Elastic Cloud Server

FAQs

Issue	01
Date	2025-11-18

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

Contents

1 Common FAQ

Remote Login

- Can I Troubleshoot ECSs By Myself?
- Why Can't I Log In to My Windows ECS?
- Why Can't I Log In to My Linux ECS?
- What Are the Username and Password for Remote Logins?
- Troubleshooting Multi-User Logins
- Applying for a License for Authenticating Multi-User Sessions and Activating the ECS

ECS Failures or Slow ECS Responses

- Why Is My Windows ECS Running Slowly?
- Why Is My Linux ECS Running Slowly?
- How Do I Know If My EIP Bandwidth Limit Has Been Exceeded?

Website or Application Access Failures

- How Do I Troubleshoot an Unresponsive Website Hosted on My ECS?
- How Do I Troubleshoot Slow Connections to a Website Hosted on My ECS?
- Why Am I Unable to Connect to a Port on an ECS?

Internet Access Failures

- Why Cannot My Windows ECS Access the Internet?
- Why Does My Linux ECS Fail to Access the Internet?
- Can an ECS Without an EIP Bound Access the Internet?
- Why Accessing a Website Outside the Chinese Mainland Is Slow on an ECS?
- How Do I Troubleshoot a Ping Failure or Packet Loss Using a Link Test?

Passwords and Key Pairs

- **Resetting the Password for Logging In to an ECS on the Management Console**

Ping Failures

- **What Should I Do If an EIP Cannot Be Pinged?**
- **Why Can I Remotely Access an ECS But Cannot Ping It?**
- **How Do I Troubleshoot a Ping Failure or Packet Loss Using a Link Test?**

2 Product Consulting

2.1 What Are the Precautions for Using ECSs?

- Do not upgrade ECS kernel or OS versions. If you want to upgrade the main OS version, for example, from CentOS 7.2 to Cent OS 7.3, use the provided OS changing function.
- Do not uninstall the performance optimization software pre-installed on your ECSs.
- Do not change NIC MAC addresses. Otherwise, the network connection will fail.

2.2 What Can I Do with ECSs?

You can use ECSs just like traditional physical servers. On an ECS, you can deploy any service application, such as an email system, web system, and Enterprise Resource Planning (ERP) system.

After creating an ECS, you can use it like using your local computer or physical server.

2.3 What Are Kunpeng and x86 CPU Architectures?

ECS supports the following architectures:

- x86 architecture

  The x86 architecture uses the complex instruction set computer (CISC). CISC is a computer architecture in which single instructions can execute several low-level operations. There are a large number of instructions, each with different lengths. CISC processors take longer time to execute instructions because they have more complex instructions.
- Kunpeng architecture

  The Kunpeng architecture uses the reduced instruction set computer (RISC). RISC is a microprocessor architecture with a simple collection and highly customized set of instructions. It is built to minimize the instruction execution time by optimizing and limiting the number of instructions.

The Kunpeng architecture provides a better balance between performance and power consumption than the x86 architecture.

2.4 Xen ECS EOS

1. **Why will Xen ECSs be EOS?**

   Since all versions of the Xen virtualization platform used by Huawei Cloud have been reached end of service (EOS), Huawei Cloud cannot obtain patch updates or community support. After detecting new security risks, Huawei Cloud cannot provide patches and technical support for users, which is risky to user services. Therefore, Xen ECSs on Huawei Cloud are EOS accordingly.

2. **What are the impacts if I continue to use Xen ECSs?**
   - After the Xen virtualization platform is EOS, Huawei Cloud cannot provide patch updates and technical support for newly detected security risks. As a result, security risks may occur in user services.
   - New disks and NICs cannot be attached to existing Xen ECSs when the ECSs are running.
   - The backups of an existing Xen ECS cannot be used to create Xen ECSs, and the KVM ECSs created using a Xen ECS backup cannot be started.

3. **Which virtualization platform will be used to replace Xen?**

   Huawei Cloud will use KVM to replace Xen. Compared with Xen, KVM provides more functions, better stability, and higher performance. KVM ECSs surpass Xen ECSs in:
   - Fault detection
   - Live migration
   - Remote high availability (HA)

   KVM can better meet the cloud computing requirements. The majority of users are using KVM, and most Xen users have switched from Xen to KVM.

4. **What should I do with my existing Xen ECSs?**

   Change a Xen ECS to a KVM ECS by modifying specifications on the ECS console.

5. **Will the price remain unchanged after I change a Xen ECS to a KVM ECS?**

   Modifying specifications will change how much you need to pay for the ECS. For details, see **Pricing of a Changed Specification**.

6. **Which ECSs require specifications modification?**
   - C1, C2, M1, and S1 Xen ECSs require specifications modification. **Table 2-2** lists recommended KVM flavors. Select target ECS flavors by region.
   - To ensure proper running of SAP services, the SUSE-based large-memory ECSs for SAP certification, including H1, E1, E2, and ET2 ECS series, are not included in this specifications modification.
   - GPU-accelerated G1 ECSs are not included in this specifications modification.

Table 2-1 Xen ECS series

Requiring Specifications Modification				Not Requiring Specifications Modification				
C1	C2	M1	S1	H1	E1	E2	ET2	G1

Table 2-2 Recommended KVM flavors

Source Xen Flavor	Target KVM Flavor (Recommended 1)	Target KVM Flavor (Recommended 2)
c1.medium	s3.small.1	s6.small.1
c1.large	s3.large.2	s6.large.2
c1.xlarge	s3.xlarge.2	s6.xlarge.2
c1.2xlarge	s3.2xlarge.2	s6.2xlarge.2
c1.4xlarge	s3.4xlarge.2	N/A
c1.8xlarge	c3.8xlarge.2	c6.8xlarge.2
c2.medium	s3.medium.2	s6.medium.2
c2.large	s3.large.2	s6.large.2
c2.xlarge	s3.xlarge.2	s6.xlarge.2
c2.2xlarge	s3.2xlarge.2	s6.2xlarge.2
c2.4xlarge	s3.4xlarge.2	N/A
c2.8xlarge	c3.8xlarge.2	c6.8xlarge.2
m1.medium	m3.large.8	m6.large.8
m1.large	m3.large.8	m6.large.8
m1.xlarge	m3.xlarge.8	m6.xlarge.8
m1.2xlarge	m3.2xlarge.8	m6.2xlarge.8
m1.4xlarge	m3.4xlarge.8	m6.4xlarge.8
s1.medium	s3.medium.4	s6.medium.4
s1.large	s3.large.4	s6.large.4
s1.xlarge	s3.xlarge.4	s6.xlarge.4
s1.2xlarge	s3.2xlarge.4	s6.2xlarge.4
s1.4xlarge	s3.4xlarge.4	N/A
s1.8xlarge	c3.8xlarge.4	c6.8xlarge.4

7. **How does the change from a Xen ECS to a KVM ECS affect services?**
   - Before changing a Xen ECS to a KVM ECS, stop the ECS, which will interrupt services running on the ECS. After the change is complete, start the ECS to restore service running.
   - After the change is complete, the underlying virtualization platform is changed from Xen to KVM, which does not affect services.
8. **How can I change a Xen ECS to a KVM ECS?**

   Before changing a Xen ECS to a KVM ECS, manually install desired drivers on the ECS. If there are no drivers installed on the ECS, the ECS will be unavailable (the OS cannot be started) after the specifications are modified. After drivers are installed, do as follows:
   - **Windows**
     i. Create a system disk snapshot.
     ii. Check the UVP VMTools version.
     iii. Install or upgrade UVP VMTools.
     iv. Modify specifications.
     v. Check disk attachment.

     For details, see **Changing a Xen ECS to a KVM ECS (Windows)**.
   - **Linux**

     For Linux, you are advised to use a script to automatically install desired drivers for specifications modification.
     - Using a script for automatic driver installation
       1) Create a system disk snapshot.
       2) Use a script to automatically install drivers.
       3) Modify specifications.
       4) Check disk attachment.

       For details, see **Automatically Changing a Xen ECS to a KVM ECS (Linux)**.
     - Manually installing drivers
       1) Create a system disk snapshot.
       2) Install drivers.
       3) Verify the ECS configuration.
       4) Modify specifications.
       5) Check disk attachment.

       For details, see **Manually Changing a Xen ECS to a KVM ECS (Linux)**.

2.5 Technical Support for Third-Party Software Used on ECSs

Dear Huawei Cloud users,

Huawei Cloud provides technical support for certain third-party software to improve product serviceability.

NOTE

Basic support plans do not cover third-party software. For details, see **Support Plans**.

Technical support includes providing suggestions on installing, configuring, and troubleshooting the following third-party software on ECSs:

- Web services
  - Apache
  - IIS
  - Nginx
- Database services
  - MySQL
  - Microsoft SQL Server
- Network security services
  - Linux Iptables
  - Windows firewall
- Other network services
  - SSH and Windows remote and routing access
  - SFTP and FTP
  - OpenVPN
  - DNS

The suggestions provided by the Huawei Cloud service team on the third-party software are dedicated for experienced system administrators or IT personnel. The Huawei Cloud service team is not responsible for installing and debugging the preceding third-party software, implementing the suggestions, or resolving the issues caused by the preceding services. The description is as follows:

Huawei provides suggestions or assists you in troubleshooting in the following:

- Web services: port connection failures and access issues with error code 4xx
- Database services: remote connection failures and changing listening ports
- Firewall services: adding rules to Iptables and firewalls and opening ports
- Network services: SSH or Windows remote connection failures
- DNS: basic Linux DNS configurations

You are responsible for configuring, troubleshooting, and optimizing services in the following scope:

- Web services: optimizing configurations, editing pseudo-static rules, and debugging plug-ins
- Database services: optimizing databases and SQL statements
- Firewall services: constructing Iptables-based automatic detection and defense tools

- Network services: improving SSH file transfer rate and limiting SFTP-based file transfer rate
- OpenVPN services: interconnecting multiple OpenVPNs
- DNS services: planning Linux DNS networking and optimizing network configurations

3 ECS Creation

3.1 What Can I Do If I Cannot Find My ECSs?

Symptom

You cannot find your purchased ECSs after logging in to the console.

Possible Causes

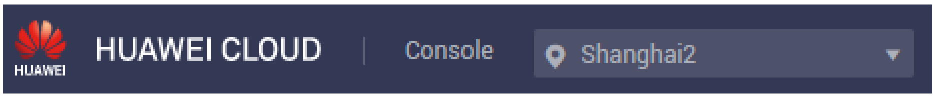
- The ECSs are not in the selected region.
- The yearly/monthly ECSs have expired, or the pay-per-use ECSs have been deleted due to arrears.

Solution

Method 1: Change the region.

1. Log in to the **management console**.
2. Select the region in which you created your ECS.

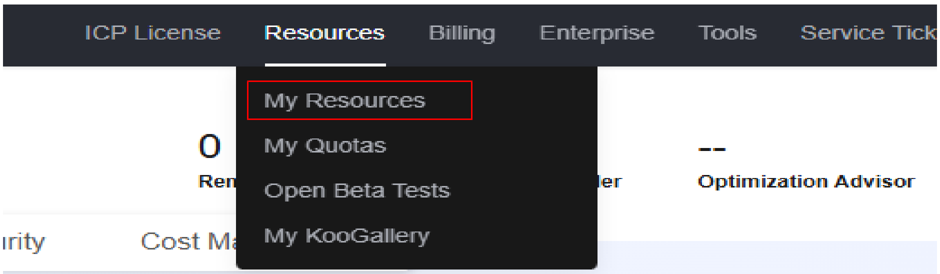
Figure 3-1 Changing a region on the management console homepage



Method 2: View resource details on the My Resources page.

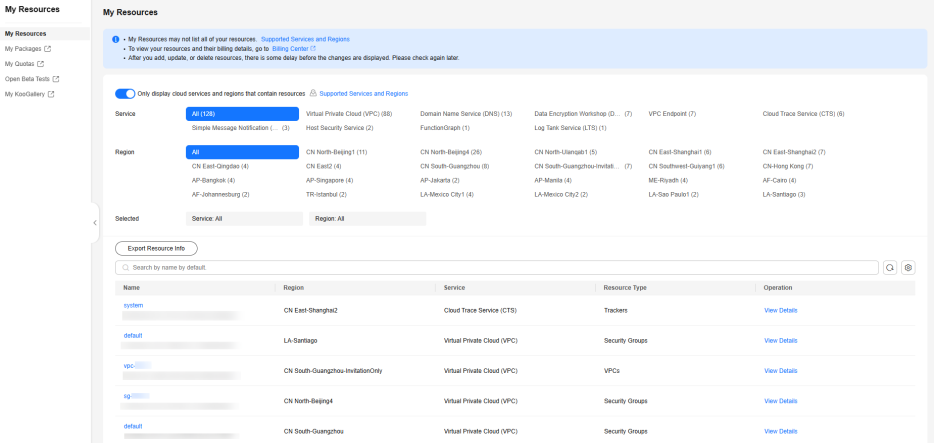
1. Log in to the **management console**.
2. On the right of the top navigation bar of the management console, choose **Resources** > **My Resources**.

Figure 3-2 My Resources



3. On the **My Resources** page, view resource details.
   - Click a resource type to display all resources of the resource type in the list.
   - Click a region to view all resources in the region.

Figure 3-3 Resource list



- My Resources may not list all of your resources. Supported Services and Regions
- To view your resources and their billing details, go to Billing Center
- After you add, update, or delete resources, there is some delay before the changes are displayed. Please check again later.

Name	Region	Service	Resource Type	Operation
system [redacted]	CN East-Shanghai2	Cloud Trace Service (CTS)	Trackers	View Details
default [redacted]	LA-Santiago	Virtual Private Cloud (VPC)	Security Groups	View Details
vpc-[redacted] [redacted]	CN South-Guangzhou-InvitationOnly	Virtual Private Cloud (VPC)	VPCs	View Details
sg-[redacted] [redacted]	CN North-Beijing4	Virtual Private Cloud (VPC)	Security Groups	View Details
default [redacted]	CN South-Guangzhou	Virtual Private Cloud (VPC)	Security Groups	View Details

Method 3: View historical resources in Billing Center.

This method is used only to view historical resources that have been unsubscribed from or deleted. For unsubscribed or deleted resources, if they are not backed up, their data cannot be restored.

- Yearly/Monthly resources
  a. Log in to the **Billing Center console**.
  b. In the navigation pane on the left, choose **Orders** > **My Orders**.
  c. On the **My Orders** page, view yearly/monthly resources.
     You can filter resources by time period, product type, or order number.
- Pay-per-use resources
  a. Log in to the **Billing Center console**.
  b. In the navigation pane on the left, choose **Billing** > **Bill Details**.
  c. Set **Data Period** to **Details** to view pay-per-use resources.
     You can filter resources using attributes in the search box.

3.2 What Should I Do If the ECS Resources to Be Purchased Are Sold Out?

When you are purchasing ECSs, the selected specifications may be sold out. In this case, the specifications cannot be purchased in the current region or AZ.

Instance specifications vary in different regions and AZs. For sold-out resources, you are advised to:

- Switch to another AZ to purchase the resources.
- In the specifications list, click the region where the sold-out resources are available and switch to the target region to purchase resources.

3.3 How Can I Set Sequential ECS Names When Creating Multiple ECSs?

Scenarios

When creating multiple ECSs at the same time, you can use either of the following methods to sequentially name the ECSs:

- Automatic naming: The system automatically numbers ECSs with a four-digit suffix in ascending order.
- Custom naming: You can create a custom naming rule using the format "name_prefix[begin_number,bits]name_suffix". The system will name the ECSs based on the rule you specify.

This section describes how to use the two methods to name ECSs.

Automatic Naming

You can customize ECS names based on the following rule: 1 to 64 characters, only containing letters, digits, underscores (_), and hyphens (-).

When you create multiple ECSs at a time, the system automatically numbers these ECSs with a four-digit suffix in ascending order. In this case, the name is 1 to 59 characters long. For example, if you are creating multiple ECSs and enter **ecs** for the ECS name, the created ECSs will be named **ecs-0001**, **ecs-0002**, and so on. If you create multiple ECSs again, the values in the new ECS names increase from the existing maximum value. For example, the existing ECS with the maximum number in name is **ecs-0010**. If you enter **ecs**, the names of the new ECSs will be **ecs-0011**, **ecs-0012**, ... When the value reaches **9999**, it will start from **0001**.

Allow duplicate name: allows ECS names to be duplicate. If you select **Allow duplicate name** and create multiple ECSs in a batch, the created ECSs will have the same name.

- Example 1: If there is no existing ECS and you enter **ecs-f526**, the ECSs will be named **ecs-f526-0001**, **ecs-f526-0002**, **ecs-f526-0003**, ...

- Example 2: If there is an ECS named **ecs-f526-0010** and you enter **ecs-f526**, the ECSs will be named **ecs-f526-0011**, **ecs-f526-0012**, **ecs-f526-0013**, ...
- Example 3: If there is an ECS named **ecs-0010** and you select **Allow duplicate ECS name**, all the ECSs will be named **ecs-0010**.

Custom Naming

You can create a custom naming rule using the format "name_prefix[begin_number,bits]name_suffix". The system will automatically name the ECSs based on the rule you specify.

Field Description for a Custom Naming Rule

Figure 3-4 shows the format of a custom naming rule.

Figure 3-4 Format of a custom naming rule

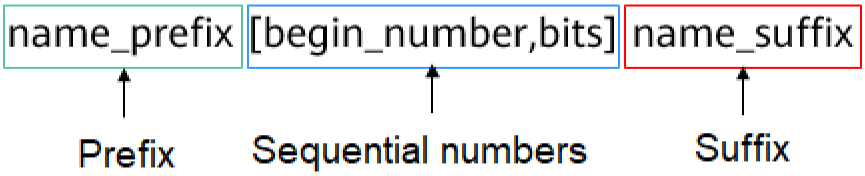


Table 3-1 describes these parameters.

Table 3-1 Parameters in a custom naming rule

Field	Mandatory	Description	Example
name_prefix	Yes	ECS name prefix The name prefix can contain only letters, digits, underscores (_), and hyphens (-).	ecs
[begin_number,bits]	Yes	Sequence numbers that increase in ascending order to differentiate multiple ECSs.	[0,4]
name_suffix	No	ECS name suffix The name suffix can contain only letters, digits, underscores (_), and hyphens (-).	f526

Table 3-2 [begin_number,bits] parameters

Field	Mandatory	Description	Example
begin_number	No	Begin number of ECS names. The begin number ranges from 0 to 9999. The default value is **0**.	0
bits	No	Number of bits for the sequential numbers in ECS names. The value ranges from 1 to 4. The default value is **4**.	4

Notes on Using the Custom Naming Rule

- Custom names cannot be duplicate.
- No space is allowed in [begin_number,bits].
- If the bits of "Begin number + Number of ECSs to be created - 1" is greater than the specified bits, the bits of "Begin number + Number of ECSs to be created - 1" will be used.

  For example, if [begin_number,bits] is set to [8,1] and the number of ECSs to be created is 2, the bits of "Begin number + Number of ECSs to be created - 1" is the same as the specified bits (1). Then, the ECSs will be named *name_prefix***8***name_suffix* and *name_prefix***9***name_suffix*.

  If [begin_number,bits] is set to [8,1] and the number of ECSs to be created is 3, the specified bits is 1, the bits of "Begin number + Number of ECSs to be created - 1" (value 10, bits 2) is different from the specified bits (1). Therefore, the bits of "Begin number + Number of ECSs to be created - 1" will be used, which is 2.

  The ECSs will be named *name_prefix***08***name_suffix*, *name_prefix***09***name_suffix*, and *name_prefix***10***name_suffix*.
- If the value of "Begin number + Number of ECSs to be created" is greater than the maximum value **9999**, the sequential numbers that exceed **9999** will consistently to be **9999**.
- If [begin_number,bits] is set to [] or [,], the begin number starts from **0**, and the number of bits is **4** by default.
- If [begin_number,bits] is set to [99] or [99,], the begin number starts from **99**, and the number of bits is **4** by default.

Custom Naming Examples

- Example 1: If you select custom naming and enter *name_prefix***[,]***name_suffix*.

  The ECSs will be named *name_prefix***0000***name_suffix*, *name_prefix***0001***name_suffix*, *name_prefix***0002***name_suffix*, ...
- Example 2: If you select custom naming and enter *name_prefix***[]***name_suffix*.

The ECSs will be named *name_prefix***0000***name_suffix*, *name_prefix***0001***name_suffix*, *name_prefix***0002***name_suffix*, ...

- Example 3: If you select custom naming and enter *name_prefix***[9,]***name_suffix*:

  The ECSs will be named *name_prefix***0009***name_suffix*, *name_prefix***0010***name_suffix*, *name_prefix***0011***name_suffix*, ...

- Example 4: If you select custom naming and enter *name_prefix***[,3]***name_suffix*:

  The ECSs will be named *name_prefix***000***name_suffix*, *name_prefix***001***name_suffix*, *name_prefix***002***name_suffix*, ...

- Example 5: If you select custom naming and enter *name_prefix***[8]***name_suffix*:

  The ECSs will be named *name_prefix***0008***name_suffix*, *name_prefix***0009***name_suffix*, *name_prefix***0010***name_suffix*, ...

- Example 6: If you select custom naming and enter *name_prefix***[9999]***name_suffix*:

  All the ECSs will be named *name_prefix***9999***name_suffix*.

- Example 7: If you select custom naming and enter *name_prefix***[8]**:

  The ECSs will be named *name_prefix***0008**, *name_prefix***0009**, *name_prefix***0010**, ...

3.4 What Is the Creation Time and Launch Time of an ECS?

Creation time: time when the ECS is created on the cloud platform.

Launch time: time when the ECS is launched for the first time.

After purchasing an ECS, you can click the ECS name on the list page and view the creation time and launch time in the **ECS Information** area.

3.5 Why Does the Failures Area Show an ECS Creation Failure But the ECS List Displays the Created ECS?

Symptom

When you attempt to create an ECS with an EIP bound on the management console, the ECS creation was successful but the EIP binding failed due to insufficient EIPs. Although the **Failures** area showed that the ECS creation failed, the ECS was displayed in the ECS list. The results of the ECS creation task were inconsistent.

Root Cause

- The ECS list displays created ECSs.
- The **Failures** area shows the ECS creation status, including the statuses of subtasks, such as creating ECS resources and binding an EIP. Only when all subtasks are successful, the ECS is created.

If the ECS is created but EIP binding failed, the task failed. However, the ECS you created is temporarily displayed in the list. After the system rolls back, the ECS is removed from the list.

3.6 When Does an ECS Become Provisioned?

The methods of provisioning ECSs vary depending on the billing mode.

- Yearly/Monthly ECSs: After you pay for an ECS and the system applies charges, the ECS is automatically provisioned.
- Pay-per-use ECSs: An ECS is automatically provisioned after it is created.

3.7 Why Cannot I View the ECSs Being Created Immediately After I Pay for Them?

You can view the ECSs being created only after the system disks attached to the ECSs are created. This requires a period of time.

3.8 What Should I Do If the ECS Fails to Be Provisioned After I Have Paid the Order?

After you have paid the order, if an SMS message is sent to your mobile phone indicating that the ECS fails to be provisioned, contact customer service of HUAWEI CLOUD at 4000-955-988. The customer service team will help you rectify the failure and provision the required ECS for you. If the failure cannot be rectified within the required time period, you can cancel the order and the customer service will refund the price you have paid to your account.

3.9 Why Does It Take Longer to Create ECSs When I Use a Full-ECS Image?

Symptom

When you use a full-ECS image that was created using a CSBS backup to create ECSs, the process is time-consuming or the system displays a message indicating that the image cannot be used to rapidly create ECSs.

Cause Analysis

If your full-ECS image is in the old backup format provided by CSBS, this issue occurs.

NOTE

- CSBS has a new backup format. You can rapidly create ECSs if the full-ECS image is in this format.

Solution

If you want to use a full-ECS image to rapidly create ECSs, ensure that the full-ECS image is created using a CSBS backup in the new format. The procedure is as follows:

- Scenario 1: The ECS based on which the target CSBS backup is created is available.

  Back up the original ECS on the **Cloud Server Backup Service** page and use the new format to create a full-ECS image. You can use the full-ECS image to rapidly create ECSs.

  - For instructions about how to back up an ECS, see *Cloud Server Backup Service User Guide*.
  - For instructions about how create a full-ECS image, see *Image Management Service User Guide*.
- Scenario 2: The ECS based on which the target CSBS backup is created is unavailable.

  a. Use the full-ECS image to create a new ECS.

  b. Back up the newly created ECS.

     For details, see *Cloud Server Backup Service User Guide*.

  c. Use the CSBS backup to create a full-ECS image.

     For details, see *Image Management Service User Guide*.

     You can use the full-ECS image to rapidly create ECSs.

3.10 What Do I Do If I Selected an Incorrect Image for My ECS?

You can change the image for your ECS on the ECS console.

1. Select the target ECS and click **Stop** in the upper left corner of the ECS list.
2. Locate the row that contains the target ECS, choose **More** > **Manage Image** > **Change OS** in the **Operation** column.

   The **Change OS** dialog box is displayed.
3. Select the target image type and image.

   NOTE

   - Only changes between free OSs are supported.
   - If an ECS is created from a private image in KooGallery and is billed on a yearly/monthly basis, the OS cannot be changed.
   - OS change between Windows and Linux is only supported in the Chinese mainland regions.
4. Set the login mode. You can select **Password** or **Key pair**.
5. Set the other parameters and click **OK**.

   After the application is submitted, the ECS status changes to **Changing OS**. When this status disappears, the OS change is complete.

For details, see **Changing the OS**.

3.11 Should I Choose Windows OS or Linux OS for My ECS?

Difference Between Windows OS and Linux OS

The following table shows the difference between Windows OS and Linux OS. Select an OS based on your service requirements.

Table 3-3 Differences

OS	Developer Language	Database
Windows	ASP.NET, MFC and C#	ACCESS and SQL Server
Linux	Shell	MySQL and SQLite
Both Windows and Linux support developer languages HTML, C, Java, and PHP.		

Windows OS

Huawei Cloud supports five versions of Windows OS, each of which is available in 32-bit and 64-bit.

Microsoft has ended support for Microsoft Windows Server 2008 and it is not recommended.

Windows Server 2012, Windows Server 2016, and Windows Server 2019 have some advanced features, such as network performance and system compatibility optimization. For the best performance, Windows Server 2019 is recommended.

Difference Between 32-bit and 64-bit OSs

A 32-bit OS allows you to use up to 4 GB of RAM, while a 64-bit OS supports more.

A 32-bit CPU can process 32-bit data at a time, while a 64-bit CPU can process 64-bit data at a time. Theoretically, the processing speed of a 64-bit CPU is faster than that of a 32-bit CPU, but the actual speed is also affected by the RAM size.

Linux OS

There are a variety of Linux versions. You can select an appropriate version based on your service requirements.

OS Change

If you want to change the OS of your ECS, perform the following operations:

1. Select the target ECS and click **Stop** in the upper left corner of the ECS list.
2. Locate the row that contains the target ECS, choose **More** > **Manage Image** > **Change OS** in the **Operation** column.

The **Change OS** dialog box is displayed.

3. Select the target image type and image.

   NOTE

   - Only changes between free OSs are supported.
   - If an ECS is created from a private image in KooGallery and is billed on a yearly/monthly basis, the OS cannot be changed.
   - OS change between Windows and Linux is only supported in the Chinese mainland regions.

