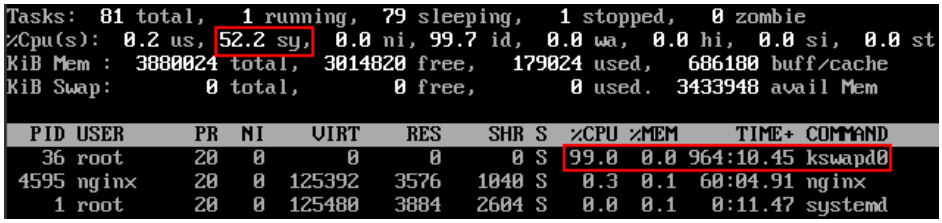


- For the **kswapd0** process

  To check the memory usage of a process, perform the following operations:

  a. Run the **top** command to check the resource usage of the **kswapd0** process.

  b. If the process remains in non-sleeping state for a long period of time, you can preliminarily determine that the system is consistently paging. In such a case, the high CPU usage is caused by insufficient memory.



  c. Run the **vmstat** command to check the virtual memory usage of the system.

     If the **si** and **so** values are large, the system is frequently paging and the physical memory of the system is insufficient.

     - **si**: volume of data written from the swap partition to the memory per second, which is transferred from the disk to the memory.
     - **so**: volume of data written from the memory to the swap partition per second, which is transferred from the memory to the disk.

  d. Further identify the causes of high memory usage. Run commands, such as **free** and **ps** to check the memory usage of the system and processes in the system.

  e. Restart the application or release the memory when traffic is light.

 Copyright © Huawei Technologies Co., Ltd.

To handle this issue, expand the HECS memory. If memory expansion is not allowed, optimize the application and enable hugepage memory.

Handling High Bandwidth Usage

If the high bandwidth usage is caused by normal service access of non-malicious processes, enlarge the bandwidth to handle this issue. If the high bandwidth usage is caused by abnormal service access, for example, malicious access from certain IP addresses, CC attacks on the HECS, or malicious processes, use the traffic monitoring tool **nethogs** to monitor the bandwidth usage of each process in real time and identify faulty processes.

- Using **nethogs** for troubleshooting
  a. Run the following command to install **nethogs**:

     yum install nethogs -y

     After the installation, run the **nethgos** command to check bandwidth usage.

     Parameters in the **nethogs** command are as follows:

     - **-d**: sets the update interval in the unit of second. The default value is **1**.
     - **-t**: enables tracing.
     - **-c**: sets the number of updates.
     - **device**: sets the NIC to be monitored. The default value is **eth0**.

     The following parameters are involved in command execution:

     - **q**: exits **nethogs**.
     - **s**: sorts processes in the process list by TX traffic in ascending or descending order.
     - **r**: sorts processes in the process list by RX traffic in ascending or descending order.
     - **m**: switches the display unit in the sequence of KB/s, KB, B, and MB.

  b. Run the following command to check the bandwidth usage of each process on the specified NIC:

     nethogs *eth1*

     The parameters in the command output are as follows:

     - **PID**: ID of the process.
     - **USER**: user who runs the process.
     - **PROGRAM**: IP addresses and port numbers of the process and connection, respectively. The former is for the server and the latter is for the client.
     - **DEV**: network port to which the traffic is destined.
     - **SENT**: volume of data sent by the process per second.
     - **RECEIVED**: volume of data received by the process per second.

  c. Stop malicious programs or blacklist malicious IP addresses.

     To stop a malicious process, run the **kill** *PID* command.

     To blacklist a malicious IP address or limit its rate, use iptables.

- Using Web Application Firewall (WAF) to protect the HECS against CC attacks

 Copyright © Huawei Technologies Co., Ltd.

If your HECS has encountered a CC attack, enable CC security protection on the WAF console. For instructions on how to use WAF, see Configuring CC Attack Protection Rules.

 Copyright © Huawei Technologies Co., Ltd.

10 Change History

Released On	Description
2021-01-08	This issue is the sixth official release. • Added 8.1 Resetting the Password for Logging In to a Windows HECS Without Password Reset Plug-ins Installed. • Added 8.2 Resetting the Password for Logging In to a Linux HECS Without Password Reset Plug-ins Installed.
2020-11-19	This issue is the fifth official release. • Added 1.5 Why Does the Console Display a Message Indicating that the Agent Is Not Installed? • Added screenshots in 4.4 Why Can't I Log In to My Windows HECS?, 4.5 Why Can't I Log In to My Linux HECS?, and 5.1 Why Can't an EIP Be Pinged?. • Added a video tutorial link in 4.6 How Can I Enable Multi-User Login on a Windows HECS?.
2020-07-13	This issue is the fourth official release. • Added the procedure for checking the IP address whitelist for SSH logins and the procedure for checking the firewall configuration in 4.4 Why Can't I Log In to My Windows HECS?. • Added the procedure for checking the IP address whitelist for SSH logins and the procedure for checking the firewall configuration in 4.5 Why Can't I Log In to My Linux HECS?. • Added the link to "Troubleshooting a Browser Launch Error Occurred in Multi-User Login" in 4.6 How Can I Enable Multi-User Login on a Windows HECS?. • Added the procedure for checking network ACLs in 5.1 Why Can't an EIP Be Pinged?.
2020-04-30	This issue is the third official release. • Added 5.2 Why Is Outbound Access Through TCP Port 25 Restricted?
2020-02-19	This issue is the second official issue.

 Copyright © Huawei Technologies Co., Ltd.

Released On	Description
	• Added 1.3 What Are the HECS Performance Metrics? • Added 1.4 Why Is My HECS Not Displayed on the Management Console? • Added 7.5 What Are the Restrictions on Attaching an EVS Disk to an HECS?
2020-02-06	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.