4. Set the login mode. You can select **Password** or **Key pair**.
5. Set the other parameters and click **OK**.

   After the application is submitted, the ECS status changes to **Changing OS**. When this status disappears, the OS change is complete.

For details, see **Changing the OS**.

3.12 How Quickly Can I Obtain an ECS?

Obtaining an ECS can take as little as a few minutes.

The time it takes to obtain an ECS depends on ECS specifications, available resources (such as EVS disks and ECSs), and system load.

NOTE

If it takes a long time to obtain your ECS, contact customer service.

3.13 How Can I Manage ECSs by Group?

You cannot manage ECSs by folders or groups, but you can use tags to organize your ECSs

Tags help you group your ECSs by usage or user.

For more information, see **Tag Management**.

3.14 Why Did I Fail to Configure an Anti-Affinity ECS Group?

When you configure an anti-affinity ECS group during ECS purchase, an error occurred. This may be caused by insufficient resources.

In this case, you can try the following measures:

- Wait for a while and try again.
- Purchase ECSs in small batches.
- Select another AZ with sufficient resources to purchase ECSs.

3.15 How Can I Tune the Local Disk Read IOPS Performance of I9 ECSs?

Performance Tuning Scenarios

Ultra-high I/O ECSs use the QingTian architecture and are equipped with high-performance Non-Volatile Memory Express (NVMe) local disks. Each flavor contains 1 to 12 NVMe local disks.

You are advised to tune the performance for I9 ECSs with 64 vCPUs or more. Performance tuning may have impact on access latency.

You can adjust the number of interrupt aggregations to optimize the performance of i9.16xlarge.4, i9.32xlarge.4, i9.16xlarge.8, and i9.32xlarge.8 ECSs.

Background

Interrupt coalescing optimizes frequent hardware interrupts in computer systems or network devices by aggregating multiple interrupts into a single event. This reduces the CPU overhead for handling interruptions, resulting in better system performance.

Interrupt Coalescing Count is a key parameter in NVMe devices. It refers to the specific number of I/O operations that are accumulated before the device triggers an interrupt. For example, if the **Interrupt Coalescing Count** is **0x0109** (265 in decimal), the device triggers an interrupt after accumulating 265 I/O operations. You can adjust this parameter to balance the interrupt frequency and delay. This is the key in performance tuning.

In practice, a too large or too small value of **Interrupt Coalescing Count** may affect performance. To achieve the optimal performance, you need to consider the hardware configuration (such as vCPUs and storage device load).

- If the value is too small, interrupts are too frequent. This can increase the CPU overhead and reduce system performance.
- If the value is too large, the delay may increase, affecting the response of real-time tasks.

Vendors usually provide a default maximum value for reference. You can adjust the value based on site requirements.

You can use the **nvme set-feature** command to dynamically adjust the **Interrupt Coalescing Count** value based on the hardware configuration and load.

During the tuning, you are advised to use a performance monitoring tool to monitor performance metrics and gradually adjust the value and test the performance to achieve the best results.

Procedure

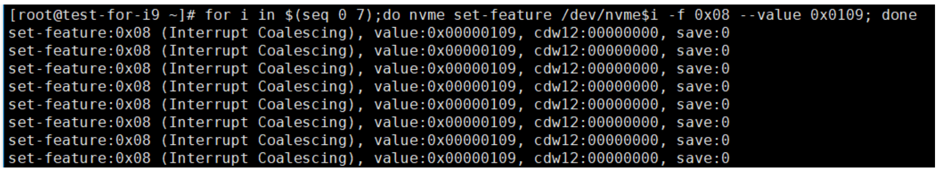
The following uses the i9.32xlarge.4 flavor as an example to describe how to batch tune read IOPS performance for local disks.

1. Log in to the **ECS console** and access the ECS list page.
2. Click 📍 in the upper left corner and select a region and project.
3. Select the ECS you want to log in to and click **Remote Login** in the **Operation** column.

   You can log in using multiple methods. For details, see **Login Overview (Windows)** and **Login Overview (Linux)**.
4. Perform batch interrupt aggregation tuning on local NVMe disks.

```
for i in $(seq 0 7);do nvme set-feature /dev/nvme$i -f 0x08 --value 0x0109; done
```

Figure 3-5 Batch tuning of read IOPS performance for local disks



```
[root@test-for-i9 ~]# for i in $(seq 0 7);do nvme set-feature /dev/nvme$i -f 0x08 --value 0x0109; done
set-feature:0x08 (Interrupt Coalescing), value:0x00000109, cdw12:00000000, save:0
set-feature:0x08 (Interrupt Coalescing), value:0x00000109, cdw12:00000000, save:0
set-feature:0x08 (Interrupt Coalescing), value:0x00000109, cdw12:00000000, save:0
set-feature:0x08 (Interrupt Coalescing), value:0x00000109, cdw12:00000000, save:0
set-feature:0x08 (Interrupt Coalescing), value:0x00000109, cdw12:00000000, save:0
set-feature:0x08 (Interrupt Coalescing), value:0x00000109, cdw12:00000000, save:0
set-feature:0x08 (Interrupt Coalescing), value:0x00000109, cdw12:00000000, save:0
set-feature:0x08 (Interrupt Coalescing), value:0x00000109, cdw12:00000000, save:0
```

Table 3-4 Parameters in the command

Parameter	Description
seq 0 7	Iterates through NVMe device IDs from 0 to 7, which means to tune 8 NVMe devices. If there are 12 NVMe devices, the device IDs are from 0 to 11. Adjust the device ID range based on the site requirements. For details about the number of NVMe devices included in the flavor, see **Ultra-high I/O ECSs**.
/dev/nvme$i	Specifies the (i+1)th NVMe device.
-f 0x08	**0x08**: sets the interrupt aggregation count.
--value 0x0109	Sets the interrupt aggregation count to **0x0109**. This means the device will trigger an interrupt after accumulating 265 I/O operations. **NOTE** **0x0109** is the reference value recommended by the vendor. You can start from the reference value and gradually adjust it to achieve the optimal performance.

4 ECS Deletion and Unsubscription

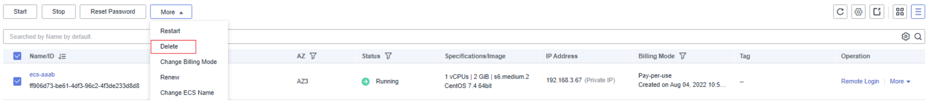
4.1 What Happens After I Click the Delete Button?

After you click **Delete**, the selected ECSs will be deleted. You can also choose to delete the EVS disks and EIPs together with the selected ECSs. If you do not delete them, they will be retained. If necessary, you can manually delete them later.

To delete selected ECSs, perform the following operations:

1. Log in to the **management console**.
2. Click ☰ . Under **Compute**, click **Elastic Cloud Server**.
3. Select the ECSs to be deleted.
4. Above the ECS list, choose **More** > **Delete**.

Figure 4-1 Deleting selected ECSs



Name/ID	AZ	Status	Specifications/Image	IP Address	Billing Mode	Tag	Operation
ecs-aaab ff906d73-be61-4df3-96c2-4f3de233d8d8	AZ3	Running	1 vCPUs | 2 GiB | s6.medium.2 CentOS 7.4 64bit	192.168.3.67 (Private IP)	Pay-per-use Created on Aug 04, 2022 10:5...	--	Remote Login | More

4.2 Can a Deleted ECS Be Provisioned Again?

No. ECSs in the **Deleted** state cannot provide services and are soon removed from the system.

A deleted ECS is retained in the ECS list on the management console only for a short period of time before it is permanently removed from the system.

You can purchase another ECS of the same specifications.

4.3 Can a Deleted ECS Be Restored?

Whether a deleted ECS can be restored depends on whether data backup was enabled for it.

- If backup was enabled, you can use the backup files to restore data.
- If backup was not enabled, data cannot be restored.

Therefore, before deleting an ECS, ensure that the data on the ECS has been backed up or migrated.

4.4 How Do I Delete or Restart an ECS?

Deleting an ECS

1. Log in to the **management console**.
2. Select the region where the ECS is located.
3. Choose **Compute** > **Elastic Cloud Server**.
4. Locate the row containing the target ECS and choose **More** > **Delete** in the **Operation** column.

NOTE

If you choose to delete the EIP and data disks associated with the ECS when deleting it, no charges will apply for the EIP and data disks. However, if they are not deleted, they will continue to incur fees.

Restarting an ECS

1. Log in to the **management console**.
2. Select the region where the ECS is located.
3. Choose **Compute** > **Elastic Cloud Server**.
4. Locate the row containing the target ECS and choose **More** > **Restart** in the **Operation** column.

4.5 Can I Forcibly Restart or Stop an ECS?

Yes. If an ECS remains in the **Restarting** or **Stopping** state for over 30 minutes after it is restarted, you can forcibly restart or stop the ECS as follows:

1. Log in to the **management console**.
2. Click 📍 in the upper left corner and select a region and project.
3. Choose **Compute** > **Elastic Cloud Server**.
4. Select the target ECS and click **Restart** or **Stop**.

   A dialog box is displayed to confirm whether you want to restart or stop the ECS.
5. Select **Forcibly restart the preceding ECSs** or **Forcibly stop the preceding ECSs**.
6. Click **OK**.

4.6 How Do I Unsubscribe from ECSs?

A yearly/monthly ECS can be unsubscribed, including the renewed resources and the resources that are being used. After the unsubscription, the ECS can no longer be used. A handling fee will be charged for unsubscribing from a resource.

Notes

- Unsubscribing from an ECS involves the renewed resources and the resources that are being used. After the unsubscription, the ECS is unavailable.
- Solution product portfolios can only be unsubscribed from as a whole.
- If an order contains resources in a primary-secondary relationship, you need to unsubscribe from the resources separately.
- For details about 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 ECS that will be unsubscribed from. After the unsubscription is complete, the ECS and any data it contains will be permanently deleted.

1. Go to the **Unsubscriptions** page.
2. Click the **Unsubscribe from In-Use Resources** tab.
3. Unsubscribe from a single resource or from resources in a batch.
   - To unsubscribe from a single resource, click **Unsubscribe** for the target resource.
   - To unsubscribe from resources in a batch, select the target resources from the resource list and click **Batch Unsubscribe** in the upper part of the resource list.
4. View the unsubscription information, select **I have confirmed that a handling fee will be charged for this unsubscription**, and click **Unsubscribe**.

5 Remote Login

5.1 Login Preparations

5.1.1 What Are the Login Requirements for ECSs?

Windows

- Obtain the login password.

  ECSs created using a public image have the one-click password reset plug-in installed by default. If you forgot your password or it has expired, reset the password on the ECS console to obtain a new password for logging in to the ECS.
- Ensure that the ECS has an EIP bound (only required for MSTSC logins).

  For details, see **Assigning an EIP**.
- Make sure that the remote desktop protocol has been enabled on the ECS (only required for MSTSC logins).

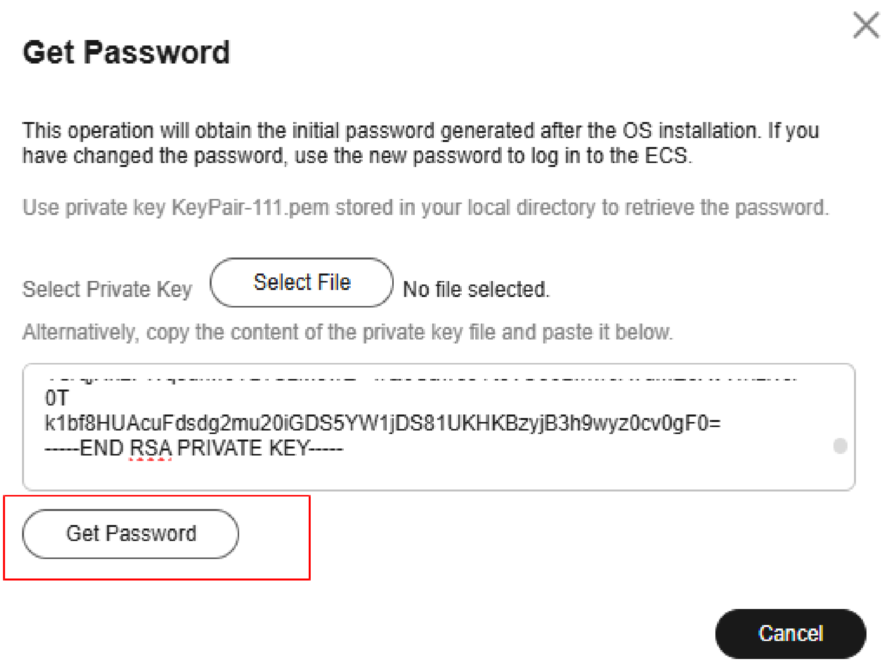
  If MSTSC-based remote desktop connection is used, log in to the ECS using VNC and enable the remote desktop protocol.

  For details, see **Logging In to a Windows ECS Using MSTSC**.

More information:

- If you created your ECS by using an external image file and the ECS does not have the password reset plug-in installed, reset the ECS login password by attaching a disk to the ECS. For details, see **Resetting the Password of a Windows ECS by Attaching a System Disk to a Temporary ECS**.
- **If your ECS is authenticated using a key pair, parse the private key file to a password before you log in to the ECS.**
  a. In the **Operation** column of ECS whose password is to be obtained, click **More** and choose **Get Password**.
  b. Copy the content of the private key file and paste it into the text box. Click **Get Password** to obtain a new random password.

Figure 5-1 Get Password



Get Password

This operation will obtain the initial password generated after the OS installation. If you have changed the password, use the new password to log in to the ECS.

Use private key KeyPair-111.pem stored in your local directory to retrieve the password.

Select Private Key: No file selected.

Alternatively, copy the content of the private key file and paste it below.

```
0T
k1bf8HUAcuFdsdg2mu20iGDS5YW1jDS81UKHKBzyjB3h9wyz0cv0gF0=
-----END RSA PRIVATE KEY-----
```

Linux

- Obtain the login password.

  ECSs created using a public image have the one-click password reset plug-in installed by default. If you forgot your password or it has expired, reset the password on the ECS console to obtain a new password for logging in to the ECS.

- Ensure that the ECS has an EIP bound (only required for SSH logins).

  SSH logins are available for Linux ECSs only. You can use a remote login tool to log in to your ECS. Ensure that the ECS has an EIP bound. For example, **use PuTTY to log in to the ECS**.

  – Check whether an ECS has an EIP bound.

    For details, see **Assigning an EIP**.

  – Check whether an EIP can be pinged.

    ■ If you use a public IP address, see **What Should I Do If an EIP Cannot Be Pinged?** for troubleshooting.

    ■ If you use a private IP address, see **Why Does Communication Fail Between Two ECSs in the Same VPC or Packet Loss Occur When They Communicate?**

  More information:

  – If you created your ECS by using an external image file and the ECS does not have the password reset plug-in installed, reset the ECS login password by attaching a disk to the ECS. For details, see **Resetting the Password of a Linux ECS by Attaching a System Disk to a Temporary ECS**.

- For a Linux ECS authenticated using a key pair:
  - For the first login, use an SSH key. For details, see **Remotely Logging In to a Linux ECS (Using an SSH Key Pair)**.
  - For a non-first login, if you want to use the remote login function (VNC) provided by the management console, log in to the ECS using the SSH key and set the password.
- For an ECS purchased using a key pair, if you fail to log in to the ECS using a private key file, the possible cause is that the password fails to be injected using Cloud-Init.

5.1.2 What Are the Username and Password for Remote Logins?

Username for logging in to an ECS:

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

If you forgot the login password or did not set a password when creating the ECS, you can **reset the password**.

If you still cannot remotely log in to the ECS after resetting the password, the one-click password reset plug-in may become invalid. You can resolve this issue by performing the following operations:

- **Resetting the Password of a Windows ECS by Attaching a System Disk to a Temporary ECS**
- **Resetting the Password of a Linux ECS by Attaching a System Disk to a Temporary ECS**

5.1.3 Can I Retrieve My Remote Login Password?

No. If you did not set a password when creating an ECS, or you forgot your password or it has expired, reset the password by following the instructions provided in **Resetting the Password for Logging In to an ECS on the Management Console**.

NOTE

Keep your password secure.

If you still cannot remotely log in to the ECS after resetting the password, the one-click password reset plug-in may become invalid. You can resolve this issue by performing the following operations:

- **Resetting the Password of a Windows ECS by Attaching a System Disk to a Temporary ECS**
- **Resetting the Password of a Linux ECS by Attaching a System Disk to a Temporary ECS**

5.1.4 Why Cannot I Use the Username and Password Configured During the Creation of a GPU-accelerated ECS to Log In to the ECS Through SSH?

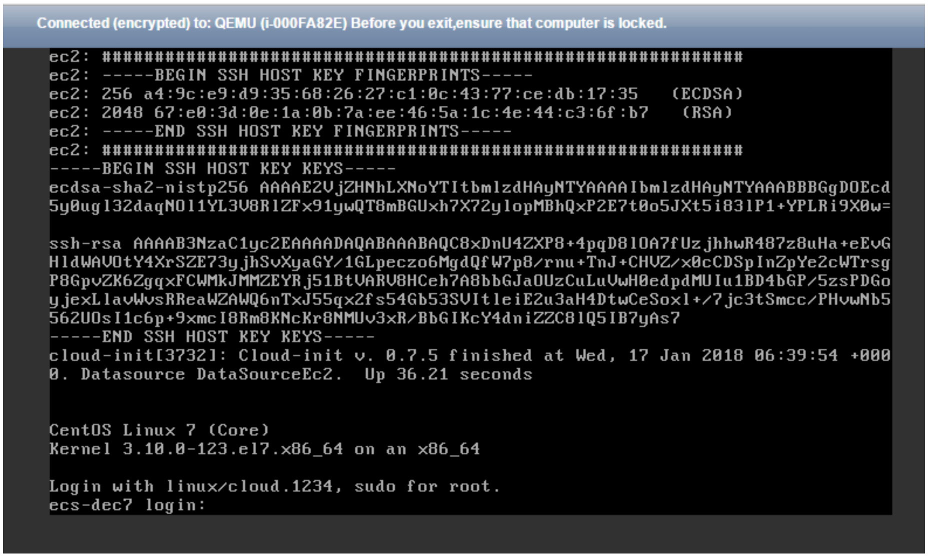
Solution

Log in to the ECS using VNC, modify the configuration file, and log in to the ECS through SSH.

1. On the ECS console, locate the ECS and click **Remote Login**.
2. On the login page, enter user **root** and its password.

   NOTE

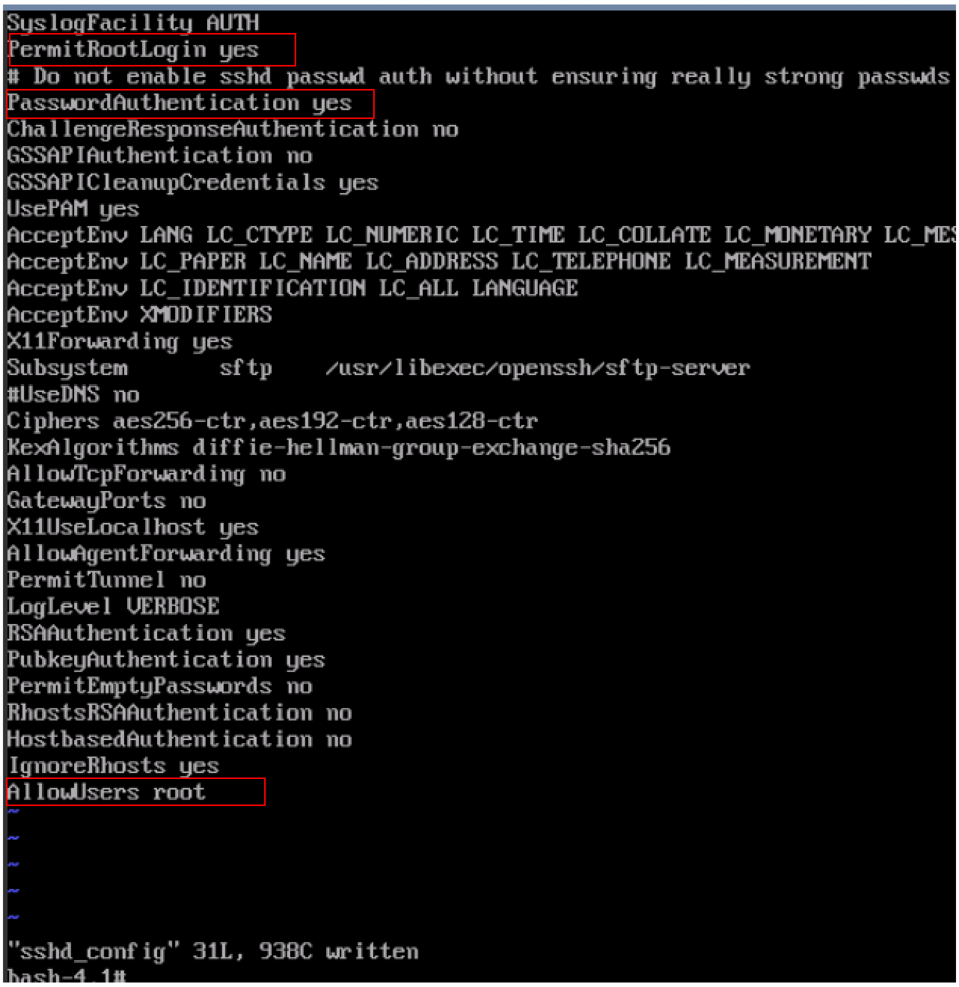
   The password is the one you set during the ECS creation.



Connected (encrypted) to: QEMU (i-000FA82E) Before you exit,ensure that computer is locked.

```
ec2: #############################################################
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
ec2: 256 a4:9c:e9:d9:35:68:26:27:c1:0c:43:77:ce:db:17:35   (ECDSA)
ec2: 2048 67:e0:3d:0e:1a:0b:7a:ee:46:5a:1c:4e:44:c3:6f:b7   (RSA)
ec2: -----END SSH HOST KEY FINGERPRINTS-----
ec2: #############################################################
-----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGgDOEcd
5y0ugl32daqNOl1YL3V8RlZFx91ywQT8mBGUxh7X72ylopMBhQxP2E7t0o5JXt5i831P1+YPLRi9X0w=

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8xDnU4ZXP8+4pqD81OA7fUzjhhwR487z8uHa+eEvG
HldWAVOtY4XrSZE73yjhSvXyaGY/1GLpeczo6MgdQfW7p8/rnu+TnJ+CHVZ/x0cCDSpInZpYe2cWTrsg
P8GpvZK6ZgqxFCWMkJMMZEYRj51BtVARV8HCeh7A8bbGJaOUzCuLuVwH0edpdMUIu1BD4bGP/5zsPDGo
yjexLlavWvsRReaWZAWQ6nTxJ55qx2fs54Gb53SVItleiE2u3aH4DtwCeSoxl+/7jc3tSmcc/PHvwNb5
562UOsI1c6p+9xmcI8Rm8KNcKr8NMUv3xR/BbGIKcY4dniZZC81Q5IB7yAs7
-----END SSH HOST KEY KEYS-----
cloud-init[3732]: Cloud-init v. 0.7.5 finished at Wed, 17 Jan 2018 06:39:54 +000
0. Datasource DataSourceEc2.  Up 36.21 seconds


CentOS Linux 7 (Core)
Kernel 3.10.0-123.el7.x86_64 on an x86_64

Login with linux/cloud.1234, sudo for root.
ecs-dec7 login:
```

3. In the **/etc/ssh/** directory, modify the three configuration items in the **sshd_config** file, as shown in the following figure.



```
SyslogFacility AUTH
PermitRootLogin yes
# Do not enable sshd passwd auth without ensuring really strong passwds
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication no
GSSAPICleanupCredentials yes
UsePAM yes
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
X11Forwarding yes
Subsystem       sftp    /usr/libexec/openssh/sftp-server
#UseDNS no
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
KexAlgorithms diffie-hellman-group-exchange-sha256
AllowTcpForwarding no
GatewayPorts no
X11UseLocalhost yes
AllowAgentForwarding yes
PermitTunnel no
LogLevel VERBOSE
RSAAuthentication yes
PubkeyAuthentication yes
PermitEmptyPasswords no
RhostsRSAAuthentication no
HostbasedAuthentication no
IgnoreRhosts yes
AllowUsers root
~
~
~
~
~

"sshd_config" 31L, 938C written
bash-4.1#
```

4. Save the modification and exit. Then, run the following command to restart SSH:

   service sshd restart

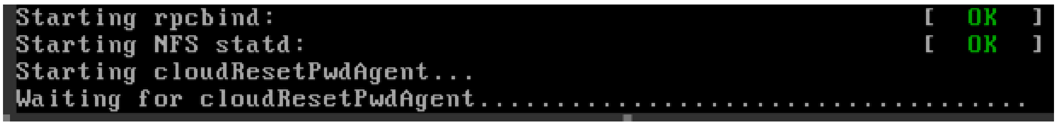
5. After the restart, use the SSH password to log in again.
6. If the fault persists, contact customer service.

5.1.5 What Should I Do If Starting an ECS Remains in "Waiting for cloudResetPwdAgent" State?

Symptom

During ECS startup, it remains in "Waiting for cloudResetPwdAgent" state for 20 to 30 seconds.

Figure 5-2 Starting cloudResetPwdAgent



```
Starting rpcbind:                                               [  OK  ]
Starting NFS statd:                                             [  OK  ]
Starting cloudResetPwdAgent...
Waiting for cloudResetPwdAgent..................................
```

Possible Causes

This issue is caused by the intranet DNS and user-defined DNS configurations.

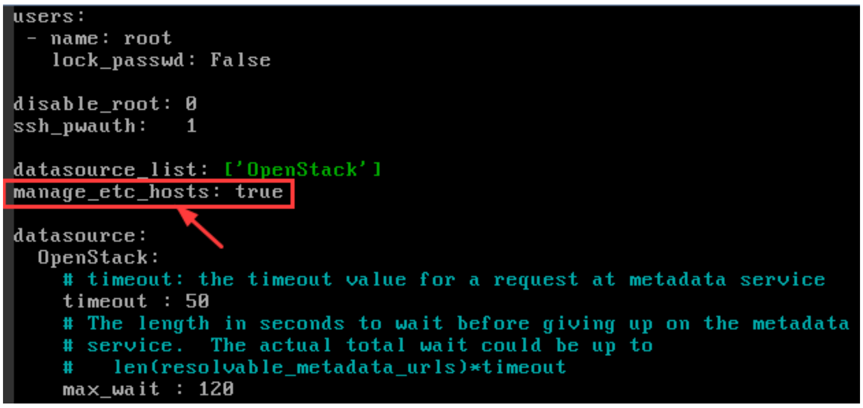
Solution

1. Log in to the ECS as user **root**.
2. Run the following command to modify the **/etc/cloud/cloud.cfg** configuration file:

   vi /etc/cloud/cloud.cfg
3. Add the following statement to the configuration file:

   manage_etc_hosts: true

Figure 5-3 Editing the configuration file



```
users:
 - name: root
   lock_passwd: False

disable_root: 0
ssh_pwauth:   1

datasource_list: ['OpenStack']
manage_etc_hosts: true

datasource:
  OpenStack:
    # timeout: the timeout value for a request at metadata service
    timeout : 50
    # The length in seconds to wait before giving up on the metadata
    # service.  The actual total wait could be up to
    #   len(resolvable_metadata_urls)*timeout
    max_wait : 120
```

5.2 Remote Logins

5.2.1 Can I Troubleshoot ECSs By Myself?

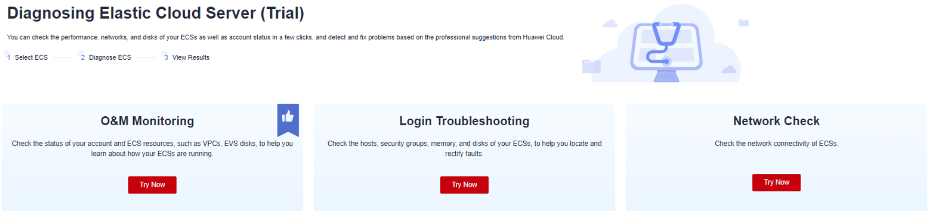
Yes. ECS provides self-service tools to help you diagnose your ECSs. You can check the performance, networks, and disks of your ECSs as well as account status in a few clicks, and detect and fix problems based on the professional suggestions from Huawei Cloud.

The following describes how to use the ECS self-service tools.

Starting a Diagnosis

1. Log in to the management console.
2. Click ☰ . Under **Compute**, click **Elastic Cloud Server**.
3. In the left navigation pane, choose **Troubleshooting**.
4. On the displayed **Self-Service Tools** page, select a self-service tool.

Figure 5-4 Self-service tools



Diagnosing Elastic Cloud Server (Trial)

You can check the performance, networks, and disks of your ECSs as well as account status in a few clicks, and detect and fix problems based on the professional suggestions from Huawei Cloud.

1 Select ECS — 2 Diagnose ECS — 3 View Results

O&M Monitoring

Check the status of your account and ECS resources, such as VPCs, EVS disks, to help you learn about how your ECSs are running.

Login Troubleshooting

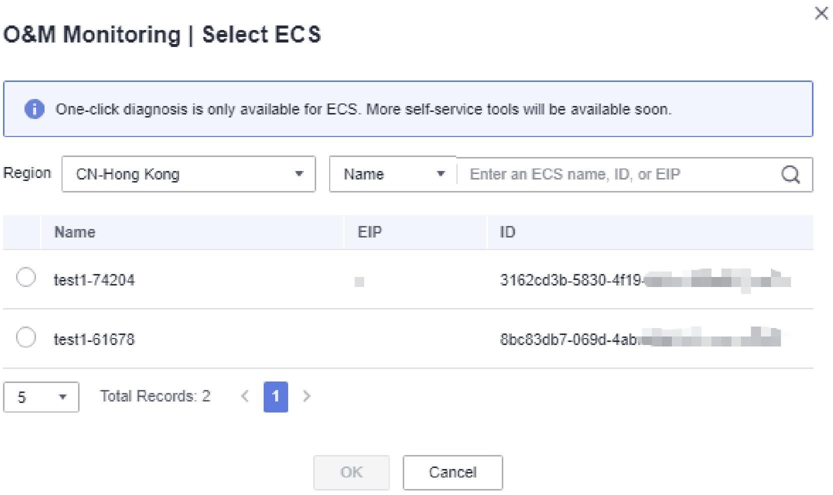
Check the hosts, security groups, memory, and disks of your ECSs, to help you locate and rectify faults.

Network Check

Check the network connectivity of ECSs.

- **O&M Monitoring**: Check the statuses of your account and ECS resources, such as VPCs, EVS disks, to help you learn about your ECS running status.
  i. In the **O&M Monitoring** card, click **Try Now**.
  ii. Select the region where the target ECS resides, select the ECS, and click **OK**.

  Figure 5-5 Selecting an ECS

  O&M Monitoring | Select ECS

  One-click diagnosis is only available for ECS. More self-service tools will be available soon.

  Region: CN-Hong Kong

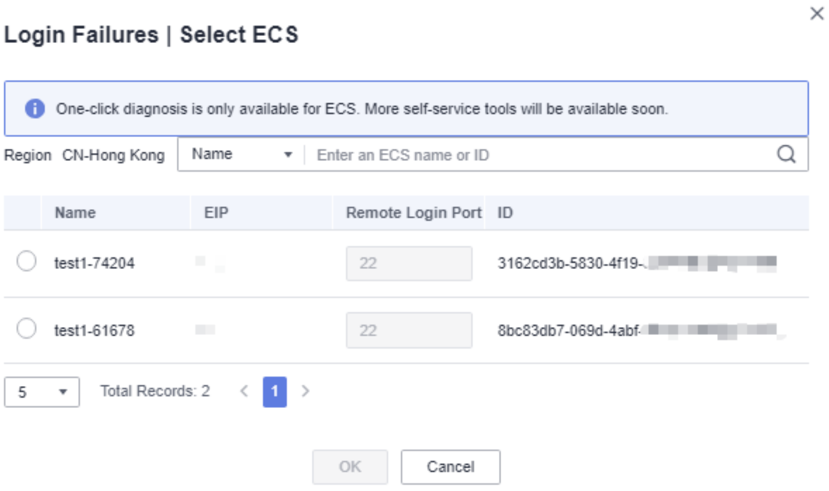
	Name	EIP	ID
○	test1-74204		3162cd3b-5830-4f19[redacted]
○	test1-61678		8bc83db7-069d-4ab[redacted]

  Total Records: 2

  In the right slide-out panel, a diagnosis report is generated for the ECS. You can rectify the faults based on the suggestions in the report.

- **Login Troubleshooting**: Check the hosts, security groups, memory, and disks of your ECSs, to help you locate and rectify faults.
  i. In the **Login Troubleshooting** card, click **Try Now**.
  ii. Select the region where the target ECS resides.
  iii. On the **Login Failures** tab, click **Diagnose**.
  iv. Select the ECS to be diagnosed and click **OK**.

Figure 5-6 Selecting an ECS



Login Failures | Select ECS

One-click diagnosis is only available for ECS. More self-service tools will be available soon.

Region CN-Hong Kong | Name ▾ | Enter an ECS name or ID

	Name	EIP	Remote Login Port	ID
○	test1-74204	[redacted]	22	3162cd3b-5830-4f19-[redacted]
○	test1-61678	[redacted]	22	8bc83db7-069d-4abf-[redacted]

5 ▾ Total Records: 2 < 1 >

NOTE

The remote login port uses the default port. If you have changed the default port, enter the new one.

Default ports: 22 (Linux ECS) and 3389 (Windows ECS)

In the right slide-out panel, a diagnosis report is generated for the ECS. You can rectify the faults based on the suggestions in the report.

If the login failure persists after the faults are rectified, record the resource details and login failure occurred time and **submit a service ticket** for technical support.

– **Network Check**: Check the network connectivity of your ECSs.

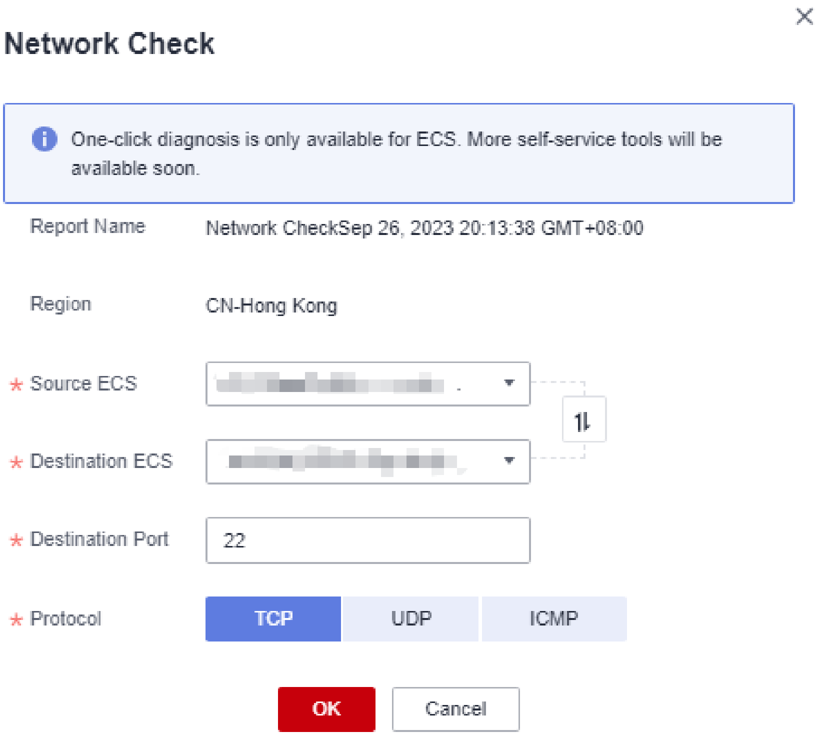
  i. In the **Network Check** card, click **Try Now**.

  ii. Select the region where the target ECS resides.

  iii. On the **Network Check** tab, click **Diagnose**.

  iv. In the displayed dialog box, specify the parameters and click **OK**.

Figure 5-7 Specifying parameters



Network Check

One-click diagnosis is only available for ECS. More self-service tools will be available soon.

Report Name: Network CheckSep 26, 2023 20:13:38 GMT+08:00

Region: CN-Hong Kong

* Source ECS: [redacted]

* Destination ECS: [redacted]

* Destination Port: 22

* Protocol: TCP

In the right slide-out panel, a diagnosis report is generated for the ECS. You can rectify the faults based on the suggestions in the report.

Follow-up Operations

- Click **Diagnosis Records** on the top of the **Self-Service Tools** page. On the displayed page, select the target region, locate the target ECS, and click **View Report** in the **Operation** column to view the historical diagnosis report.
- After the fault is rectified according to the handling suggestions, you can click **Re-diagnose** in the **Operation** column of the target ECS to start a diagnosis again.

  The re-diagnosis will generate a new diagnosis record and will not overwrite the historical records.

Helpful Links

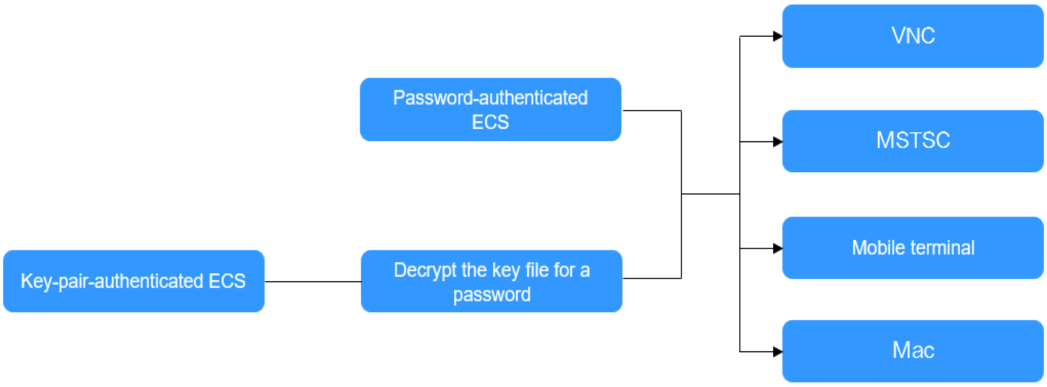
- **Why Can't I Log In to My Linux ECS?**
- **Why Can't I Log In to My Windows ECS?**

5.2.2 How Do I Log In to My ECS?

Logging In to a Windows ECS

Figure 5-8 shows the modes in which a Windows ECS can be logged in to.

Figure 5-8 Windows ECS login modes


Password-authenticated ECS
Key-pair-authenticated ECS
Decrypt the key file for a password
VNC
MSTSC
Mobile terminal
Mac

1. (Optional) Retrieve your password from the key file.

   To log in to a key-pair-authenticated ECS, use the password obtaining function provided by the management console to decrypt the key file used during ECS creation to obtain a password.

   For details, see **Obtaining the Password for Logging In to a Windows ECS**.

2. Select a login method and log in to the ECS.
   - Using VNC on the management console

     The login username is **Administrator**.

     For details, see **Logging In to a Windows ECS Using VNC**.
   - Using MSTSC

     The login username is **Administrator**, and the ECS must have an EIP bound.

     For details, see **Logging In to a Windows ECS Using MSTSC**.
   - From a mobile terminal

     The login username is **Administrator**, and the ECS must have an EIP bound.

     For details, see **Logging In to a Windows ECS from a Mobile Terminal**.
   - From a Mac

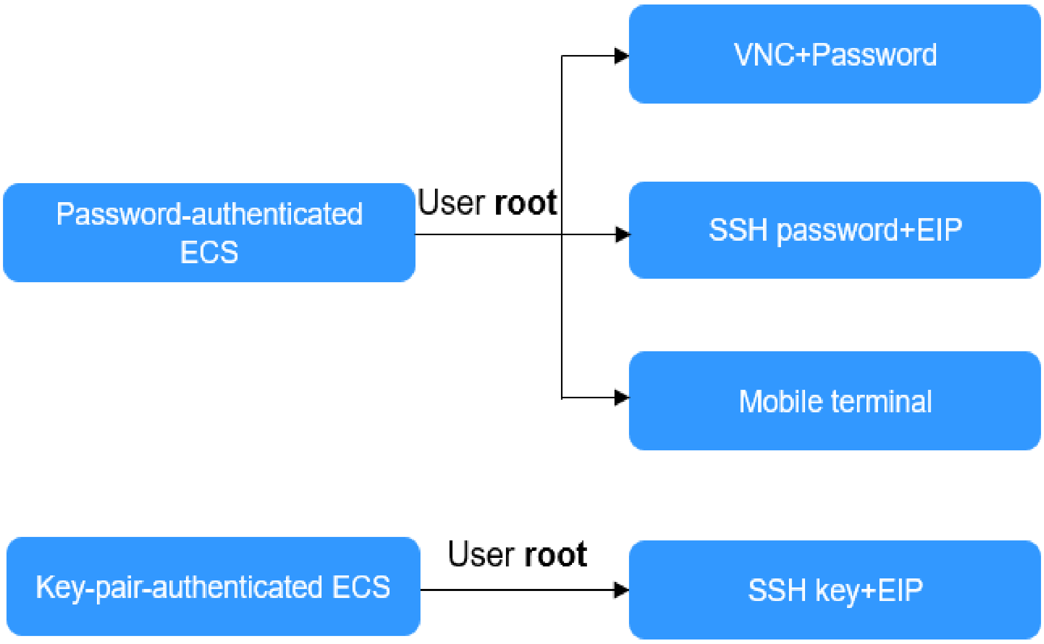
     The login username is **Administrator**, and the ECS must have an EIP bound.

     For details, see **Logging In to a Windows ECS from a Mac**.

Logging In to a Linux ECS

The method of logging in to an ECS varies depending on the login authentication configured during ECS creation.

Figure 5-9 Linux ECS login modes



- To log in to a password-authenticated ECS for the first time, use one of the following methods:
  - Using VNC on the management console with login username **root**

    For details, see **Logging In to a Linux ECS Using VNC**.
  - Using an SSH password

    The login username is **root**, and the ECS must have an EIP bound.

    For details, see **Logging In to a Linux ECS Using an SSH Password**.
  - From a mobile terminal

    The login username is **root**, and the ECS must have an EIP bound.

    For details, see **Logging In to a Linux ECS from a Mobile Terminal**.
- To log in to a key-pair-authenticated ECS for the first time, use a tool, such as PuTTY or Xshell, and the desired SSH key as user **root**. Ensure that the ECS has an EIP bound.

  For instructions about how to log in to a Linux ECS using an SSH key, see **Logging In to a Linux ECS Using an SSH Key Pair**.

  NOTE

  If you want to log in to an ECS using VNC provided on the management console, log in to the ECS using an SSH key, configure the login password, and use the password for login.

Follow-up Procedure

- If you have added a data disk during ECS creation, you must initialize the data disk after logging in to the ECS.

  For details, see **Initialization Overview**.

- Certain ECSs require the installation of a driver after you log in to them. For details about available ECS types and functions, see **ECS Types**. For details about constraints on using different types of ECSs, see their notes.

5.2.3 Why Can't I Log In to My Windows ECS?

Symptom

A Windows ECS fails to be logged in to due to some reasons. For example, the network is abnormal, the firewall blocks the local port required for remote desktop, or the ECS vCPUs are overloaded.

This section describes how to troubleshoot Windows ECS login failures.

If you cannot log in to your Windows ECS, follow the instructions provided in **Checking the VNC Login**. Then, locate the login fault by referring to **Fault Locating**.

Checking the VNC Login

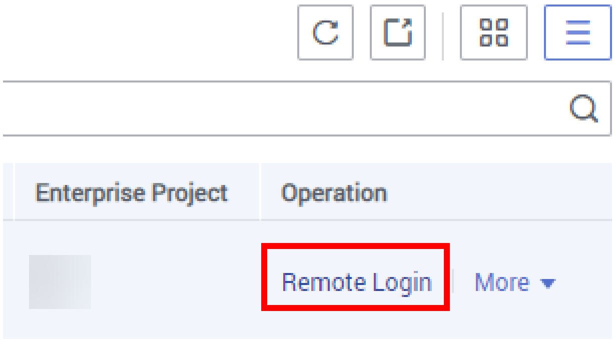
Check whether you can log in to the ECS using VNC on the management console.

NOTE

See **What Are the Login Requirements for ECSs?** to learn the requirements for logging in to an ECS.

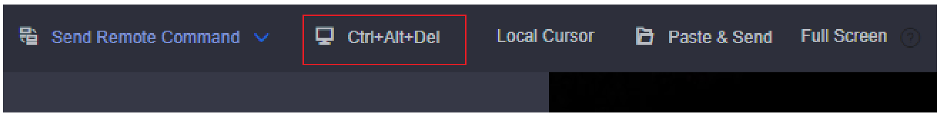
1. Log in to the **management console**.
2. Choose **Compute** > **Elastic Cloud Server**.
3. In the **Operation** column of the target ECS, click **Remote Login**.

Figure 5-10 Remote Login



4. (Optional) When the system displays "Press Ctrl+Alt+Delete to unlock", click **Ctrl+Alt+Del** in the upper part of the remote login page to log in to the ECS.

Figure 5-11 Ctrl+Alt+Del



For details about VNC login FAQs, see **VNC Login**.

If the VNC login still fails, record the resource details and fault occurred time. Then, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the management console to submit a ticket.

Self-Service Troubleshooting

ECS provides self-service tools to help you diagnose and troubleshoot your ECSs. If you cannot log in to your ECS, you can use self-service tools to check the host, security group, memory, and disk status of the ECS for troubleshooting.

For details, see **Can I Troubleshoot ECSs By Myself?**

If the fault persists, record the abnormal items in the diagnosis report and submit a service ticket (in the upper right corner of the management console) for technical support.

Fault Locating

If you can log in to the ECS using VNC but cannot log in to it using a remote desktop connection, locate the fault by referring to this section.

The following fault causes are sequenced based on their occurrence probability.

If the fault persists after you have ruled out a cause, check other causes.

Table 5-1 Possible causes and solutions

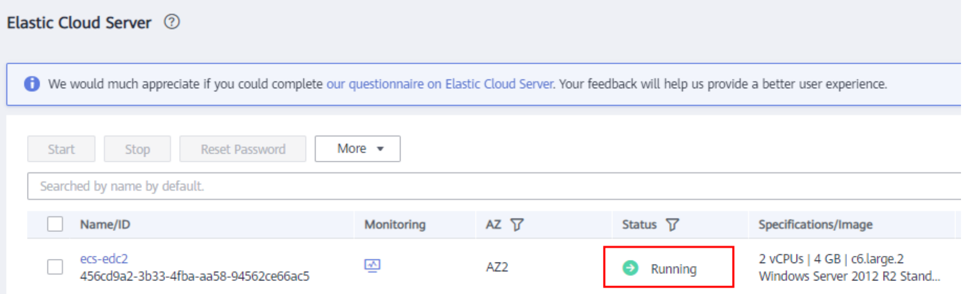
Possible Cause	Solution
The ECS is frozen or stopped.	Make sure that the ECS is in the **Running** state. For details, see **Checking the ECS Status**.
The entered username or password is incorrect.	The default username for Windows ECSs is **Administrator**. If the password is incorrect, reset the password on the management console. For details, see **Checking the Login Mode**.
The ECS is overloaded.	If the bandwidth or CPU usage of the ECS is excessively high, login failures may occur. For details, see **Checking Whether the ECS Is Overloaded**.
The ECS has no EIP bound.	To log in to an ECS using RDP or MSTSC, ensure that the ECS has an EIP bound. For details, see **Checking Whether an ECS Has an EIP Bound**.
The access is blocked by the Internet service provider (ISP).	Check whether you can access the ECS using another hotspot or network. For details, see **Checking Whether the Network Is Normal**.
The access is blocked by the firewall.	Disable the firewall and try again. For details, see **Checking Whether the Firewall Is Correctly Configured**.

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

Checking the ECS Status

Check whether the ECS is in the **Running** state on the management console. If the ECS is stopped, start it and try to log in to the ECS again.

Figure 5-12 Checking the ECS status



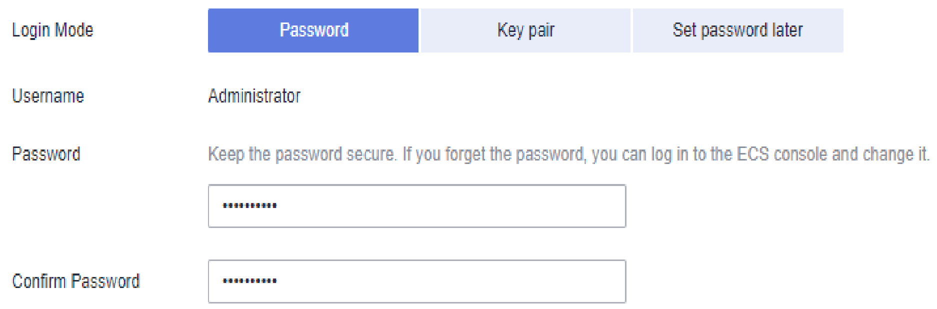
We would much appreciate if you could complete our questionnaire on Elastic Cloud Server. Your feedback will help us provide a better user experience.

☐	Name/ID	Monitoring	AZ	Status	Specifications/Image
☐	ecs-edc2 456cd9a2-3b33-4fba-aa58-94562ce66ac5		AZ2	Running	2 vCPUs | 4 GB | c6.large.2 Windows Server 2012 R2 Stand...

Checking the Login Mode

Check the login mode you set when you created the ECS.

Figure 5-13 Login Mode



Login Mode: Password | Key pair | Set password later

Username: Administrator

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.

••••••••••

Confirm Password: ••••••••••

- **Password**: Check whether the login password is correct. If you forgot your password, reset the password. After you reset the password, restart the ECS for the new password to take effect.
- **Key pair**: If your ECS is authenticated using a key pair, use the key pair to obtain a password before logging in.
  a. Locate the ECS whose password is to be obtained, choose **More** > **Manage Password** > **Get Password** in the **Operation** column.
  b. Copy the content of the private key file and paste it into the text box. Click **Get Password** to obtain a new random password.
- **Set password later**: If you did not set a login mode when you create an ECS, you can reset the password on the ECS console by choosing **More** > **Reset Password** in the **Operation** column of the target ECS. After you reset the password, restart the ECS for the new password to take effect.

Checking Whether the ECS Is Overloaded

If the bandwidth or CPU usage of the ECS is excessively high, login failures may occur.

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

To resolve this issue, perform the operations described in **Why Is My Windows ECS Running Slowly?**

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

  You can also upgrade the vCPUs and memory by **modifying ECS 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 Know If My EIP Bandwidth Limit Has Been Exceeded?**

  If the bandwidth exceeds the limit, increase the bandwidth. For details, see **Changing an EIP Bandwidth**.

  NOTE

  If network jitter or packet loss occurs frequently, dynamic BGP may be used in cross-border access. In this case, you are advised to use premium BGP.

  For details, see **Why Is There Network Jitter or Packet Loss During Cross-Border Communications?**

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

Checking Whether an ECS Has an EIP Bound

An ECS can access the Internet only after it has an EIP bound.

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

NOTE

If you log in to an ECS over an intranet, for example, using VPN or Direct Connect, you do not need to bind an EIP to the ECS.

Checking Whether the Network Is Normal

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

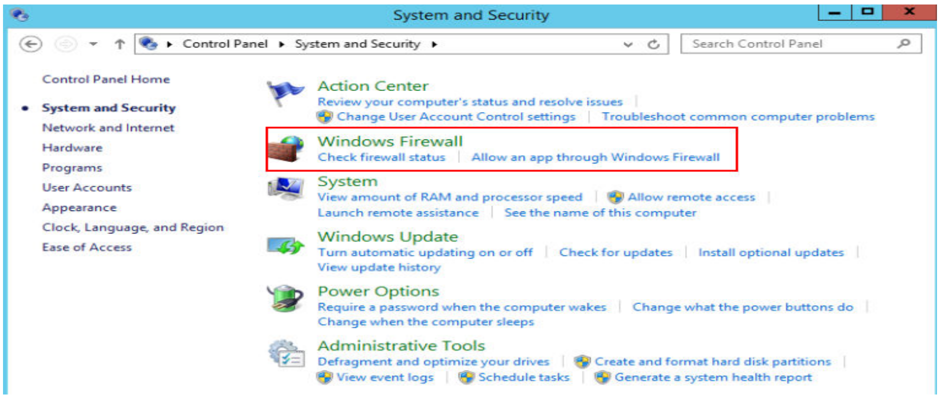
After you perform the preceding operations, try to remotely log in to the ECS again.

Checking Whether the Firewall Is Correctly Configured

Check whether the firewall is enabled.

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

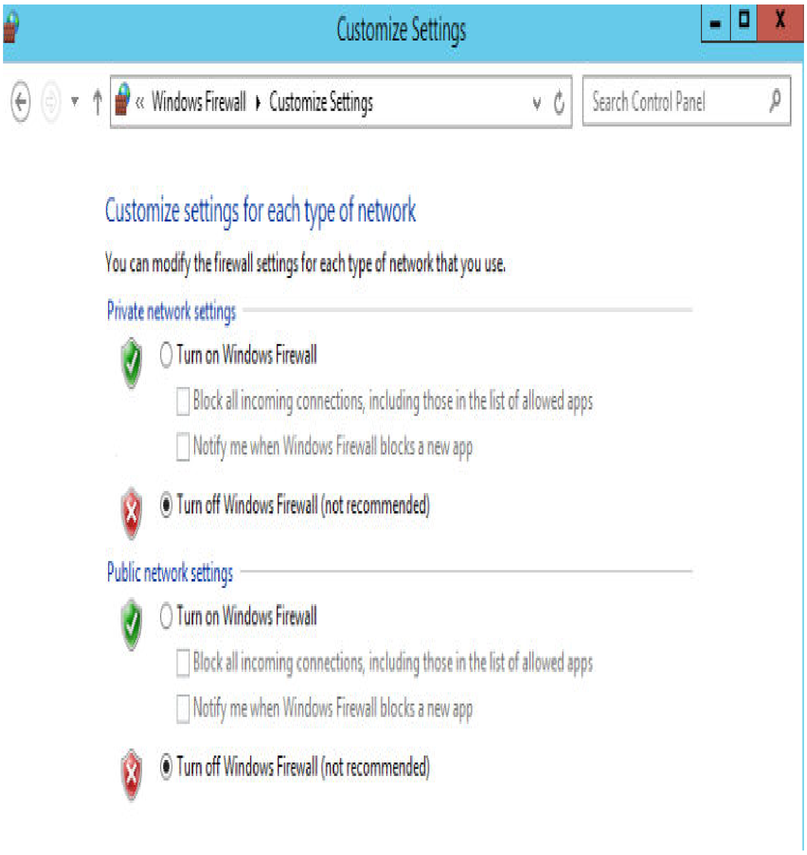
Figure 5-14 Windows Firewall


System and Security
Control Panel ▸ System and Security ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware
Programs
User Accounts
Appearance
Clock, Language, and Region
Ease of Access
Action Center
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Windows Update
Turn automatic updating on or off
Check for updates
Install optional updates
View update history
Power Options
Require a password when the computer wakes
Change what the power buttons do
Change when the computer sleeps
Administrative Tools
Defragment and optimize your drives
Create and format hard disk partitions
View event logs
Schedule tasks
Generate a system health report

3. Click **Check firewall status** and select **Turn on Windows Firewall** or **Turn off Windows Firewall**.

   View and set the firewall status.

Figure 5-15 Turning off a firewall



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☐ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Public network settings

○ Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☐ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

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 will fail. If this occurs, add the port configured on the remote server in the inbound rule of the firewall.

For details, see **How Do I Disable a Windows ECS Firewall and Add 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 you perform the preceding operations, try to remotely log in to the ECS again.

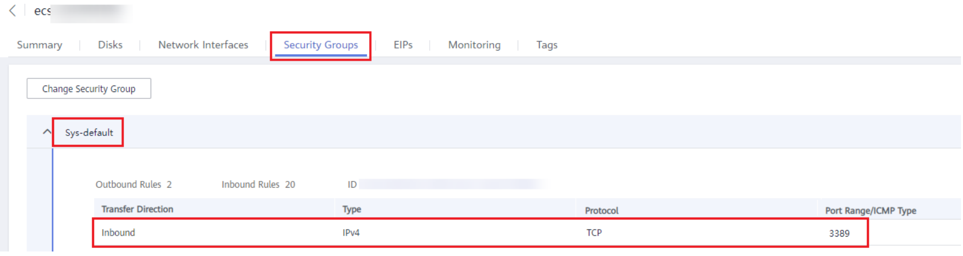
Checking Whether the Remote Access Port Is Correctly Configured

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

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

   On the ECS details page, click the **Security Groups** tab and check port 3389 in the inbound rule of the security group.

   Figure 5-16 Checking remote access ports

   Outbound Rules 2 Inbound Rules 20 ID [redacted]

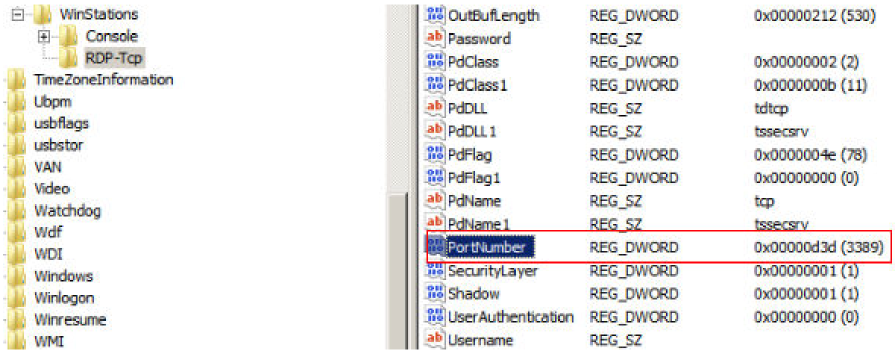
Transfer Direction	Type	Protocol	Port Range/ICMP Type
Inbound	IPv4	TCP	3389

   If you need to modify security group rules, see **Modifying a Security Group Rule**.

2. Check whether the remote connection port is 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 port 3389.

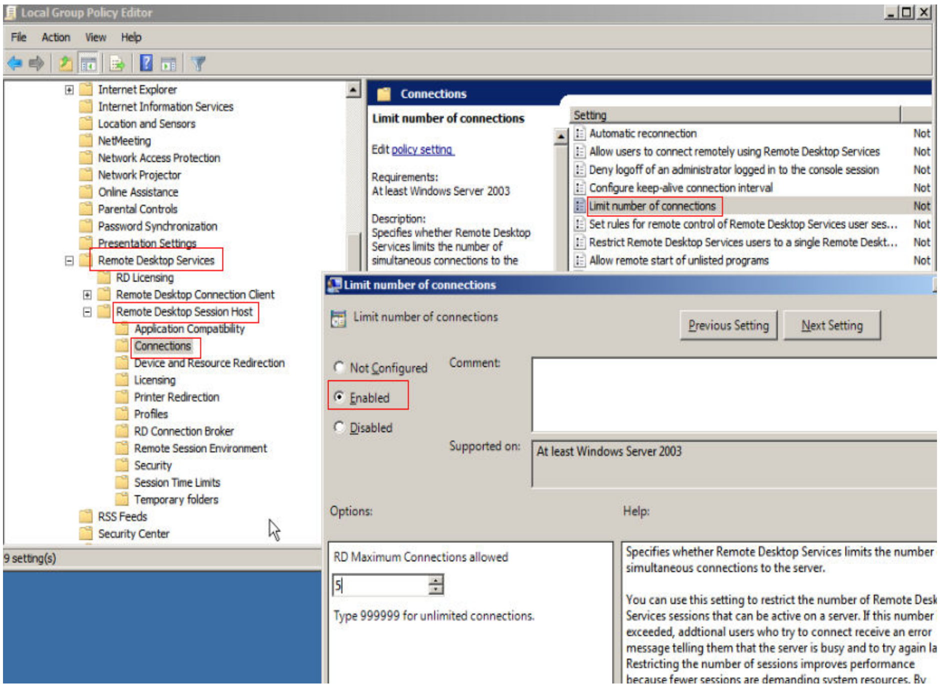
OutBufLength	REG_DWORD	0x00000212 (530)
Password	REG_SZ	
PdClass	REG_DWORD	0x00000002 (2)
PdClass1	REG_DWORD	0x0000000b (11)
PdDLL	REG_SZ	tdtcp
PdDLL1	REG_SZ	tssecsrv
PdFlag	REG_DWORD	0x0000004e (78)
PdFlag1	REG_DWORD	0x00000000 (0)
PdName	REG_SZ	tcp
PdName1	REG_SZ	tssecsrv
PortNumber	REG_DWORD	0x00000d3d (3389)
SecurityLayer	REG_DWORD	0x00000001 (1)
Shadow	REG_DWORD	0x00000001 (1)
UserAuthentication	REG_DWORD	0x00000000 (0)
Username	REG_SZ	

3. Check whether the number of connections is limited.

   Check the internal remote desktop configuration of the ECS.

   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 of connections is limited.



Limit number of connections

Requirements:
At least Windows Server 2003

Description:
Specifies whether Remote Desktop Services limits the number of simultaneous connections to the

Setting	
Automatic reconnection	Not
Allow users to connect remotely using Remote Desktop Services	Not
Deny logoff of an administrator logged in to the console session	Not
Configure keep-alive connection interval	Not
Limit number of connections	Not
Set rules for remote control of Remote Desktop Services user ses...	Not
Restrict Remote Desktop Services users to a single Remote Deskt...	Not
Allow remote start of unlisted programs	Not

Limit number of connections

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2003

RD Maximum Connections allowed: 5

Type 999999 for unlimited connections.

Specifies whether Remote Desktop Services limits the number simultaneous connections to the server.

You can use this setting to restrict the number of Remote Desk Services sessions that can be active on a server. If this number exceeded, addtional users who try to connect receive an error message telling them that the server is busy and to try again la Restricting the number of sessions improves performance because fewer sessions are demanding system resources. By

NOTE

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

After you perform the preceding operations, try to remotely log in to the ECS 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 ECSs, effectively preventing account cracking.

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

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 it has been enabled, 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 allowlist. Otherwise, you cannot remotely log in to your ECS through SSH.
- Exercise caution when adding a local IP address to the allowlist. This will make HSS no longer restrict access from this IP address to your ECSs.

For more details, see **Configuring Server Login Protection**.

Checking the Remote Desktop Protocol on the ECS

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

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

For details, see **Enabling RDP**.

Checking Whether the Access Is Blocked by Antivirus Software

Third-party antivirus software may lead to a failure in accessing the ECS.

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

You can also disable or uninstall the third-party antivirus software and try to remotely log in to the ECS again.

Checking Whether an Error Occurred During a Remote Login

If an error message is displayed during remote login, check the operation guide based on the error information.

For more information, see **Remote Login Errors on Windows**.

If the fault persists, record the resource details and fault occurred time, and contact technical support for assistance

If the fault persists after the preceding operations are performed, record the resource details and fault occurred time. Then, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the management console to submit a ticket.

5.2.4 Why Can't I Log In to My Linux ECS?

Symptom

A Linux ECS cannot be logged in to due to some reasons. For example, the network is abnormal, the firewall does not allow access to the local port for accessing the remote desktop, or the ECS vCPUs are overloaded.

This section describes how to troubleshoot Linux ECS login failures.

If you cannot log in to your Linux ECS, follow the instructions provided in **Checking the VNC Login**. Then, locate the login fault by referring to **Fault Locating**.

Checking the VNC Login

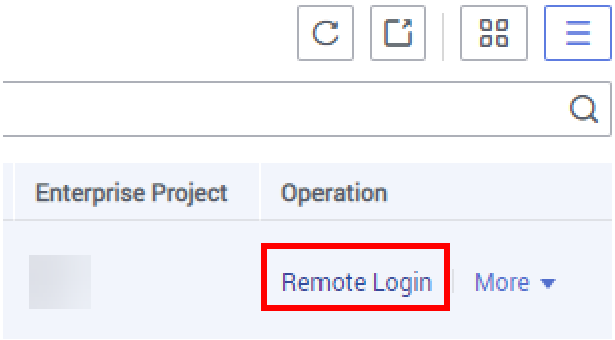
Check whether you can log in to the ECS using VNC on the management console.

NOTE

See **What Are the Login Requirements for ECSs?** to learn the requirements for logging in to an ECS.

1. Log in to the **management console**.
2. Choose **Compute** > **Elastic Cloud Server**.
3. In the **Operation** column of the target ECS, click **Remote Login**.

Figure 5-17 Remote Login



4. (Optional) When the system displays "Press CTRL+ALT+DELETE to log on", click **Ctrl+Alt+Del** in the upper part of the remote login page to log in to the ECS.

   NOTE

   Do not press **CTRL+ALT+DELETE** on the physical keyboard because this operation does not take effect.

If the VNC login still fails, record the resource details and fault occurred time. Then, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the management console to submit a ticket.

Self-Service Troubleshooting

ECS provides self-service tools to help you diagnose and troubleshoot your ECSs. If you cannot log in to your ECS, you can use self-service tools to check the host, security group, memory, and disk status of the ECS for troubleshooting.

For details, see **Can I Troubleshoot ECSs By Myself?**

If the fault persists, record the abnormal items in the diagnosis report and submit a service ticket (in the upper right corner of the management console) for technical support.

Fault Locating

If you can log in to the ECS using VNC but cannot log in to it using a remote desktop connection, locate the fault by referring to this section.

The following fault causes are sequenced based on their occurrence probability.

If the fault persists after you have ruled out a cause, check other causes.

Table 5-2 Possible causes and solutions

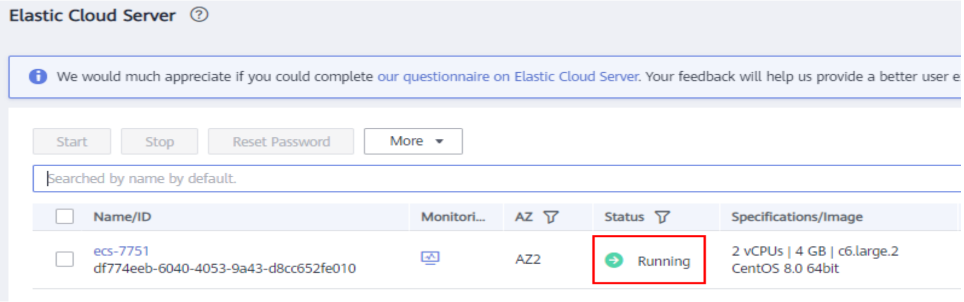
Possible Cause	Solution
The ECS is frozen or stopped.	Make sure that the ECS is in the **Running** state. For details, see **Checking the ECS Status**.
The entered username or password is incorrect.	The default username for Linux ECSs is **root**. If the password is incorrect, reset the password on the management console. For details, see **Checking the Login Mode**.
The ECS is overloaded.	If the bandwidth or CPU usage of the ECS is excessively high, login failures may occur. For details, see **Checking Whether the ECS Is Overloaded**.
The ECS has no EIP bound.	To log in to an ECS using RDP or MSTSC, ensure that the ECS has an EIP bound. For details, see **Checking Whether an ECS Has an EIP Bound**.
The access is blocked by the ISP.	Check whether you can access the ECS using another hotspot or network. For details, see **Checking Whether the Network Is Normal**.
The security group of the ECS denies inbound traffic on the remote login port.	Check whether the security group allows inbound traffic on the remote login port. For details, see **Checking Whether the Security Group Is Correctly Configured**.
The remote access port is incorrectly configured.	Check whether the remote access port is correctly configured on the local computer and the ECS. For details, see **Checking Whether the Remote Access Port Is Correctly Configured**.
An IP address whitelist for SSH logins has been configured.	Ensure your IP address is included in the whitelist. For details, see **Checking the IP Address Whitelist for SSH Logins (with HSS Enabled)**.
An OS fault has occurred.	The file system is damaged. For details, see **Checking Whether an OS Fault Has Occurred**.
The access is blocked by third-party antivirus software.	Disable or uninstall the third-party antivirus software and try again. For details, see **Checking Whether the Access Is Blocked by Antivirus Software**.

Possible Cause	Solution
The cause is displayed in the error message.	If an error message is displayed during remote login, check the operation guide based on the error information. For details, see **Checking Whether an Error Occurred During a Remote Login**.

Checking the ECS Status

Check whether the ECS is in the **Running** state on the management console. If the ECS is stopped, start it and try to log in to the ECS again.

Figure 5-18 Checking the ECS status



We would much appreciate if you could complete our questionnaire on Elastic Cloud Server. Your feedback will help us provide a better user e

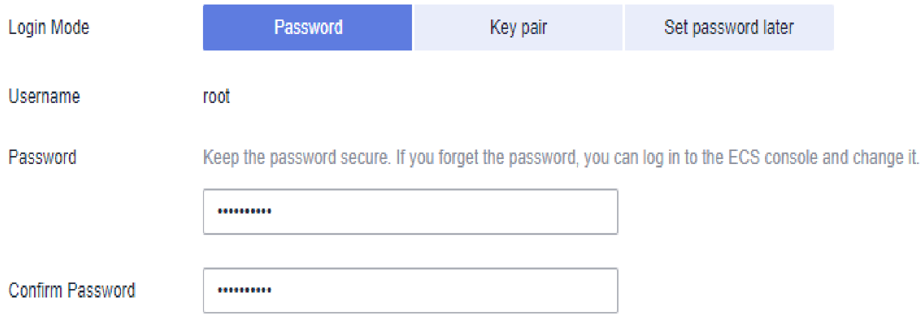
Searched by name by default.

☐	Name/ID	Monitori...	AZ	Status	Specifications/Image
☐	ecs-7751 df774eeb-6040-4053-9a43-d8cc652fe010		AZ2	Running	2 vCPUs | 4 GB | c6.large.2 CentOS 8.0 64bit

Checking the Login Mode

Check the login mode you set when you created the ECS.

Figure 5-19 Login Mode



Login Mode: Password

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.

••••••••••

Confirm Password: ••••••••••

- **Password**: Check whether the login password is correct. If you forgot your password, reset the password. After you reset the password, restart the ECS for the new password to take effect.
- **Key pair**
  - For the first login, use an SSH key. For details, see **Remotely Logging In to a Linux ECS (Using an SSH Key Pair)**.
  - For a non-first login, if you want to use the remote login function (VNC) provided by the management console, log in to the ECS using the SSH key and set the password.

- **Set password later**: If you did not set a login mode when you create an ECS, you can reset the password on the ECS console by choosing **More** > **Reset Password** in the **Operation** column of the target ECS. After you reset the password, restart the ECS for the new password to take effect.

Checking Whether the ECS Is Overloaded

If the bandwidth or CPU usage of the ECS is excessively high, login failures may occur.

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

To resolve this issue, perform the operations described in **Why Is My Linux ECS Running Slowly?**

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

  You can also upgrade the vCPUs and memory by **modifying ECS 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 Know If My EIP Bandwidth Limit Has Been Exceeded?**

  If the bandwidth exceeds the limit, increase the bandwidth. For details, see **Changing an EIP Bandwidth**.

  NOTE

  If network jitter or packet loss occurs frequently, dynamic BGP may be used in cross-border access. In this case, you are advised to use premium BGP.

  For details, see **Why Is There Network Jitter or Packet Loss During Cross-Border Communications?**

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

Checking Whether an ECS Has an EIP Bound

If you need to use a remote login tool (such as PuTTY or Xshell) to access the ECS, bind an EIP to the ECS.

For details, see **Assigning an EIP**.

Checking Whether the Network Is Normal

Use a local PC in another network or use another hotspot to access the ECS. 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 ECS again.

Checking Whether the Security Group Is Correctly Configured

Check whether the local host can access port 22 on the ECS.

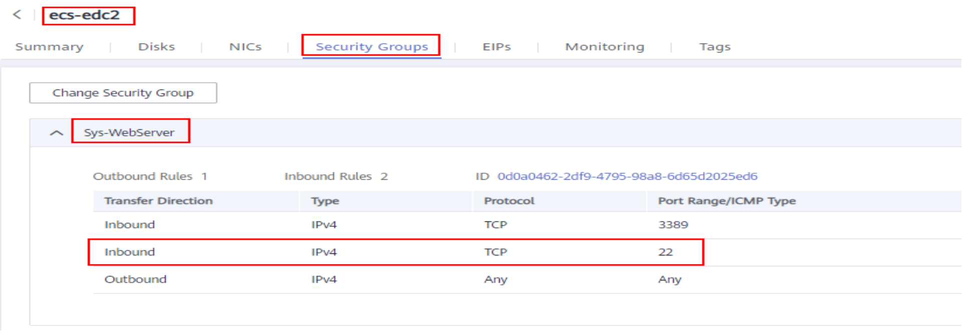
Run the following command to check whether port 22 is accessible:

telnet *ECS private IP address*

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

On the ECS details page, click the **Security Groups** tab and check that port 22 is configured in the inbound rule of the security group.

Figure 5-20 Checking remote access ports



Outbound Rules 1 Inbound Rules 2 ID 0d0a0462-2df9-4795-98a8-6d65d2025ed6

Transfer Direction	Type	Protocol	Port Range/ICMP Type
Inbound	IPv4	TCP	3389
Inbound	IPv4	TCP	22
Outbound	IPv4	Any	Any

For details about how to modify a security group rule, see **Modifying a Security Group Rule**.

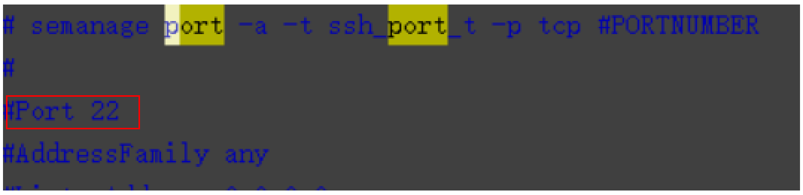
After you perform the preceding operations, try to remotely log in to the ECS again.

Checking Whether the Remote Access Port Is Correctly Configured

Check ECS settings.

1. Check whether the sshd process is running.
2. Check whether your local PC is denied by the ECS.
   a. Log in to the ECS and run the following command:
      vi /etc/hosts.deny
   b. If the IP address of the local PC is in the **hosts.deny** file, the ECS denies connection attempts from the local PC. In such a case, delete the IP address from the file.

3. Open the **/etc/ssh/ssh_config** file in the local PC and view the default login port. Then, open the **/etc/ssh/sshd_config** file in the ECS and check whether the SSH port is the default port 22.



```
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
```

After you perform the preceding operations, try to remotely log in to the ECS 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 ECSs, effectively preventing account cracking.

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

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 it has been enabled, 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 allowlist. Otherwise, you cannot remotely log in to your ECS through SSH.
- Exercise caution when adding a local IP address to the allowlist. This will make HSS no longer restrict access from this IP address to your ECSs.

For more details, see **Configuring Server Login Protection**.

Checking Whether an OS Fault Has Occurred

- Password injection failure

  The password failed to be injected using Cloud-Init.

  For details about how to install Cloud-Init, see **(Optional) Installing and Configuring Cloud-Init**.

- File system damaged after a forcible stop

  There is a low probability that the file system is damaged after a forcible stop, which causes the ECS fails to be restarted. For details, see **Why Does a Forcibly-Stopped Linux ECS Fail to Be Restarted?**

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

Checking Whether the Access Is Blocked by Antivirus Software

Third-party antivirus software may lead to a failure in accessing the ECS.

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

You can also disable or uninstall the third-party antivirus software and try to remotely log in to the ECS again.

Checking Whether an Error Occurred During a Remote Login

If an error message is displayed during remote login, check the operation guide based on the error information.

For more information, see **Remote Login Errors on Linux**.

If the fault persists, record the resource details and fault occurred time, and contact technical support for assistance.

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

5.2.5 What Should I Do If I Cannot Use MSTSC to Log In to an ECS Running the Windows Server 2012 OS?

Symptom

An ECS running the Windows Server 2012 OS has password authentication configured during ECS creation. When a user used the initial password and MSTSC to log in to the ECS, the login failed and the system displayed the message "You must change your password before logging on for the first time. Please update your password or contact your system administrator or technical support."

Possible Causes

The local computer used by the user is running the Windows 10 OS.

Due to limitations, the Windows 10 OS does not support remote logins to an ECS running the Windows Server 2012 OS using the initial password.

Solutions

- Solution 1

  Use a local computer running the Windows 7 OS to remotely log in to the ECS running the Windows Server 2012 OS.
- Solution 2

  Retain the original local computer and change the initial login password.

   a. Use VNC to log in to the ECS running the Windows Server 2012 OS for the first time.
   b. Change the login password as prompted.
   c. Use the changed password and MSTSC to log in to the ECS again.

- Solution 3:

  Retain the original local computer and initial login password.

   a. Choose **Start**. In the **Search programs and files** text box, enter **mstsc** and press **Enter**.

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

   b. Enter the EIP and click **Connect**. Then, use username **administrator** and the login password configured during ECS creation for connection.

      The connection fails, and the system displays the message "You must change your password before logging on for the first time. Please update your password or contact your system administrator or technical support."

   c. Click **Options** in the lower left corner of the **Remote Desktop Connection** page.
   d. On the **General** tab, click **Save As** in the **Connection settings** pane and save the remote desktop file in .rdp format.
   e. Open the .rdp file saved in **d**.
   f. Add the following statement to the last line of the .rdp file and save the file.

      enablecredsspsupport:i:0

   g. Double-click the edited .rdp file to set up the remote desktop connection.
   h. Click **Connect** to connect to the ECS running the Windows Server 2012 OS again.

5.2.6 How Can I Change a Remote Login Port?

Scenarios

This section describes how to change a port for remote logins.

Windows

The following procedure uses an ECS running Windows Server 2012 as an example. The default login port of a Windows ECS is 3389. To change it to port 2020, for example, do as follows:

1. Modify the security group rule.
   a. Log in to the **management console**.
   b. Click 📍 in the upper left corner and select a region and project.
   c. Click ☰. Under **Compute**, click **Elastic Cloud Server**.
   d. On the ECS list, click the name of an ECS for which you want to modify the security group rule.

e. On the ECS details page, click the security group in the **Security Groups** area to go to the security group details page.

f. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set **Protocol & Port** as follows:

- **Protocols**: TCP (Custom ports)
- **Port**: 2020

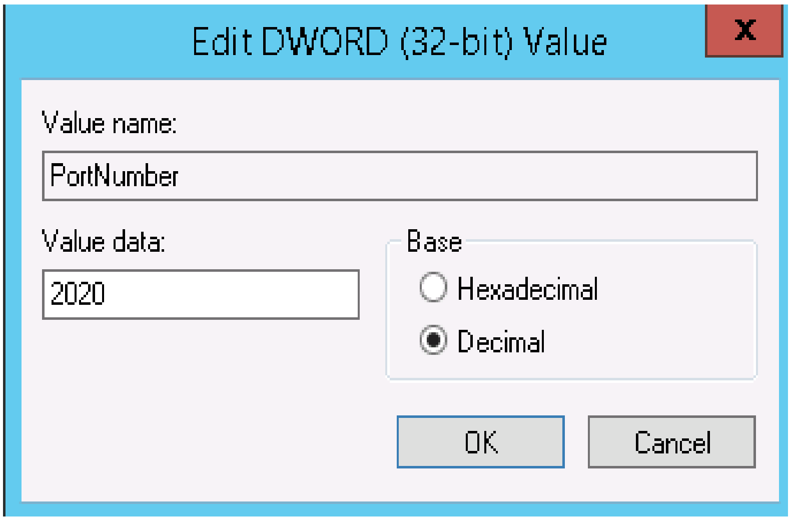
For details, see **Adding a Security Group Rule**.

2. Log in to the ECS.
3. In the **Run** dialog box, enter **regedit** to access the registry editor.
4. In **Registry Editor**, choose **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **Terminal Server** > **Wds** > **rdpwd** > **Tds** > **tcp** and double-click **PortNumber**.

a. In the dialog box that is displayed, set **Base** to **Decimal**.

b. Change the value in **Value data** to the new port number, which is **2020** in this example.

Figure 5-21 Changing the port number to 2020



Edit DWORD (32-bit) Value

Value name: PortNumber

Value data: 2020

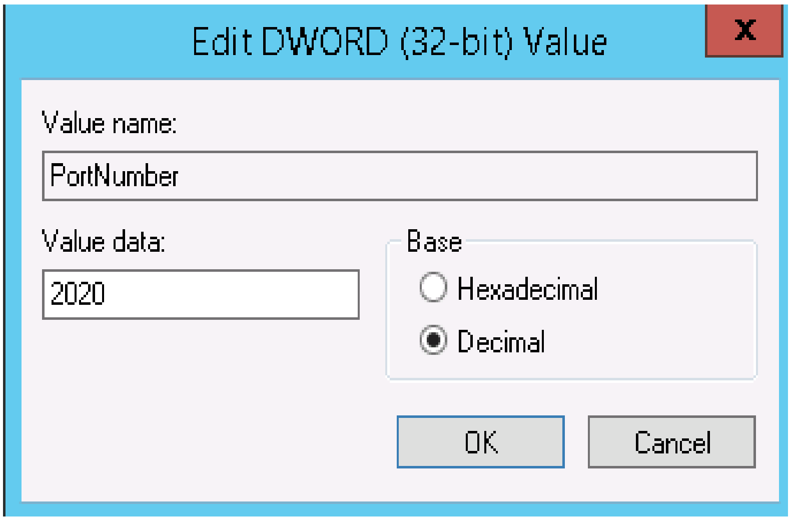
Base
○ Hexadecimal
● Decimal

5. In **Registry Editor**, choose **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **Terminal Server** > **WinStations** > **RDP-Tcp** and double-click **PortNumber**.

a. In the dialog box that is displayed, set **Base** to **Decimal**.

b. Change the value in **Value data** to the new port number, which is **2020** in this example.

Figure 5-22 Changing the port number to 2020



Value name: PortNumber

Value data: 2020

○ Hexadecimal

● Decimal

6. (Skip this step if the firewall is disabled.) Modify the inbound rules of the firewall.

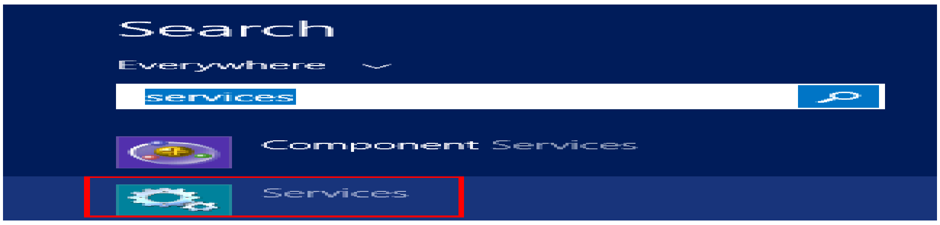
   Choose **Control Panel** > **Windows Firewall** > **Advanced Settings** > **Inbound Rules** > **New Rule**.

   - **Rule Type**: **Port**
   - Protocol in **Protocol and Ports**: **TCP**
   - Port in **Protocol and Ports**: **Specific local ports**, **2020** in this example
   - **Action**: **Allow the connection**
   - **Profile**: Default settings
   - **Name**: **RDP-2020**

   After the configuration, refresh the page to view the new rule.

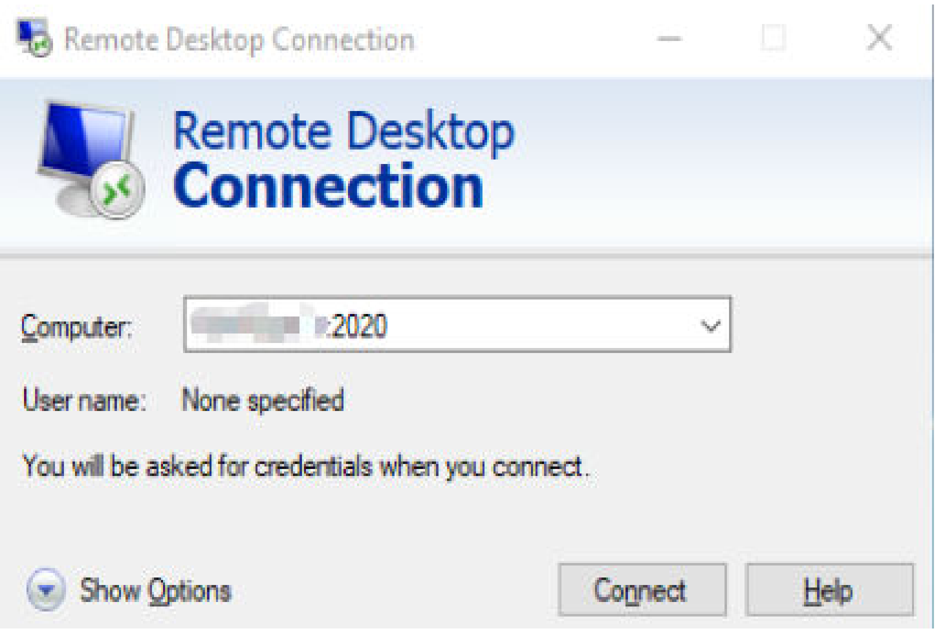
7. Open the Windows search box, enter **services**, and select **Services**.

Figure 5-23 Selecting Services



8. In the **Services** window, restart **Remote Desktop Services** or the ECS.
9. Use "IP address:Port" to remotely access the ECS.

Figure 5-24 Remote Desktop Connection



Computer: [redacted]:2020

User name: None specified

You will be asked for credentials when you connect.

Linux

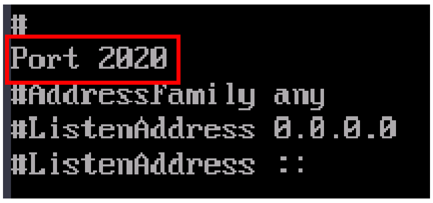
The following procedure uses an ECS running CentOS 7.3 as an example. The default login port of a Linux ECS is 22. To change it to port 2020, for example, do as follows:

1. Modify the security group rule.
   a. Log in to the **management console**.
   b. Click 📍 in the upper left corner and select a region and project.
   c. Click ☰ . Under **Compute**, click **Elastic Cloud Server**.
   d. On the ECS list, click the name of an ECS for which you want to modify the security group rule.
   e. On the ECS details page, click the security group in the **Security Groups** area to go to the security group details page.
   f. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set **Protocol & Port** as follows:
      - **Protocols**: TCP (Custom ports)
      - **Port**: 2020

      For details, see **Adding a Security Group Rule**.
2. Log in to the ECS.
3. Run the following command to edit the sshd configuration file:

   ```
   vi /etc/ssh/sshd_config
   ```
4. Delete the comment tag (#) from the **#port 22** line and change **22** to **2020**.

Figure 5-25 Changing the port number to 2020



```
#
Port 2020
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

5. Press **Esc** to exit Insert mode and enter **:wq!** to save the settings and exit.
6. Run either of the following commands to restart sshd:

   service sshd restart

   Or

   systemctl restart sshd
7. Skip this step if the firewall is disabled. Configure the firewall.

   The firewall varies depending on the CentOS version. CentOS 7 uses firewalld, and CentOS 6 uses iptables. The following operations use CentOS 7 as an example.

   Run the **firewall-cmd --state** command to check the firewall status.
   - (Recommended) Method 1: Add information about a new port to firewalld.
     1. Run the following commands to add a rule for port 2020:

        firewall-cmd --zone=public --add-port=2020/tcp --permanent

        firewall-cmd --reload
     2. View the added port. The TCP connection of port 2020 will have been added.

        firewall-cmd --list-all
     3. Restart firewalld.

        systemctl restart firewalld.service
   - Method 2: Disable the firewall and the function of automatically enabling the firewall upon ECS startup.

     systemctl stop firewalld

     systemctl disable firewalld
8. Run the following command to check whether the port is open:

   telnet ***EIP port***

   For example: **telnet** ***xx.xx.xx.xx*** **2020**

5.2.7 Why Cannot I Use a Non-Default SSH Port to Log In to My Linux ECS?

Symptom

After changing the default SSH port, you could not use the new port to log in to the ECS.

Possible Causes

- The access to the new port is not allowed in the security group.
- The new port is not enabled on the firewall.
- The new port is not added to the SSH configuration file.
- The hosts configuration file is incorrectly configured.

Checking Security Group Rules

Check whether the security group is correctly configured.

For example, if the new SSH port number is 2020, ensure that there is a security group rule without restriction in the outbound direction and allowing access to this port in the inbound direction.

Checking Firewall Rules

Run the **iptables** command to check whether the new SSH port, for example, port 2020 is enabled on the firewall.

1. Log in to the Linux ECS.
2. Take CentOS 7.5 as an example. Run the following command to edit the iptables file:

   vi /etc/sysconfig/iptables
3. Add a rule for port 2020.
   ```
   -A INPUT -m state -state NEW -m tcp -p tcp -dport 2020 -j ACCEPT
   ```
4. Restart iptables.

   systemctl restart iptables

Checking the SSH Configuration File

Log in to the ECS and check the SSH configuration file.

1. Run the following command to check whether port 2020 has been configured:

   vi /etc/ssh/sshd_config
2. If the port has not been configured, replace **#Port 22** with **Port 2020**.
3. Run the following command to restart SSH:

   service sshd restart

Checking the hosts Configuration File

The **/etc/hosts.allow** and **/etc/hosts.deny** files of a Linux ECS are used to permit or deny an IP address or an IP address segment, respectively, to remotely access the ECS using SSH.

1. Add the following statement to **/etc/hosts.allow** to allow the IP address 192.168.1.3 to access the ECS using SSH:
   ```
   sshd: 192.168.1.3
   ```
2. Check **/etc/hosts.deny**. If **sshd:all:deny** is contained, comment it out.

NOTE

If a rule is set in both **hosts.allow** and **hosts.deny**, the rule in **hosts.allow** takes precedence. For example, if "sshd: 192.168.1.3" is set in **hosts.allow** and "sshd:all:deny" is set in **hosts.deny**, the ECS allows only the SSH login from IP address 192.168.1.3.

5.2.8 Why Can't I Obtain the Password for Logging In to My Windows ECS Authenticated Using a Key Pair?

Symptom

A private key cannot be used to obtain the password for logging in to a Windows ECS that is authenticated using a key pair.

Possible Causes

The password fails to inject using Cloudbase-Init due to:

- A network fault, leading to the failure of the connection from the ECS to the Cloudbase-Init server.
- No configuration on the image for Cloudbase-Init to obtain the password.
- Other reasons.

Solution

If logging in to an ECS with Cloudbase-Init enabled failed, perform the following operations to locate the fault:

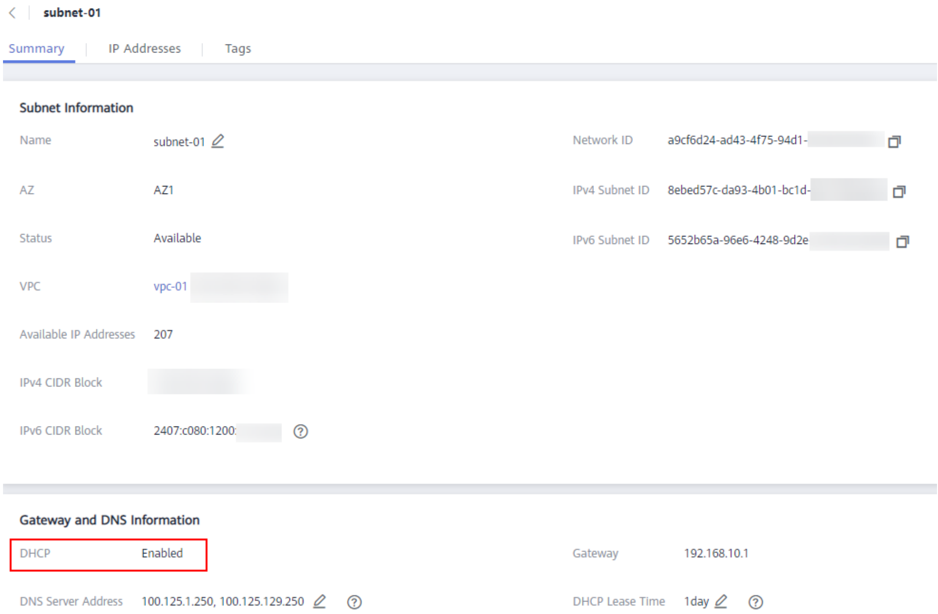
1. Ensure that Cloudbase-Init has been correctly configured on the image that was used to create the ECS.
   - If Cloudbase-Init has not been configured, your ECS will not allow customized configurations, and you can log in to it only by using the original image password.
   - The ECSs created using a public image have Cloudbase-Init installed by default. You do not need to install and configure Cloudbase-Init anymore.
   - If you created your ECS by using an external image file, install and configure Cloudbase-Init.

     For details, see **Installing and Configuring Cloudbase-Init**.
2. Ensure that the key pair for logging in to the ECS is correct.

   The key used for obtaining the password must be the key used during the ECS creation.
3. Ensure that DHCP is enabled in the VPC to which the ECS belongs.

   On the management console, check whether DHCP has been enabled in the target subnet.

Figure 5-26 DHCP



Subnet Information

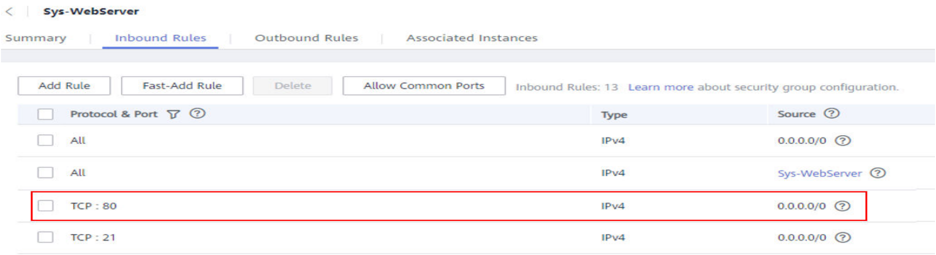
Name	subnet-01	Network ID	a9cf6d24-ad43-4f75-94d1-[redacted]
AZ	AZ1	IPv4 Subnet ID	8ebed57c-da93-4b01-bc1d-[redacted]
Status	Available	IPv6 Subnet ID	5652b65a-96e6-4248-9d2e[redacted]
VPC	vpc-01[redacted]		
Available IP Addresses	207		
IPv4 CIDR Block	[redacted]		
IPv6 CIDR Block	2407:c080:1200:[redacted]		

Gateway and DNS Information

DHCP	Enabled	Gateway	192.168.10.1
DNS Server Address	100.125.1.250, 100.125.129.250	DHCP Lease Time	1day

4. Ensure that the ECS has an EIP bound.
5. Ensure that traffic to and from port 80 is allowed in security group rules.

Figure 5-27 Security group rules for port 80

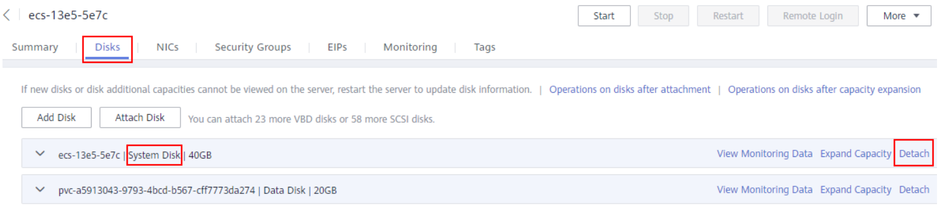


Inbound Rules: 13 Learn more about security group configuration.

Protocol & Port	Type	Source
All	IPv4	0.0.0.0/0
All	IPv4	Sys-WebServer
TCP : 80	IPv4	0.0.0.0/0
TCP : 21	IPv4	0.0.0.0/0

6. Check Cloudbase-Init logs to identify the cause.
   a. Stop the affected ECS and detach the system disk from it.

Figure 5-28 Detaching the system disk



If new disks or disk additional capacities cannot be viewed on the server, restart the server to update disk information. | Operations on disks after attachment | Operations on disks after capacity expansion

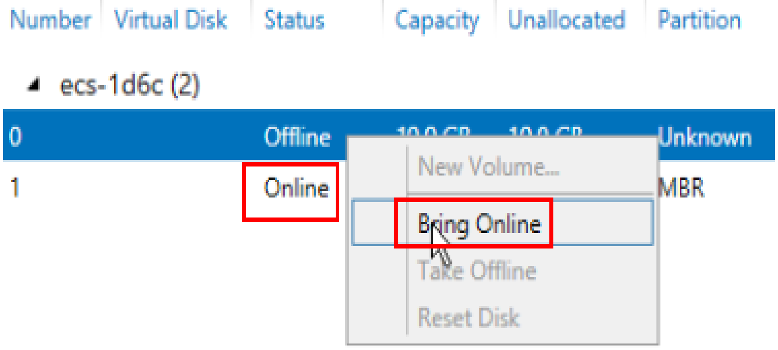
You can attach 23 more VBD disks or 58 more SCSI disks.

ecs-13e5-5e7c | System Disk | 40GB

pvc-a5913043-9793-4bcd-b567-cff7773da274 | Data Disk | 20GB

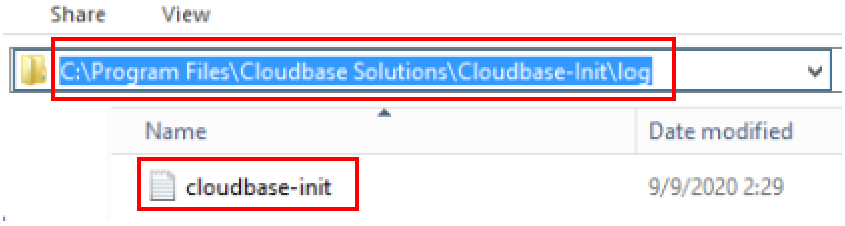
   b. Use a public image to create a temporary Windows ECS and attach the system disk detached in 6.a to the ECS.
   c. Log in to the temporary ECS, open the **Server Manager** page, choose **File and Storage Services** > **Volumes** > **Disks**, right-click the offline disk, and choose **Online** from the shortcut menu.

Figure 5-29 Setting disk online



d. Switch to the **cloudbase-init** file in **/Program Files/Cloudbase Solution/Cloudbase-Init/log** of this disk to view the log for fault locating.

Figure 5-30 cloudbase-init



C:\Program Files\Cloudbase Solutions\Cloudbase-Init\log

cloudbase-init 9/9/2020 2:29

5.2.9 What Browser Version Is Required to Remotely Log In to an ECS?

When you use a browser to remotely log in to an ECS, ensure that the browser version meets the requirements listed in **Table 5-3**.

Table 5-3 Browser version requirements

Browser	Version
Google Chrome	31.0 or later
Mozilla Firefox	27.0 or later
Internet Explorer	10.0 or later
Microsoft Edge	12.0 or later

5.2.10 What Should I Do If I Cannot Access a Windows Server 2012 OS After Uninstalling Some Software?

Issue Description

Installing applications on a Windows Server 2012 OS requires .net framework 3.5, and .net framework 4.5 delivered with the OS must be uninstalled. However, after the uninstallation, blank screen occurs or OS login fails.

Possible Causes

After .net framework 4.5 is uninstalled, the system mode is changed from full to core, and the system desktop is not enabled.

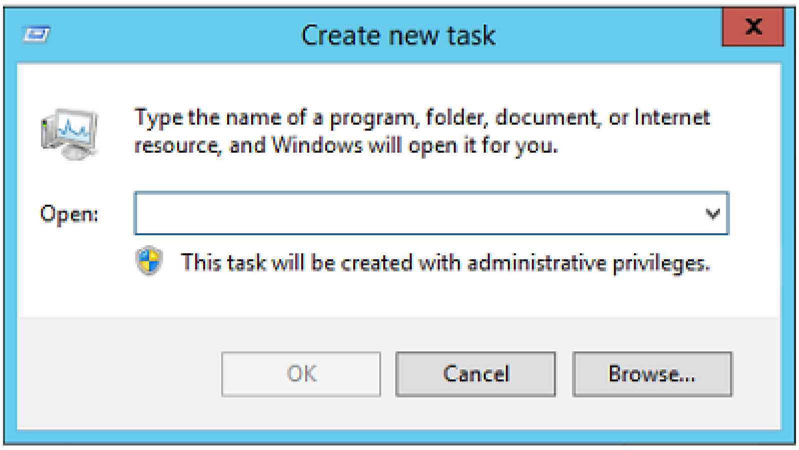
Handling Method

To handle this issue, perform the following operations to change the core mode back to full:

1. Log in to the ECS.
2. In the upper right corner, click **Send CtrlAltDel** and start the task manager.
3. Choose **File** > **Run new task**.

   The **Create new task** page is displayed.

   Figure 5-31 Creating a new task

   Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

   This task will be created with administrative privileges.

4. In the **Open** text box, type **cmd** and press **Enter**.
5. Run the following command to change the system mode from core to full:

   Dism /online /enable-feature /all /featurename:Server-Gui-Mgmt /featurename:Server-Gui-Shell /featurename:ServerCore-FullServer
6. After about 10 minutes, the system displays a message, asking you whether to restart the system. In such a case, press **Y** to restart the system.

   You can access the desktop after logging in to the ECS again.

5.2.11 How Can I Log In to an ECS After It Exchanged the System Disk with Another ECS Running the Same OS?

Symptom

Two pay-per-use ECSs run the same OS, for example, both run Windows or Linux. The system disks attached to the two stopped ECSs are exchanged. After the exchange, the passwords or keys used to log in to the ECSs may change. In this case, how do I log in to the ECS whose system disk has been replaced?

NOTE

Before stopping an ECS for disk detachment, release the IP address assigned to the ECS using DHCP so that ECS can correctly obtain an IP address later. To do so, perform the following operations:

1. Log in to the Windows ECS.
2. Run the following command to release the IP address:

   ipconfig /release

   This operation will interrupt network connections and affect the use of the ECS. After the ECS is restarted, network connections will automatically recover.

Windows

Login methods vary according to the login authentication used on the ECSs. Assume that there are three Windows ECSs and they are configured as shown in Table 5-4.

Table 5-4 ECS configurations

ECS	System Disk	Login Authentication	Password/Key Pair
ecs_01	vol_01	Password or key pair	If a password is used for login authentication, take **Ecs@01** as an example. If a key pair is used for login authentication, take private key file **Keypair_01** as an example.
ecs_02	vol_02	Password	Ecs@02
ecs_03	vol_03	Key pair	Keypair_03

- Scenario 1: System disk vol_01 is detached from ecs_01 offline and then attached to ecs_02 as the system disk. How can I log in to ecs_02?

  After ecs_02 starts up, use its initial password **Ecs@02** to log in to the ECS.
- Scenario 2: System disk vol_01 is detached from ecs_01 offline and then attached to ecs_03 as the system disk. How can I log in to ecs_03?

  The random password for logging in to ecs_03 must be resolved again. The procedure is as follows:

  a. Delete the initial password for logging in to ecs_03.

     Locate the row containing ecs_03, click **More** in the **Operation** column, and select **Delete Password** from the drop-down list. Then, click **OK**.

     NOTE

     The ecs_03 must be stopped.

  b. Start ecs_03.

Locate the row containing ecs_03, click **More** in the **Operation** column, and select **Start** from the drop-down list. Then, in the **Start ECS** dialog box, click **OK**.

c. Obtain the password for logging in to ecs_03.
   i. Locate the row that contains **ecs_03**, click **More** in the **Operation** column and choose **Get Password**.
   ii. Click **Select File** and upload private key file **Keypair_03** of ecs_03.
   iii. Click **Get Password** to obtain a new random password.

d. Use the random password obtained in step **c** to log in to ecs_03 with the system disk replaced.

Linux

Login methods vary according to the login authentication used on the ECSs. Assume that there are three Linux ECSs and they are configured as shown in **Table 5-5**.

Table 5-5 ECS configurations

ECS	System Disk	Login Authentication	Password/Key Pair
ecs_01	vol_01	Password or key pair	If a password is used for login authentication, take **Ecs@01** as an example. If a key pair is used for login authentication, take private key file **Keypair_01** as an example.
ecs_02	vol_02	Password	Ecs@02
ecs_03	vol_03	Key pair	Keypair_03

- Scenario 1: System disk vol_01 is detached from ecs_01 offline and then attached to ecs_02 as the system disk. How can I log in to ecs_02?

  Use either of the following methods to log in to ecs_02:
  - Use private key file **Keypair_01** (if available) of ecs_01.
  - Use the original password **Ecs@02** of ecs_02.
- Scenario 2: System disk vol_01 is detached from ecs_01 offline and then attached to ecs_03 as the system disk. How can I log in to ecs_03?

  Use one of the following methods to log in to ecs_03:
  - Use the password **Ecs@01** (if available) of ecs_01.
  - Use private key file **Keypair_01** (if available) of ecs_01.
  - Use private key file **Keypair_03** of ecs_03.

5.2.12 Why Does the System Display a Message Indicating that the Password for Logging In to an ECS Cannot Be Obtained?

Symptom

Password authentication is required to log in to a Windows ECS. Therefore, you require a key file to obtain the initial password for logging in to the ECS. However, after you click **Get Password**, the system displays a message indicating that the password could not be obtained, resulting in an ECS login failure.

Possible Causes

Possible causes vary depending on the image used to create the Windows ECS.

- Cause 1: The image used to create the Windows ECS is a private image, on which Cloudbase-Init has not been installed.
- Cause 2: Cloudbase-Init has been installed on the image, but the key pair has not been obtained when the Windows ECS was created.

Solution

- If the issue is a result of cause 1, proceed as follows:

  If a private image is created without Cloudbase-Init installed, the ECS configuration cannot be customized. As a result, you can log in to the ECS only using the original image password.

  The original image password is the OS password configured when the private image was created.

  If the original image password has been forgotten, reset the password on the ECS console.
- If the issue is a result of cause 2, proceed as follows:
  a. Locate the row containing the target ECS, click **More** in the **Operation** column, and select **Restart**.
  b. After the reset, click **More** in the **Operation** column and choose **Get Password** to check whether the password can be obtained.
     - If you can obtain the password, no further action is required.
     - If you cannot obtain the password, contact customer service.

5.2.13 How Can I Change the Resolution of a Windows ECS?

Scenarios

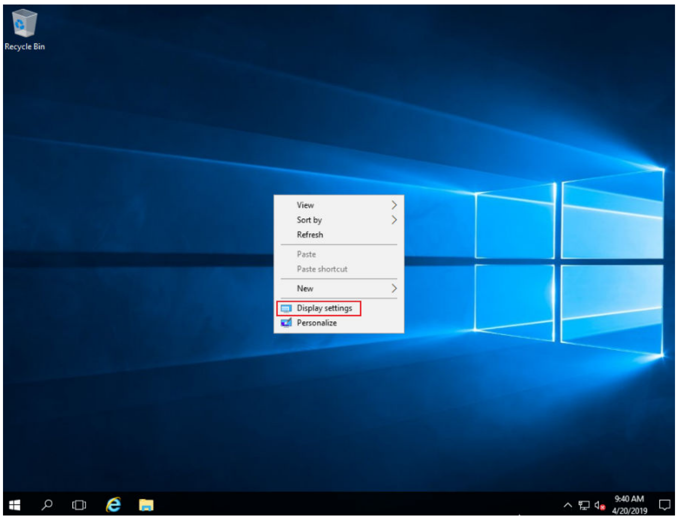
You can change the resolution of Windows ECSs.

Solution 1: Using VNC

The operations of changing an ECS resolution vary according to the Windows OS. This section uses the Windows Server 2016 Standard 64-bit edition as an example to describe how to change the resolution of a Windows ECS.

1. Log in to the ECS using VNC.
2. Right-click the desktop and choose **Display settings** from the shortcut menu.

Figure 5-32 Display settings

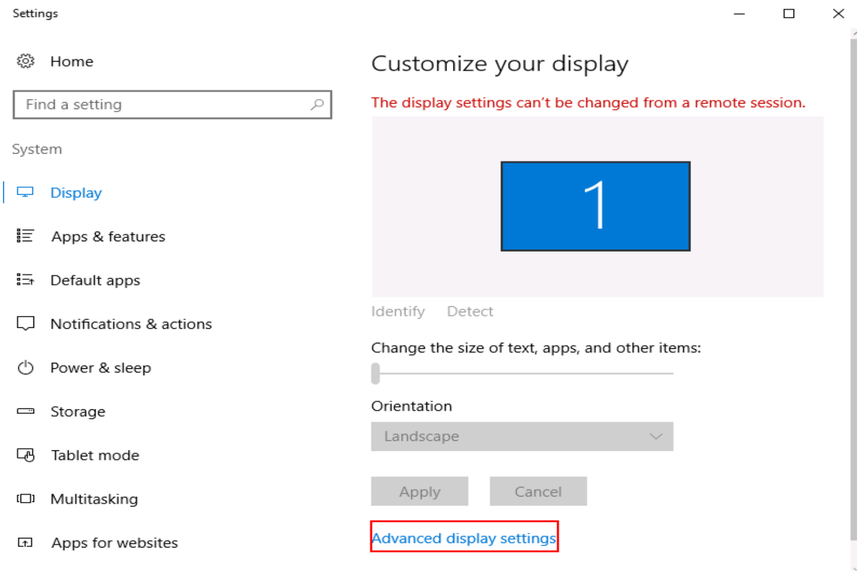


3. On the **Settings** page, click the **Display** tab and then **Advanced display settings**.

NOTE

If the remote desktop is not fully displayed, set **Change the size of text, apps, and other items** to **100%**.

Figure 5-33 Settings



Customize your display

The display settings can't be changed from a remote session.

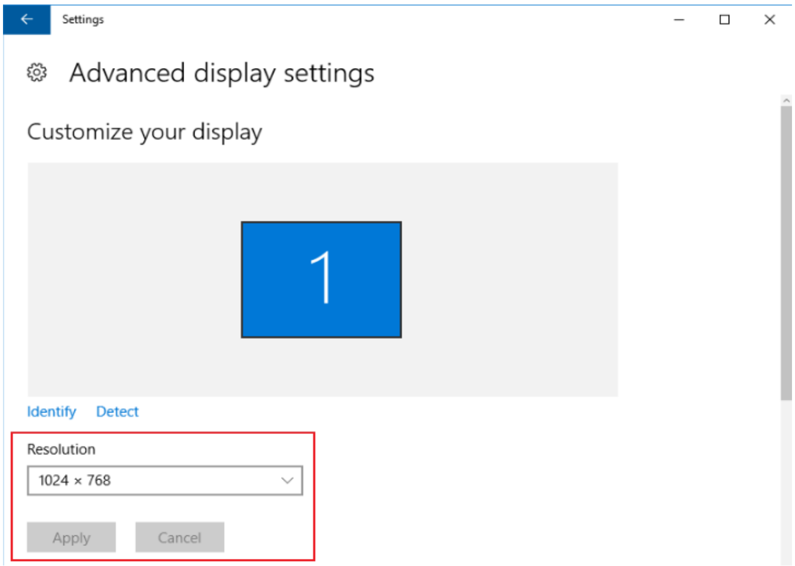
Change the size of text, apps, and other items:

Orientation

Landscape

4. In the **Resolution** drop-down list, select the desired resolution.

Figure 5-34 Setting a resolution



Resolution: 1024 × 768

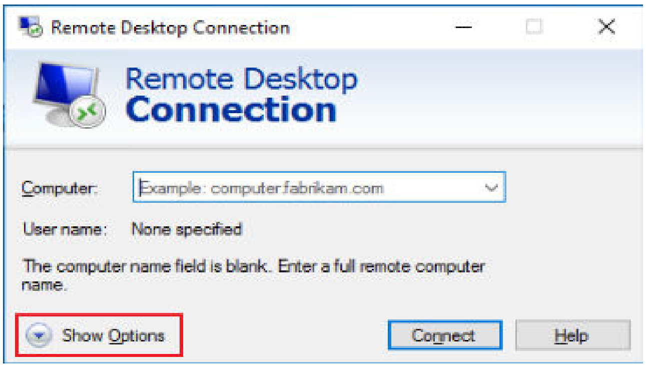
5. Click **Apply**.

Solution 2: Using MSTSC

Before remotely logging in to your ECS using MSTSC, change the resolution of the Windows ECS.

1. On your local computer (client), click **Start**.
2. In the **Search programs and files** text box, enter **mstsc**.
3. In the **Remote Desktop Connection** window, click **Show Options** in the lower left corner.

Figure 5-35 Remote Desktop Connection



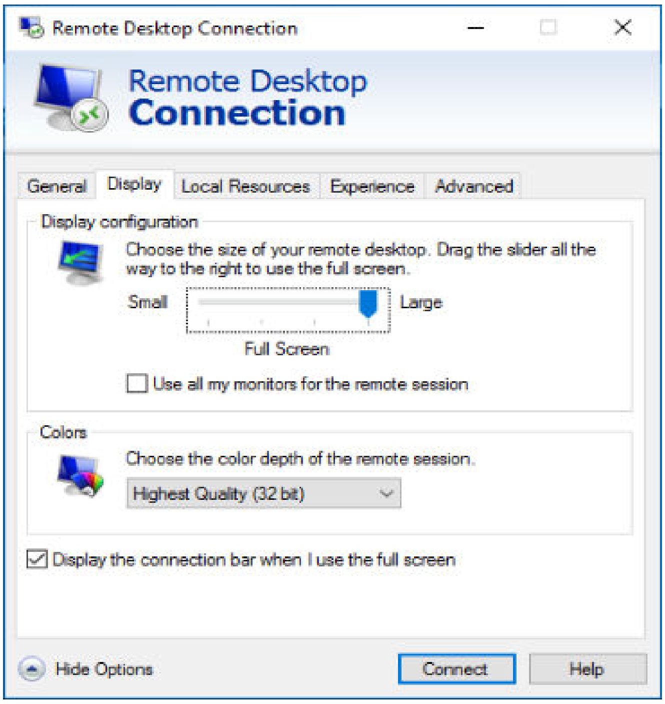
Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

4. Click the **Display** tab. Then, in the **Display configuration** pane, set the resolution.

Figure 5-36 Display



Display configuration

Choose the size of your remote desktop. Drag the slider all the way to the right to use the full screen.

Full Screen

☐ Use all my monitors for the remote session

Colors

Choose the color depth of the remote session.

Highest Quality (32 bit)

☑ Display the connection bar when I use the full screen

5. Use MSTSC to log in to the ECS.

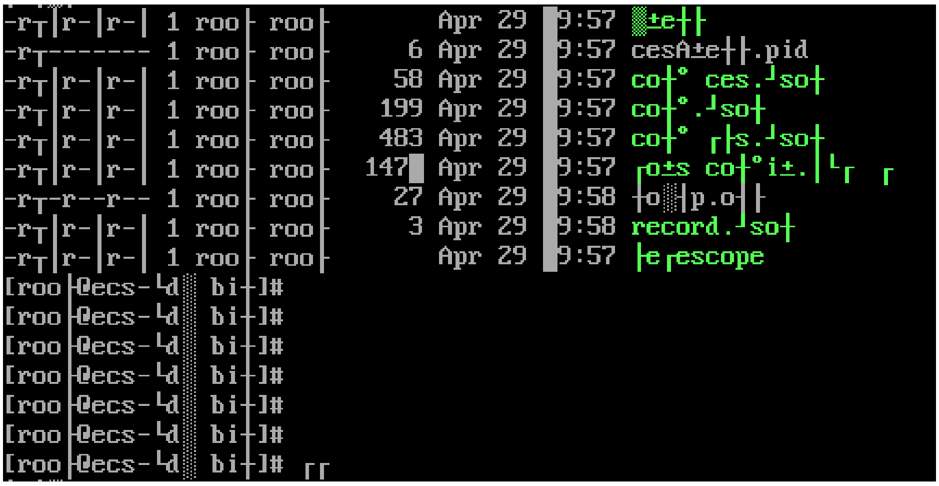
5.3 VNC Login

5.3.1 Why Are Garbled Characters Displayed When I Log In to My ECS Using VNC?

Symptom

After I attempt to log in to my Linux ECS using VNC, garbled characters are displayed, as shown in **Figure 5-37**.

Figure 5-37 Garbled characters on the VNC-based login page



```
-r┬│r-│r-│ 1 roo├ roo├      Apr 29 █9:57 ▓±e┼├
-r┬------- 1 roo├ roo├    6 Apr 29 █9:57 cesA±e┼├.pid
-r┬│r-│r-│ 1 roo├ roo├   58 Apr 29 █9:57 co┼° ces.┘so┼
-r┬│r-│r-│ 1 roo├ roo├  199 Apr 29 █9:57 co┼°.┘so┼
-r┬│r-│r-│ 1 roo├ roo├  483 Apr 29 █9:57 co┼° ┌├s.┘so┼
-r┬│r-│r-│ 1 roo├ roo├ 147█ Apr 29 █9:57 ┌o±s co┼°i±.│└┌  ┌
-r┬-r--r-- 1 roo├ roo├   27 Apr 29 █9:58 ┼o░┤p.o┤├
-r┬│r-│r-│ 1 roo├ roo├    3 Apr 29 █9:58 record.┘so┼
-r┬│r-│r-│ 1 roo├ roo├      Apr 29 █9:57 ├e┌escope
[roo├@ecs-└d░ bi┼]#
[roo├@ecs-└d░ bi┼]#
[roo├@ecs-└d░ bi┼]#
[roo├@ecs-└d░ bi┼]#
[roo├@ecs-└d░ bi┼]#
[roo├@ecs-└d░ bi┼]#
[roo├@ecs-└d░ bi┼]# ┌┌
```

Possible Causes

The **cat** command was executed to display a large binary file, leading to garbled characters.

Solution

Log in to the ECS as user **root** and run the following command for recovery:

reset

NOTE

The **reset** command is used to re-initialize the ECS and refresh the terminal display. After the **reset** command is executed, the garbled characters are cleared and the fault is rectified.

5.3.2 What Should I Do If the Page Does not Respond After I Log In to an ECS Using VNC and Do Not Perform Any Operation for a Long Period of Time?

If you log in to an ECS running Windows 7 through VNC using Internet Explorer 10 or 11 and do not perform any operation for a long time, the VNC page may not respond.

In this case, you can click **AltGr** twice on the VNC page to activate the page.

If the fault persists, contact technical support.

5.3.3 What Should I Do If I Cannot View Data After Logging In to an ECS Using VNC?

After you log in to an ECS using VNC and view data, for example, play videos or run the **cat** command to view large files in Linux OSs, VNC may become unavailable due to the high memory usage of the browser.

In such a case, use another browser and log in to the ECS again.

If the fault persists, contact technical support.

5.3.4 Why Does a Blank Screen Appear After I Attempted to Log In to an ECS Using VNC?

The blank screen means that another user has logged in to this ECS using VNC, so you were logged out.

Only one user can be logged in to an ECS using VNC at a time. If you are already logged in and another user logs in to the same ECS, you will be automatically logged out.

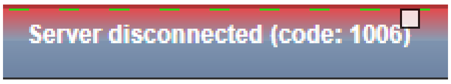
You can log back in, but that will kick the other user out.

5.3.5 What Should I Do If Error Code 1006 or 1000 Is Displayed When I Log In to an ECS Through the Management Console?

Symptom

When I attempted to remotely log in to an ECS using VNC, the system displayed error code 1006, as shown in **Figure 5-38**.

Figure 5-38 Error message displayed in a VNC-based remote login



Server disconnected (code: 1006)

Possible Causes

- The ECS is abnormal.
- Another user has logged in to the ECS.
- No operations are performed on the ECS and it is automatically disconnected.

Troubleshooting

1. Log in to the ECS again using VNC.
   - If the login is successful, no further action is required.
   - If the fault persists, go to **2**.
2. Check whether the ECS is normal.

   Error code 1006 is displayed if the ECS is stopped, deleted, being migrated or restarted, or encounters a connection timeout.
3. Check whether another user has logged in to the ECS.

   If yes, you can log in to the ECS only after that user logs out.

5.3.6 Why No Audio File Can Be Properly Played on My Windows ECS Logged In Using VNC?

Symptom

When I logged in to my Windows ECS using MSTSC, audio files can be properly played. However, when I logged in to that ECS using VNC, audio files failed to be played.

Possible Causes

VNC does not support audio playing.

Solution

Use your local PC (running Windows 7, for example) to play the audio files.

1. Start your local PC.

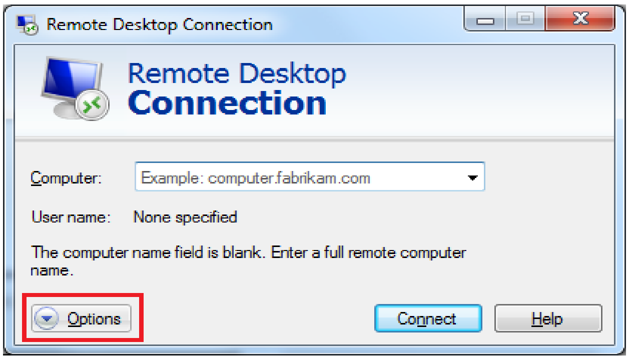
   NOTE

   Start your local PC, instead of logging in to your Windows ECS.

2. Press **Win+R** to start the **Run** text box.
3. Enter **mstsc** and click **OK**.

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

Figure 5-39 Remote Desktop Connection



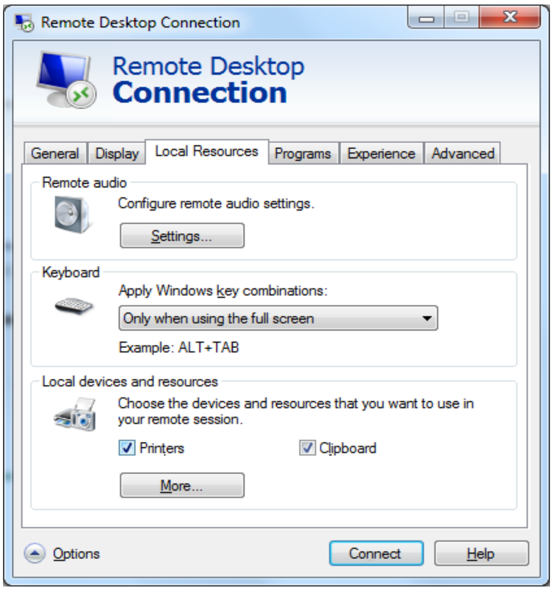
Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

4. Click **Options** in the lower left corner and click the **Local Resources** tab.

Figure 5-40 Local Resources



Configure remote audio settings.

Apply Windows key combinations: Only when using the full screen

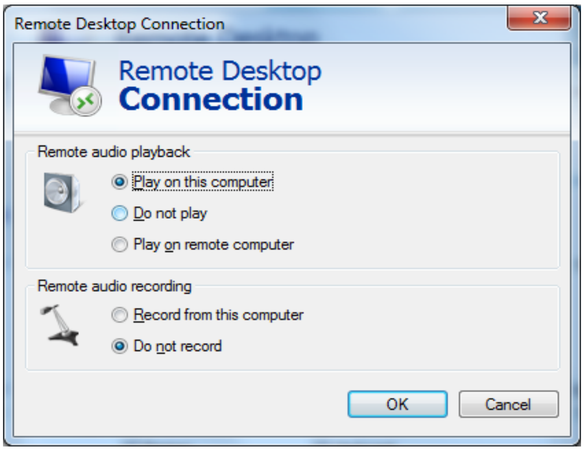
Example: ALT+TAB

Choose the devices and resources that you want to use in your remote session.

☑ Printers ☑ Clipboard

5. In the **Remote audio** pane, click **Settings**.

Figure 5-41 Setting remote audio playback



6. In the **Remote audio playback** pane, select **Play on this computer**.

5.4 Remote Login Errors on Windows

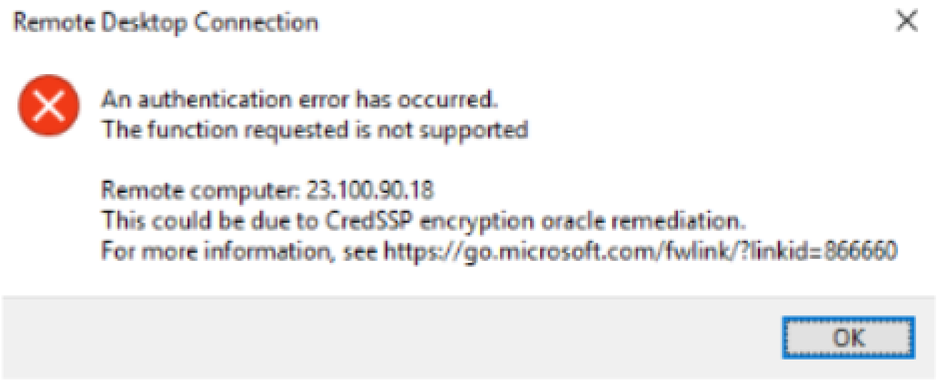
5.4.1 Why Does an Authentication Failure Occurs After I Attempt to Remotely Log In to a Windows ECS?

Symptom

When a local computer running Windows attempts to access a Windows ECS using RDP (for example, MSTSC), an identity authentication failure occurs and the desired function is not supported.

- If the error message contains only the information that an identity authentication failure occurs and that the desired function is not supported, rectify the fault by following the instructions provided in **Solution**.
- If the error message shows that the fault was caused by "CredSSP Encryption Oracle Remediation", as shown in **Figure 5-42**, the fault may be caused by a security patch released by Microsoft in March 2018. This patch may affect RDP-based CredSSP connections. As a result, setting up RDP-based connections to ECSs failed. Rectify the fault by following the instructions provided in the official Microsoft document *CredSSP updates for CVE-2018-0886*.

Figure 5-42 Failed to set up a remote desktop connection



An authentication error has occurred.
The function requested is not supported

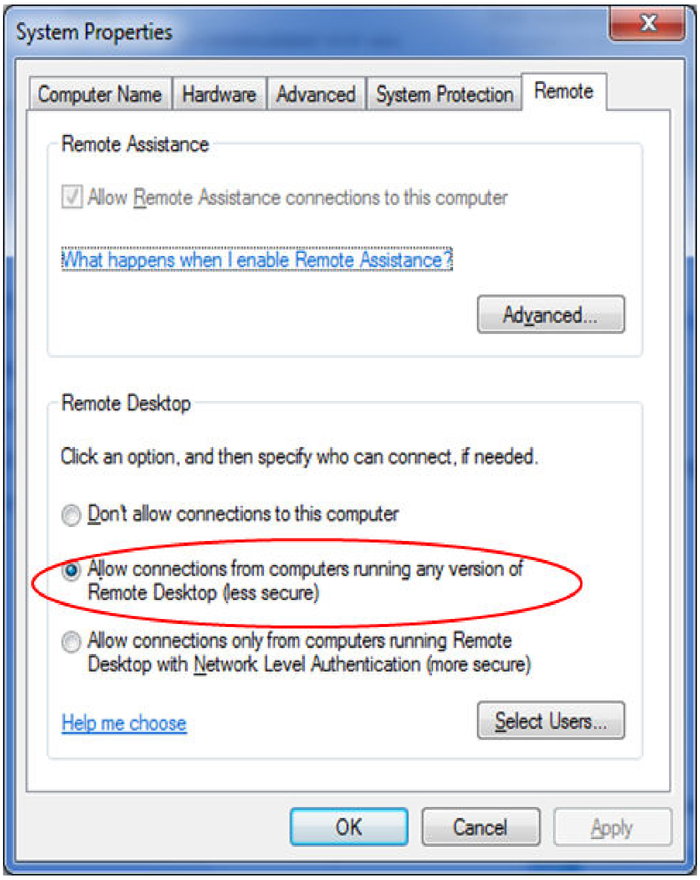
Remote computer: 23.100.90.18
This could be due to CredSSP encryption oracle remediation.
For more information, see https://go.microsoft.com/fwlink/?linkid=866660

Solution

Modify the remote desktop connection settings on the Windows ECS:

1. Log in to the ECS.
2. Click **Start** in the lower left corner, right-click **Computer**, and choose **Properties** from the shortcut menu.
3. In the left navigation pane, choose **Remote settings**.
4. Click the **Remote** tab. In the **Remote Desktop** pane, select **Allow connections from computers running any version of Remote Desktop (less secure)**.

Figure 5-43 Remote settings



Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

● Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

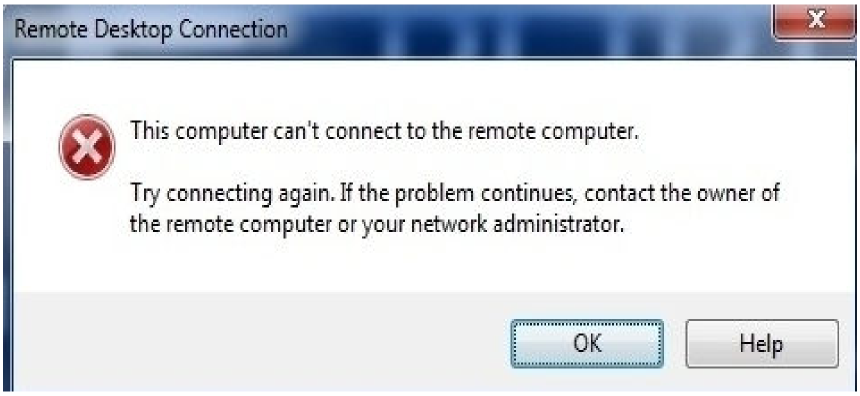
5. Click **OK**.

5.4.2 Why Can't I Use the Local Computer to Connect to My Windows ECS?

Symptom

An error message is displayed indicating that your local computer cannot connect to the remote computer.

Figure 5-44 Cannot connect to the remote computer



This computer can't connect to the remote computer.

Try connecting again. If the problem continues, contact the owner of the remote computer or your network administrator.

Possible Causes

- Port 3389 of the security group on the ECS is disabled. For details, see **Checking Port Configuration on the ECS**.
- The firewall on the ECS is disabled. For details, see **Checking Whether the Firewall Is Correctly Configured**.
- The remote desktop connection is not correctly configured. For details, see **Checking Remote Desktop Connection Settings**.
- Remote Desktop Services are not started. For solution, see **Checking Remote Desktop Services**.
- Remote Desktop Session Host is not correctly configured. For details, see **Checking Remote Desktop Session Host Configuration**.

Checking Port Configuration on the ECS

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

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

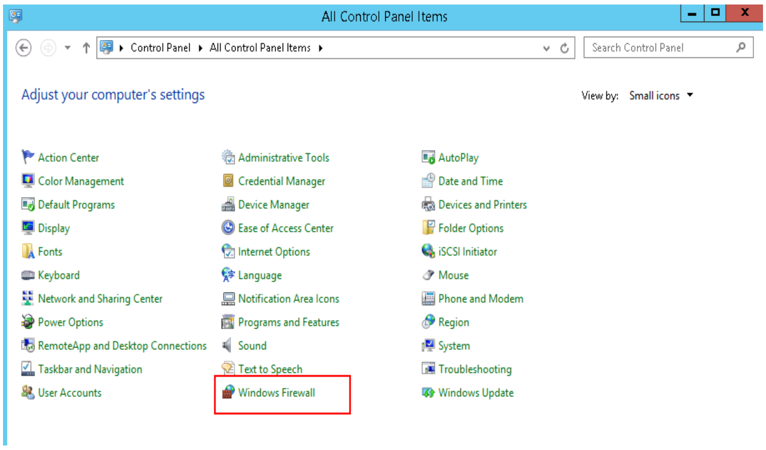
On the ECS details page, click the **Security Groups** tab and check port 3389 in the inbound rule of the security group.

Checking Whether the Firewall Is Correctly Configured

Check whether the firewall is enabled on the ECS.

1. Log in to the ECS using VNC available on the management console.
2. Click the Windows icon in the lower left corner of the desktop and choose **Control Panel** > **Windows Firewall**.

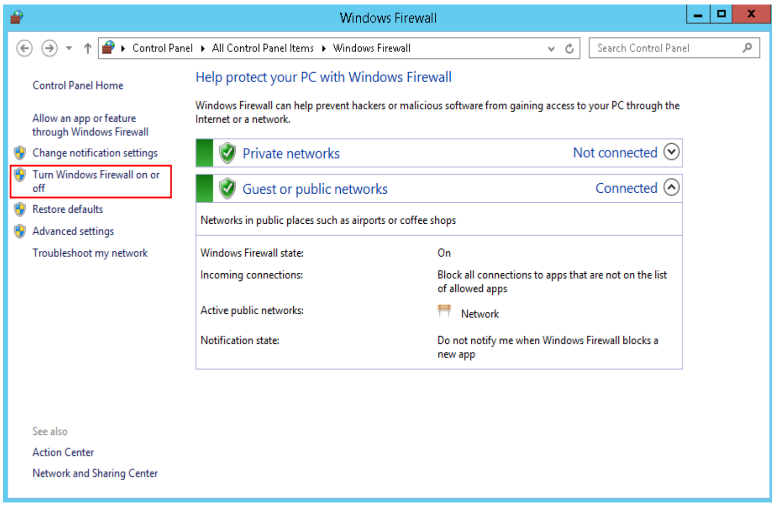
Figure 5-45 Windows Firewall



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

   View and set the firewall status.

Figure 5-46 Checking firewall status


Windows Firewall
Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

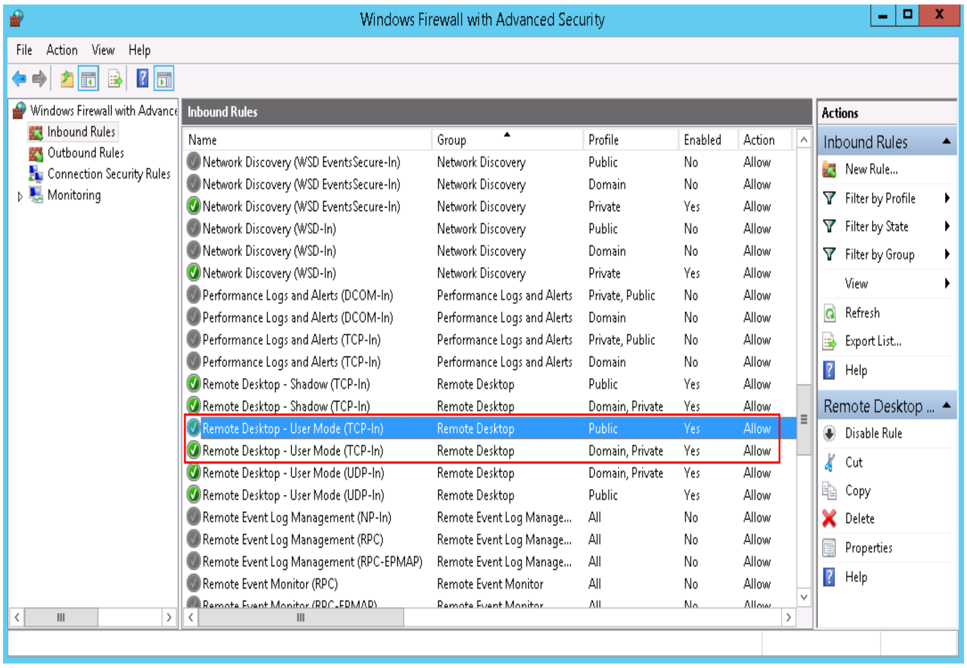
Active public networks: Network

Notification state: Do not notify me when Windows Firewall blocks a new app

To enable Windows firewall, perform the following steps:

4. Click **Advanced settings**.
5. Check **Inbound Rules** and ensure that the following rules are enabled:
   - Remote Desktop - User Mode (TCP-In), Public
   - Remote Desktop - User Mode (TCP-In), Domain, Private

Figure 5-47 Inbound Rules



Inbound Rules

Name	Group	Profile	Enabled	Action
Network Discovery (WSD EventsSecure-In)	Network Discovery	Public	No	Allow
Network Discovery (WSD EventsSecure-In)	Network Discovery	Domain	No	Allow
Network Discovery (WSD EventsSecure-In)	Network Discovery	Private	Yes	Allow
Network Discovery (WSD-In)	Network Discovery	Public	No	Allow
Network Discovery (WSD-In)	Network Discovery	Domain	No	Allow
Network Discovery (WSD-In)	Network Discovery	Private	Yes	Allow
Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Private, Public	No	Allow
Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Domain	No	Allow
Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Private, Public	No	Allow
Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Domain	No	Allow
Remote Desktop - Shadow (TCP-In)	Remote Desktop	Public	Yes	Allow
Remote Desktop - Shadow (TCP-In)	Remote Desktop	Domain, Private	Yes	Allow
Remote Desktop - User Mode (TCP-In)	Remote Desktop	Public	Yes	Allow
Remote Desktop - User Mode (TCP-In)	Remote Desktop	Domain, Private	Yes	Allow
Remote Desktop - User Mode (UDP-In)	Remote Desktop	Domain, Private	Yes	Allow
Remote Desktop - User Mode (UDP-In)	Remote Desktop	Public	Yes	Allow
Remote Event Log Management (NP-In)	Remote Event Log Manage...	All	No	Allow
Remote Event Log Management (RPC)	Remote Event Log Manage...	All	No	Allow
Remote Event Log Management (RPC-EPMAP)	Remote Event Log Manage...	All	No	Allow
Remote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow
Remote Event Monitor (RPC-EPMAP)	Remote Event Monitor	All	No	Allow

If the port configured in the inbound rule of the firewall is different from that configured on the remote server, the remote login will fail. If this occurs, add the port configured on the remote server in the inbound rule of the firewall.

For details, see **How Do I Disable a Windows ECS Firewall and Add 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.

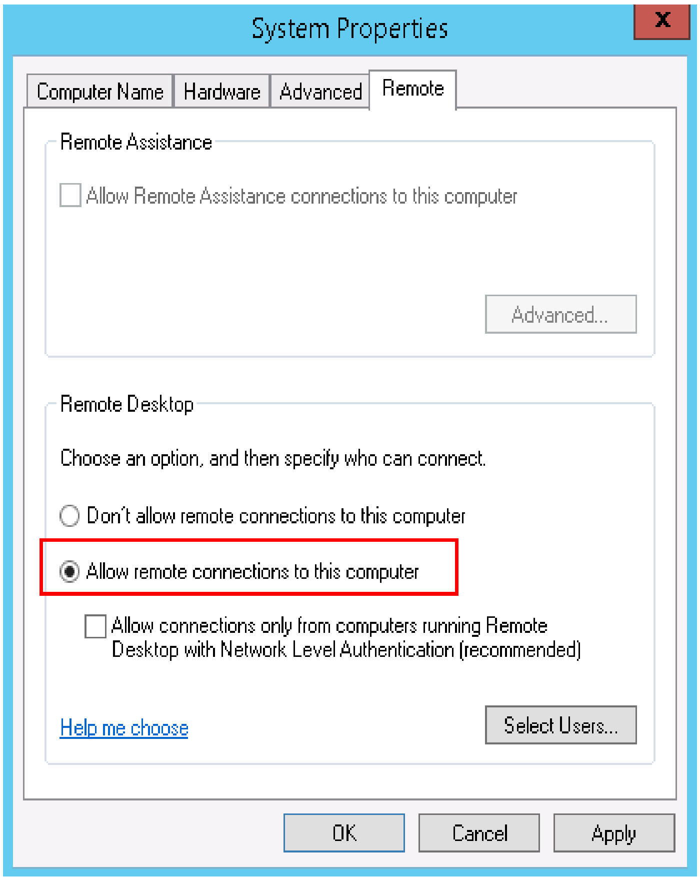
After you perform the preceding operations, try to remotely log in to the ECS again.

Checking Remote Desktop Connection Settings

Modify the remote desktop connection settings of the Windows ECS: Select **Allow remote connections to this computer**. The procedure is as follows:

1. Log in to the ECS.
2. Click **Start** in the lower left corner, right-click **Computer**, and choose **Properties** from the shortcut menu.
3. In the left navigation pane, choose **Remote settings**.
4. Click the **Remote** tab. In the **Remote Desktop** pane, select **Allow remote connections to this computer**.

Figure 5-48 Remote settings



Remote Assistance

☐ Allow Remote Assistance connections to this computer

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☐ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

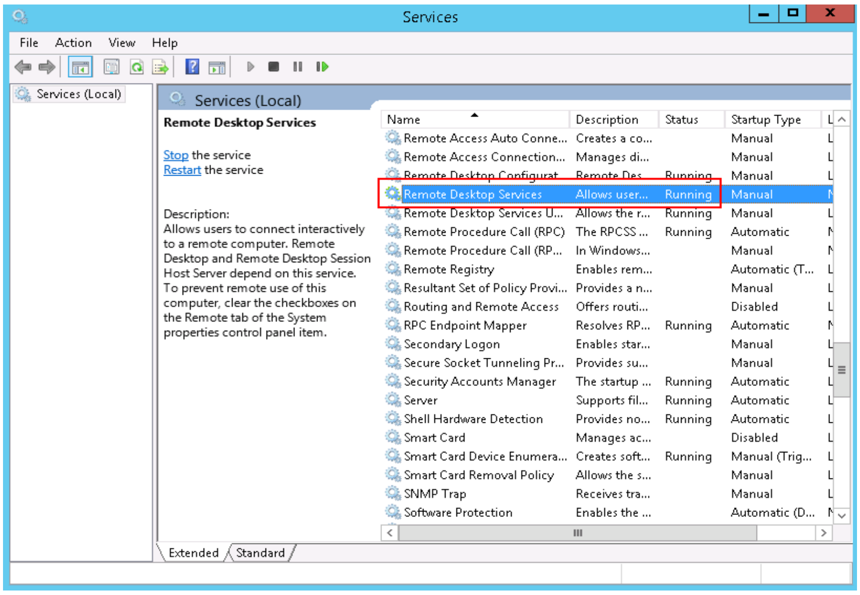
5. Click **OK**.

Checking Remote Desktop Services

1. Open the Windows search box, enter **services**, and select **Services**.

2. In the **Services** window, restart **Remote Desktop Services**. Ensure that **Remote Desktop Services** is in the **Running** status.

Figure 5-49 Remote Desktop Services



Remote Desktop Services

Stop the service
Restart the service

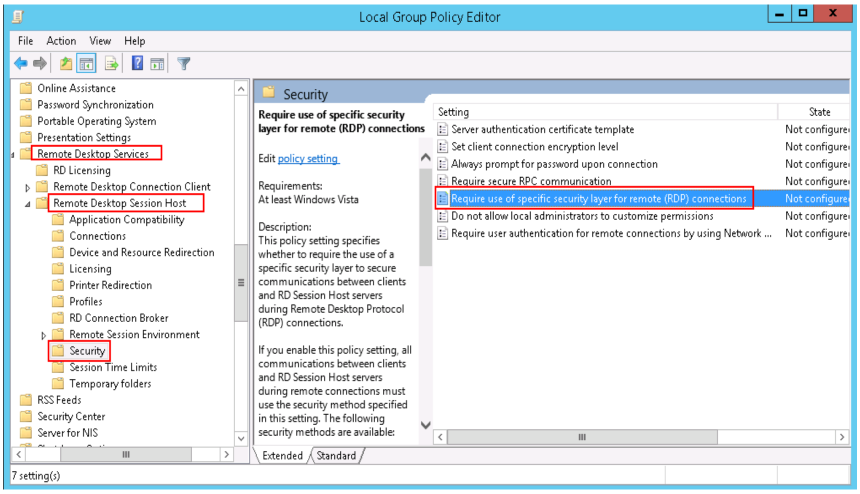
Description:
Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service. To prevent remote use of this computer, clear the checkboxes on the Remote tab of the System properties control panel item.

Name	Description	Status	Startup Type	L
Remote Access Auto Conne...	Creates a co...		Manual	L
Remote Access Connection...	Manages di...		Manual	L
Remote Desktop Configurat...	Remote Des...	Running	Manual	L
Remote Desktop Services	Allows user...	Running	Manual	N
Remote Desktop Services U...	Allows the r...	Running	Manual	L
Remote Procedure Call (RPC)	The RPCSS ...	Running	Automatic	N
Remote Procedure Call (RP...	In Windows...		Manual	N
Remote Registry	Enables rem...		Automatic (T...	L
Resultant Set of Policy Provi...	Provides a n...		Manual	L
Routing and Remote Access	Offers routi...		Disabled	L
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	N
Secondary Logon	Enables star...		Manual	L
Secure Socket Tunneling Pr...	Provides su...		Manual	L
Security Accounts Manager	The startup ...	Running	Automatic	L
Server	Supports fil...	Running	Automatic	L
Shell Hardware Detection	Provides no...	Running	Automatic	L
Smart Card	Manages ac...		Disabled	L
Smart Card Device Enumera...	Creates soft...	Running	Manual (Trig...	L
Smart Card Removal Policy	Allows the s...		Manual	L
SNMP Trap	Receives tra...		Manual	L
Software Protection	Enables the ...		Automatic (D...	N

Checking Remote Desktop Session Host Configuration

1. Open the **cmd** window and enter **gpedit.msc**.
2. Click **OK** to start Local Group Policy Editor.
3. Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services**.
4. Choose **Remote Desktop Session Host** > **Security** > **Require use of specific security layer for remote (RDP) connections**.

Figure 5-50 Require use of specific security layer for remote (RDP) connections



Require use of specific security layer for remote (RDP) connections

Edit policy setting

Requirements:
At least Windows Vista

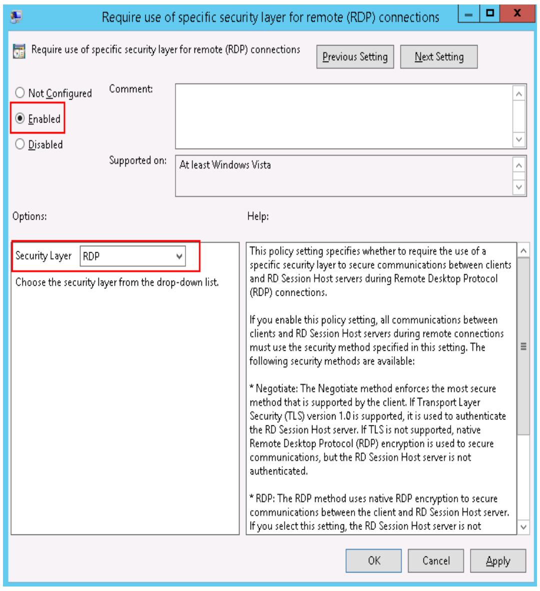
Description:
This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

If you enable this policy setting, all communications between clients and RD Session Host servers during remote connections must use the security method specified in this setting. The following security methods are available:

Setting	State
Server authentication certificate template	Not configure
Set client connection encryption level	Not configure
Always prompt for password upon connection	Not configure
Require secure RPC communication	Not configure
Require use of specific security layer for remote (RDP) connections	Not configure
Do not allow local administrators to customize permissions	Not configure
Require user authentication for remote connections by using Network ...	Not configure

5. Set **Require use of specific security layer for remote (RDP) connections** to **Enabled** and **Security layer** to **RDP**.

Figure 5-51 Setting security layer to RDP



Require use of specific security layer for remote (RDP) connections

Require use of specific security layer for remote (RDP) connections

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Security Layer: RDP

Choose the security layer from the drop-down list.

Help:

This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

If you enable this policy setting, all communications between clients and RD Session Host servers during remote connections must use the security method specified in this setting. The following security methods are available:

* Negotiate: The Negotiate method enforces the most secure method that is supported by the client. If Transport Layer Security (TLS) version 1.0 is supported, it is used to authenticate the RD Session Host server. If TLS is not supported, native Remote Desktop Protocol (RDP) encryption is used to secure communications, but the RD Session Host server is not authenticated.

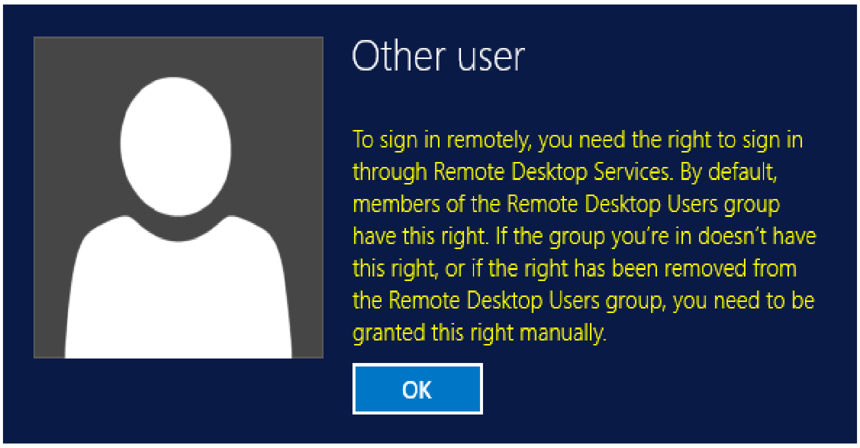
* RDP: The RDP method uses native RDP encryption to secure communications between the client and RD Session Host server. If you select this setting, the RD Session Host server is not

5.4.3 How Can I Obtain the Permission to Remotely Log In to a Windows ECS?

Symptom

When you connect a remote desktop to a Windows ECS, the system prompts that you need to be granted the right to sign in through Remote Desktop Services.

Figure 5-52 Remote login right missing.



Other user

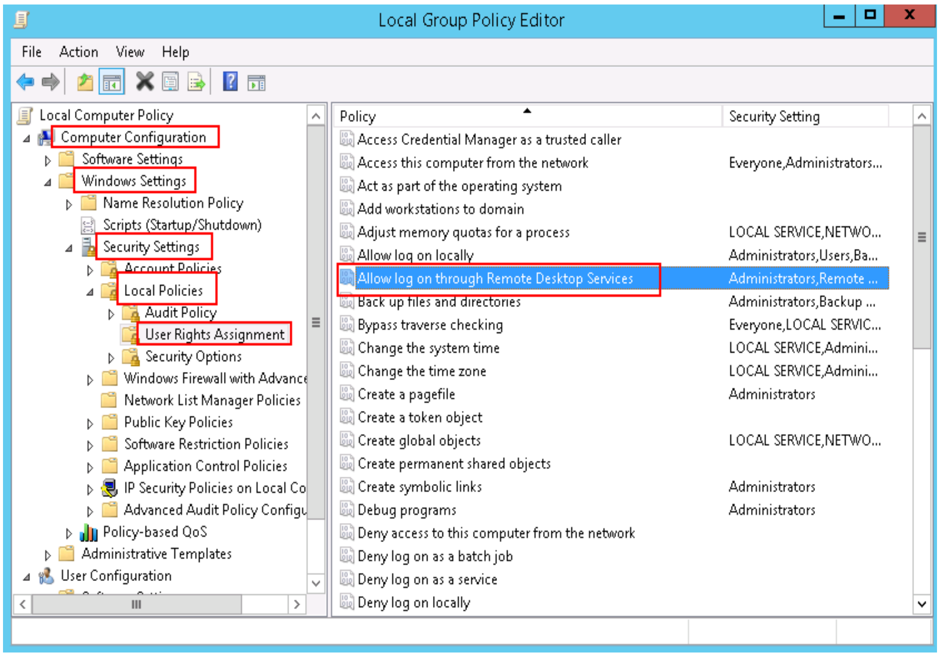
To sign in remotely, you need the right to sign in through Remote Desktop Services. By default, members of the Remote Desktop Users group have this right. If the group you're in doesn't have this right, or if the right has been removed from the Remote Desktop Users group, you need to be granted this right manually.

Solution

1. Open the **cmd** window and enter **gpedit.msc**.
2. Click **OK** to start Local Group Policy Editor.
3. Choose **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.

a. Locate and double-click **Allow log on through Remote Desktop Services**. Ensure that **Administrators** and **Remote Desktop Users** have been added.

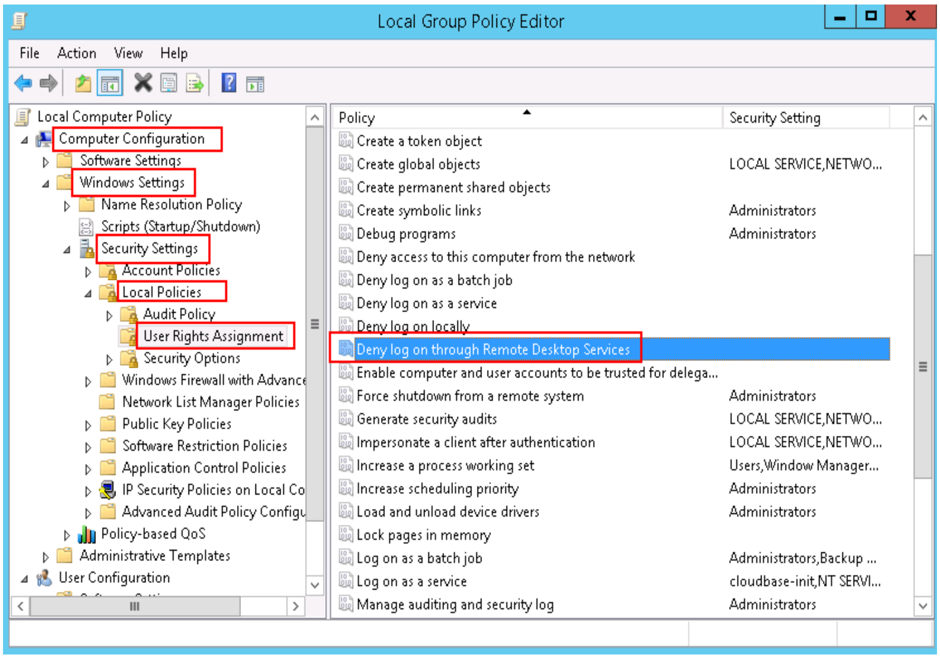
Figure 5-53 Allow log on through Remote Desktop Services properties



Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWO...
Allow log on locally	Administrators,Users,Ba...
Allow log on through Remote Desktop Services	Administrators,Remote ...
Back up files and directories	Administrators,Backup ...
Bypass traverse checking	Everyone,LOCAL SERVIC...
Change the system time	LOCAL SERVICE,Admini...
Change the time zone	LOCAL SERVICE,Admini...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWO...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	

b. Locate and double-click **Deny log on through Remote Desktop Services**. If the administrator account exists, delete it.

Figure 5-54 Deny log on through Remote Desktop Services properties



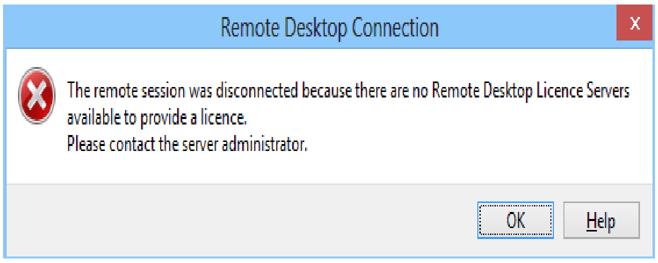
Policy	Security Setting
Create a token object	
Create global objects	LOCAL SERVICE,NETWO...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Deny log on through Remote Desktop Services	
Enable computer and user accounts to be trusted for delega...	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWO...
Impersonate a client after authentication	LOCAL SERVICE,NETWO...
Increase a process working set	Users,Window Manager...
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Administrators,Backup ...
Log on as a service	cloudbase-init,NT SERVI...
Manage auditing and security log	Administrators

5.4.4 Why Does the System Display No Remote Desktop License Servers Available to Provide a License When I Log In to a Windows ECS?

Symptom

An error message is displayed indicating that there are no Remote Desktop License Servers available to provide a license and asks you to contact the administrator.

Figure 5-55 No Remote Desktop License Servers available to provide a license



The remote session was disconnected because there are no Remote Desktop Licence Servers available to provide a licence.
Please contact the server administrator.

Possible Causes

You have installed the Remote Desktop Session Host.

The grace period for Remote Desktop Services is 120 days. If you do not pay for it when the period expires, the service will stop. Windows allows a maximum of two users (including the local user) in remote desktop connections. To allow the access of more users, install the Remote Desktop Session Host and configure the desired number of authorized users. However, installing the Remote Desktop Session Host will automatically revoke the original two free connections. This leads to the preceding fault if desired number of authorized users has not been configured.

Solution

- Method 1: Apply for a license for authenticating multi-user sessions and activate the ECS. Note that you need to purchase a remote desktop access license from the official Microsoft website.

  For details, see **How Do I Apply for a License for Authenticating Multi-User Sessions and Activate an ECS?**
- Method 2: Delete Remote Desktop Session Host (Windows Server 2008) or Remote Desktop Services (Windows Server 2012).

  After you delete the role, the ECS allows a maximum of two users (including local login users) to access.
- Method 3: Reconfigure multi-user login after reinstalling or changing the ECS OS.

  Windows Server 2008 public images are no longer supported. If you are using a Windows Server 2008 ECS, change its OS to a Windows Server 2012 OS.

  Back up data on the system disk before reinstalling or changing the OS.

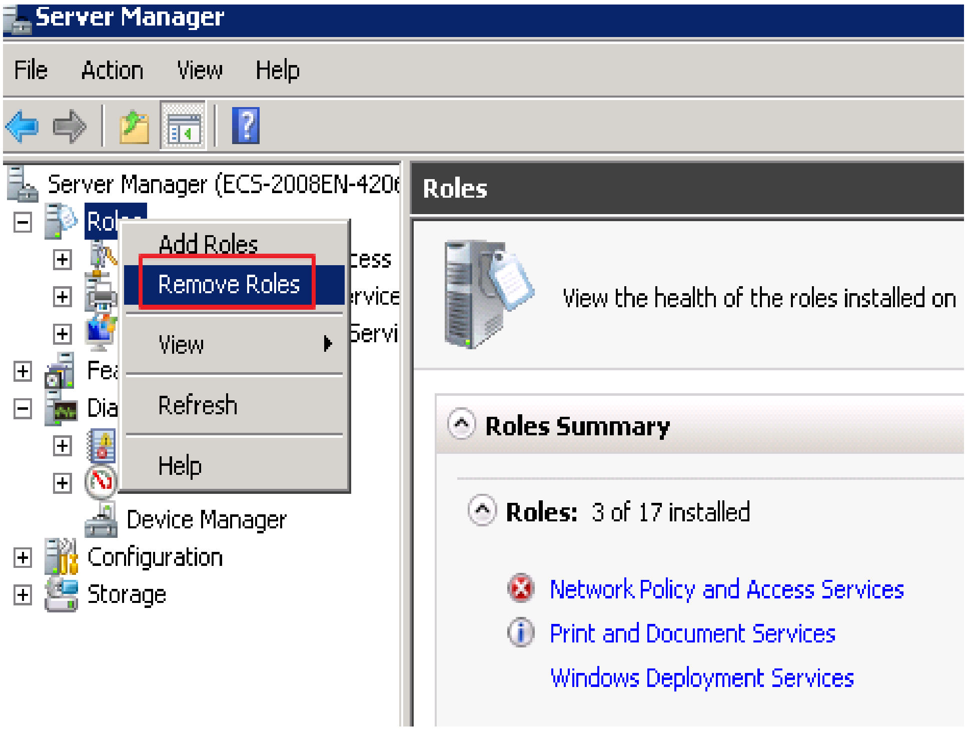
Precautions

- The operations described in this section apply to the ECSs running a Windows Server 2008 or Windows Server 2012.
- The ECS must be restarted during the operation, which may interrupt services. Back up data before restarting the ECS.

Windows Server 2008

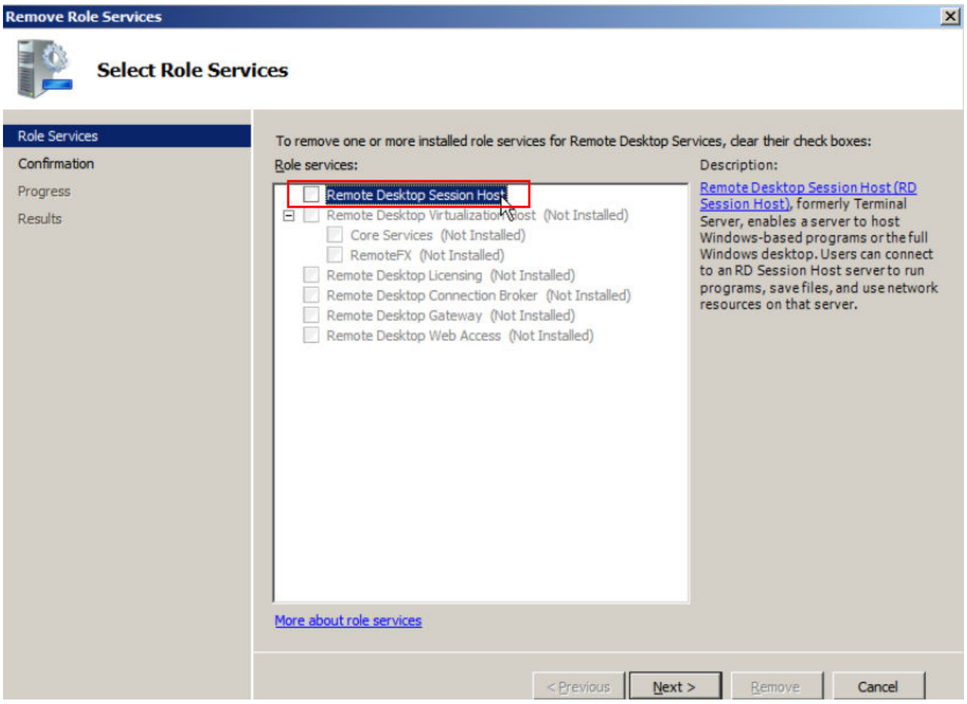
1. Log in to the Windows ECS using VNC available on the management console.
2. Open **Server Manager**, right-click **Remote Desktop Services** under **Roles**, and choose **Remove Roles** from the shortcut menu.

Figure 5-56 Deleting roles



3. In the displayed dialog box, deselect **Remote Desktop Session Host** and keep clicking **Next** till you finish the operation.

Figure 5-57 Deselecting Remote Desktop Session Host



To remove one or more installed role services for Remote Desktop Services, clear their check boxes:

☐ Remote Desktop Session Host
☐ Remote Desktop Virtualization Host (Not Installed)
  ☐ Core Services (Not Installed)
  ☐ RemoteFX (Not Installed)
☐ Remote Desktop Licensing (Not Installed)
☐ Remote Desktop Connection Broker (Not Installed)
☐ Remote Desktop Gateway (Not Installed)
☐ Remote Desktop Web Access (Not Installed)

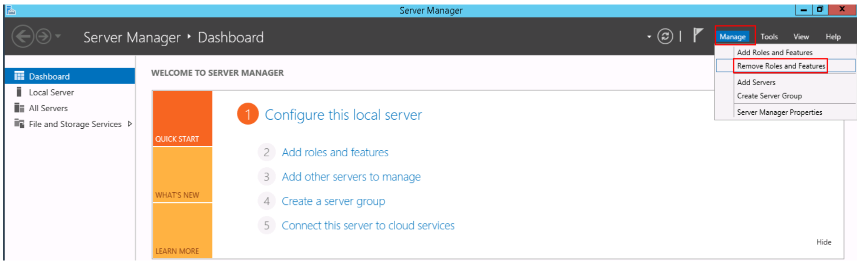
Remote Desktop Session Host (RD Session Host), formerly Terminal Server, enables a server to host Windows-based programs or the full Windows desktop. Users can connect to an RD Session Host server to run programs, save files, and use network resources on that server.

4. Click **Delete**.
5. Restart the ECS.

Windows Server 2012

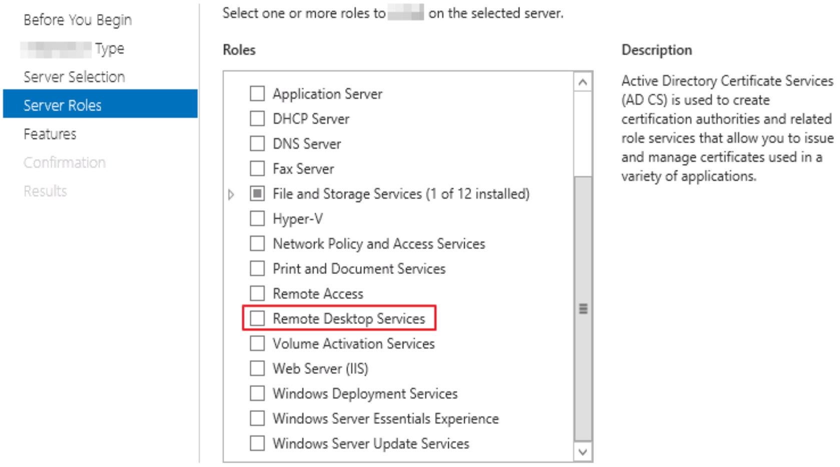
1. Log in to the Windows ECS using VNC available on the management console.
2. Open **Server Manager**, choose **Manage** > **Remove Roles and Features**, and click **Next**.

Figure 5-58 Deleting roles and features


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide

3. Select the destination server and click **Next**.
4. Deselect **Remote Desktop Services**.

Figure 5-59 Deselecting Remote Desktop Services



Select one or more roles to [redacted] on the selected server.

Roles

☐ Application Server
☐ DHCP Server
☐ DNS Server
☐ Fax Server
▣ File and Storage Services (1 of 12 installed)
☐ Hyper-V
☐ Network Policy and Access Services
☐ Print and Document Services
☐ Remote Access
☐ Remote Desktop Services
☐ Volume Activation Services
☐ Web Server (IIS)
☐ Windows Deployment Services
☐ Windows Server Essentials Experience
☐ Windows Server Update Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

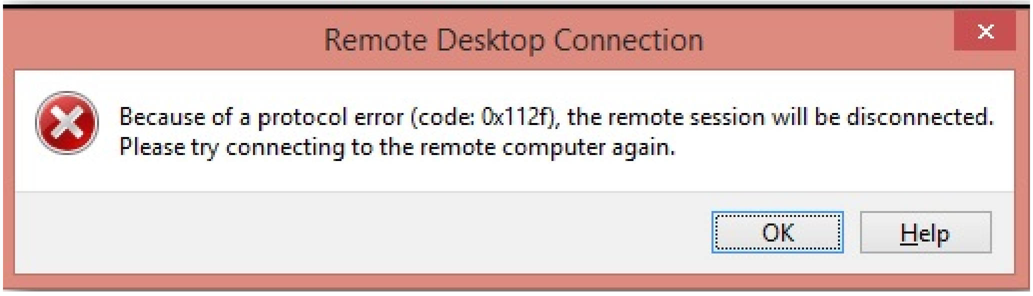
5. Click **Delete**.
6. Restart the ECS.

5.4.5 Why Does the System Display Error Code 0x112f When I Log In to a Windows ECS?

Symptom

When you log in to a Windows ECS, the system displays error code 0x112f, as shown in **Figure 5-60**.

Figure 5-60 Error message (code: 0x112f)



Because of a protocol error (code: 0x112f), the remote session will be disconnected. Please try connecting to the remote computer again.

Possible Causes

The ECS memory is insufficient.

Solution

- Method 1 (recommended)

  Modify the ECS specifications to increase the vCPUs and memory size. For details about how to modify specifications, see **Modifying Individual ECS Specifications**.
- Method 2:

  Enable virtual memory on the ECS to obtain its idle memory.

For details about how to enable virtual memory, see **How Can I Enable Virtual Memory on a Windows ECS?**

NOTE

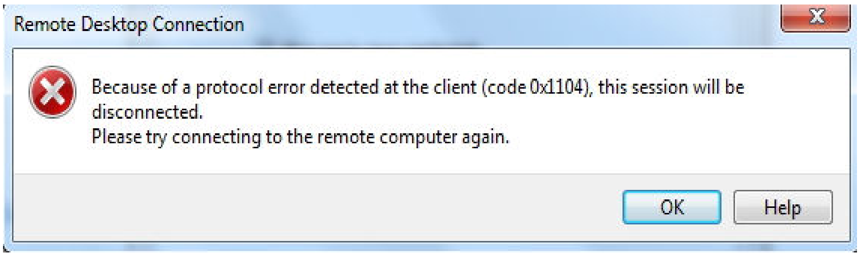
This method will deteriorate the disk I/O performance, so use this method only when necessary.

5.4.6 Why Does the System Display Error Code 0x1104 When I Log In to a Windows ECS?

Symptom

The system displays an error message indicating that a protocol error (code: 0x1104) is detected when you use MSTSC to access an ECS running Windows Server 2008.

Figure 5-61 Protocol error (code: 0x1104)



Because of a protocol error detected at the client (code 0x1104), this session will be disconnected.
Please try connecting to the remote computer again.

Possible Causes

- Port 3389 of the security group on the ECS is disabled.
- The firewall on the ECS is disabled.
- Port 3389 on the ECS is used by other processes.
- The Remote Desktop Session Host is incorrectly configured.

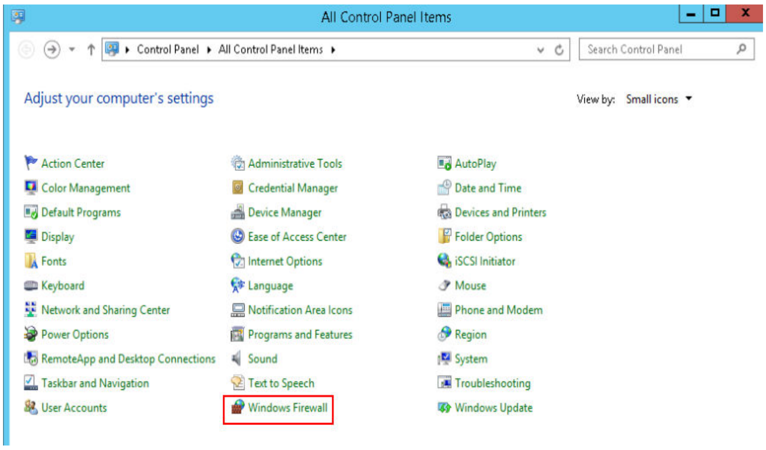
Solution

Step 1 Check security group settings.

Check whether port 3389 is allowed in inbound direction. If it is allowed, go to **Step 2**.

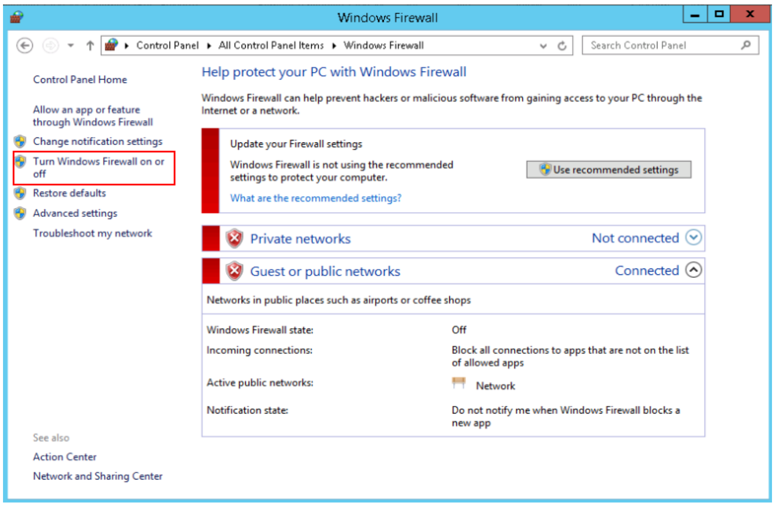
Step 2 Check whether the firewall is disabled:

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



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

   View and set the firewall status.


Windows Firewall
Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Use recommended settings
What are the recommended settings?

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

Private networks Not connected

Guest or public networks Connected

Networks in public places such as airports or coffee shops

Windows Firewall state: Off

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active public networks: Network

Notification state: Do not notify me when Windows Firewall blocks a new app

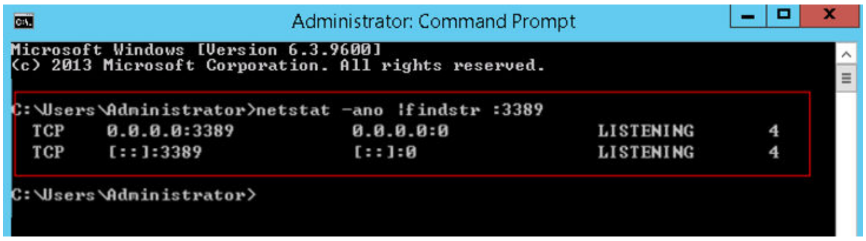
If the firewall is enabled, go to **Step 3**.

Step 3 Log in to the ECS using VNC and check the port.

1. Open the **cmd** window and run the following command:

   netstat -ano |findstr: 3389

Figure 5-62 Checking port 3389



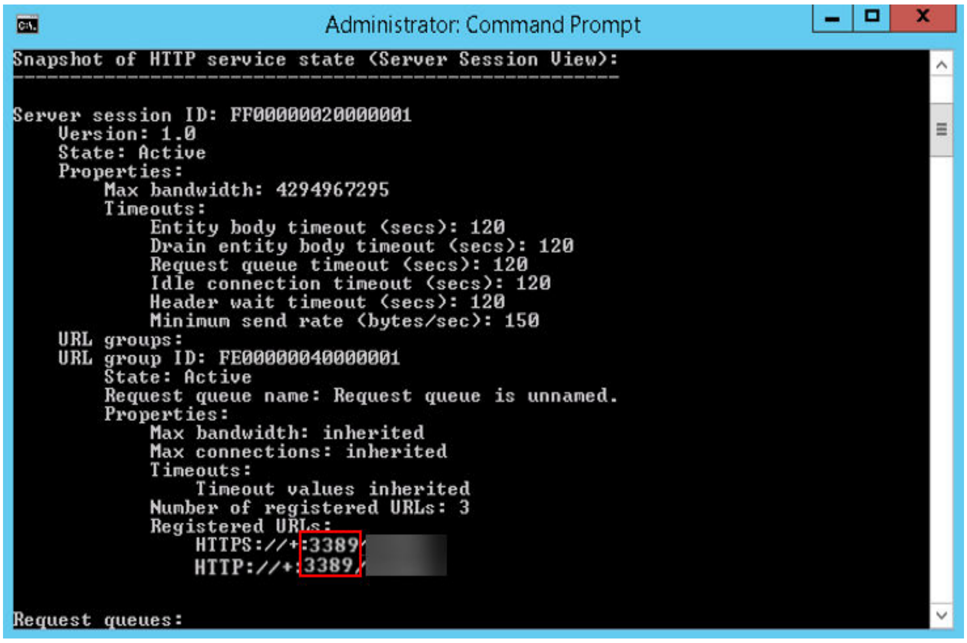
```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netstat -ano |findstr :3389
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       4

C:\Users\Administrator>
```

   As shown in **Figure 5-62**, port 3389 is used by the process with ID of 4.

2. Open Task Manager and find the process with ID of 4 is the System process.
3. Generally, the IIS and SQL Server run as the System process. Run the following HTTP command for further check.

netsh http show servicestate

Figure 5-63 Checking System process



```
Snapshot of HTTP service state (Server Session View):
-----------------------------------------------------

Server session ID: FF00000020000001
    Version: 1.0
    State: Active
    Properties:
        Max bandwidth: 4294967295
        Timeouts:
            Entity body timeout (secs): 120
            Drain entity body timeout (secs): 120
            Request queue timeout (secs): 120
            Idle connection timeout (secs): 120
            Header wait timeout (secs): 120
            Minimum send rate (bytes/sec): 150
    URL groups:
    URL group ID: FE00000040000001
        State: Active
        Request queue name: Request queue is unnamed.
        Properties:
            Max bandwidth: inherited
            Max connections: inherited
            Timeouts:
                Timeout values inherited
            Number of registered URLs: 3
            Registered URLs:
                HTTPS://+:3389/[redacted]
                HTTP://+:3389/

Request queues:
```

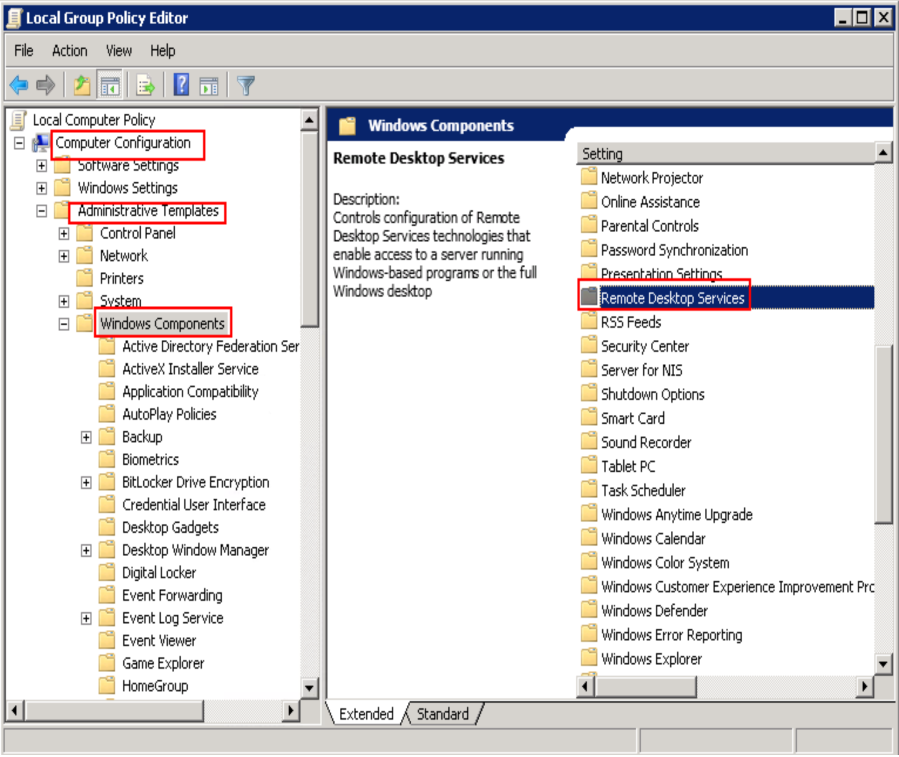
4. If port 3389 is used by HTTP protocols, it indicates that the port is used by IIS.
5. Enter **http://127.0.0.1:3389** in the address box of the browser and press **Enter**. Check whether the website can be visited normally.
6. Change the port used by IIS and restart IIS.

Step 4 If no error occurs during the preceding steps, go to step **Step 5** to check whether error 0x1104 is caused by the configuration of Remote Desktop Session Host.

Step 5 Check the remote desktop session host configuration.

1. Log in to the ECS using VNC.
2. Open the **cmd** window and enter **gpedit.msc**.
3. Click **OK** to start Local Group Policy Editor.
4. Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services**.

Figure 5-64 Remote Desktop Services

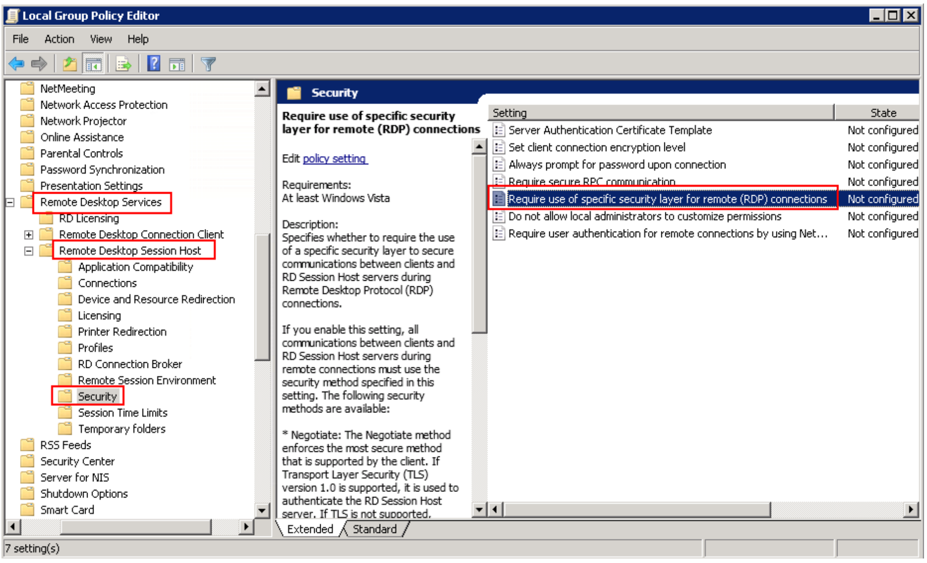


Remote Desktop Services

Description:
Controls configuration of Remote Desktop Services technologies that enable access to a server running Windows-based programs or the full Windows desktop

5. **Remote Desktop Session Host** > **Security**.

Figure 5-65 Remote (RDP) Connection requires the use of the specified security layer



Require use of specific security layer for remote (RDP) connections

Edit policy setting

Requirements:
At least Windows Vista

Description:
Specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

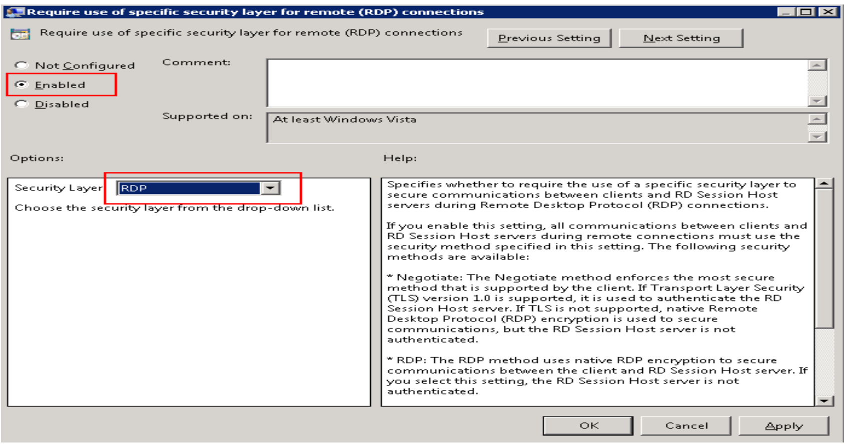
If you enable this setting, all communications between clients and RD Session Host servers during remote connections must use the security method specified in this setting. The following security methods are available:

* Negotiate: The Negotiate method enforces the most secure method that is supported by the client. If Transport Layer Security (TLS) version 1.0 is supported, it is used to authenticate the RD Session Host server. If TLS is not supported,

Setting	State
Server Authentication Certificate Template	Not configured
Set client connection encryption level	Not configured
Always prompt for password upon connection	Not configured
Require secure RPC communication	Not configured
Require use of specific security layer for remote (RDP) connections	Not configured
Do not allow local administrators to customize permissions	Not configured
Require user authentication for remote connections by using Net…	Not configured

6. Set **Require use of specific security layer for remote (RDP) connections** to **Enabled** and **Security layer** to **RDP**.

Figure 5-66 Setting security layer


Require use of specific security layer for remote (RDP) connections
Require use of specific security layer for remote (RDP) connections
Previous Setting
Next Setting
Comment:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Vista

Security Layer: RDP

Choose the security layer from the drop-down list.

Specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

If you enable this setting, all communications between clients and RD Session Host servers during remote connections must use the security method specified in this setting. The following security methods are available:

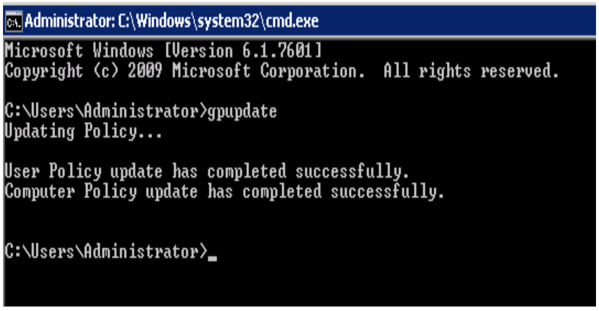
* Negotiate: The Negotiate method enforces the most secure method that is supported by the client. If Transport Layer Security (TLS) version 1.0 is supported, it is used to authenticate the RD Session Host server. If TLS is not supported, native Remote Desktop Protocol (RDP) encryption is used to secure communications, but the RD Session Host server is not authenticated.

* RDP: The RDP method uses native RDP encryption to secure communications between the client and RD Session Host server. If you select this setting, the RD Session Host server is not authenticated.

7. Click **OK**.
8. After the configuration is complete, open the **cmd** window.
9. Run the following command to update the group policy:

   gpupdate

Figure 5-67 Updating the group policy



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>gpupdate
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.


C:\Users\Administrator>_
```

----End

5.4.7 Why Does the System Display Error Code 122.112... When I Log In to a Windows ECS?

Symptom

The system displays error 122.112... when you use RDC to locally access an ECS running Windows Server 2012. The ECS is frequently disconnected and the Windows login process is unexpectedly interrupted.

Possible Causes

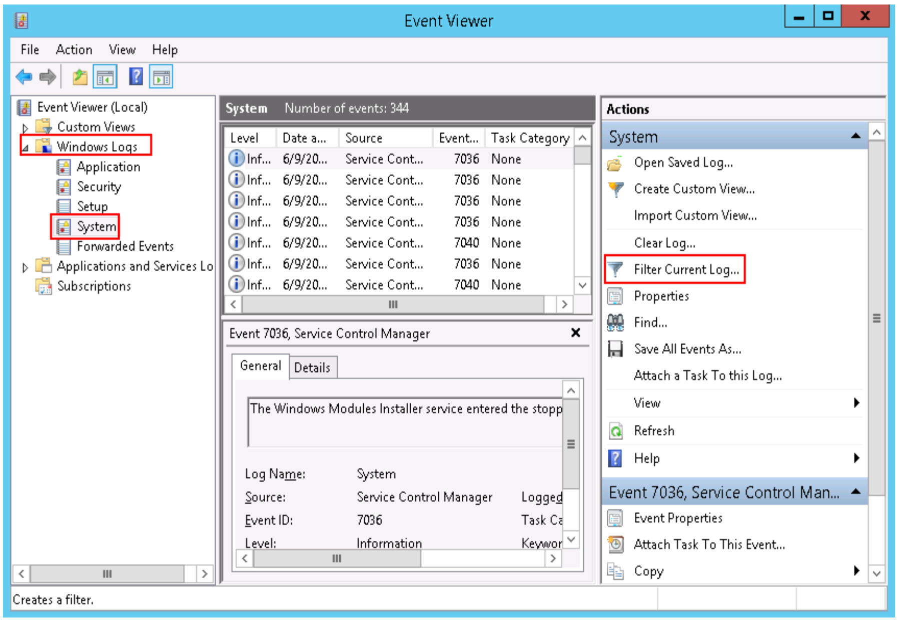
1. System resources are insufficient or unavailable.
2. The services cannot be started.

Solution

Step 1 Check system logs.

1. Log in to the ECS using VNC.
2. Click to start the service manager and choose **Administrative Tools** > **Event Viewer** > **Windows Logs** > **System** > **Filter Current Logs**.

Figure 5-68 Event viewer



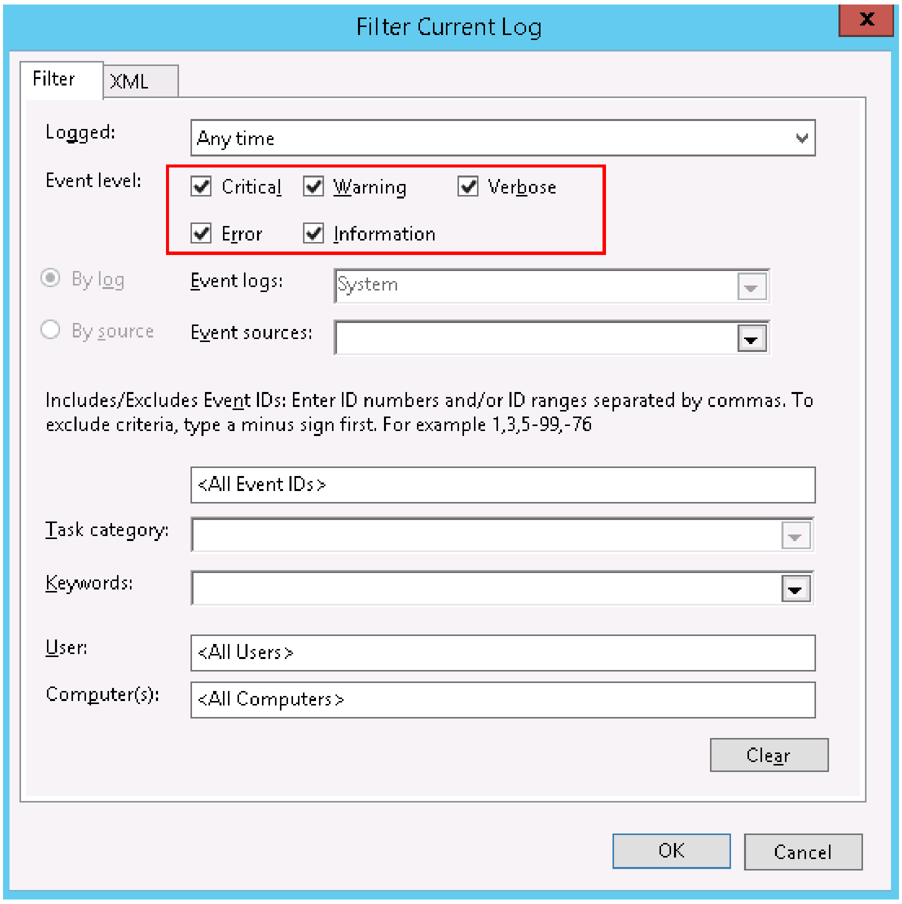
Level	Date a...	Source	Event...	Task Category
Inf...	6/9/20...	Service Cont...	7036	None
Inf...	6/9/20...	Service Cont...	7036	None
Inf...	6/9/20...	Service Cont...	7036	None
Inf...	6/9/20...	Service Cont...	7036	None
Inf...	6/9/20...	Service Cont...	7040	None
Inf...	6/9/20...	Service Cont...	7036	None
Inf...	6/9/20...	Service Cont...	7040	None

The Windows Modules Installer service entered the stopp

Log Name: System
Source: Service Control Manager Logged
Event ID: 7036 Task Ca
Level: Information Keywor

3. In the **Event Level** pane, select event levels.

Figure 5-69 Filtering logs



Logged: Any time

Event level: ☑ Critical ☑ Warning ☑ Verbose ☑ Error ☑ Information

● By log Event logs: System

○ By source

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

User: <All Users>

Computer(s): <All Computers>

4. Search for login logs.

Step 2 Check the usage of host resources.

1. Choose **Start** > **Task Manager** > **Performance**.
2. Check usage of CPU and memory.

Step 3 Check whether the purchased Windows ECS is with 1 vCPU and 1 GB of memory.

If it is, change the flavor or stop unnecessary processes.

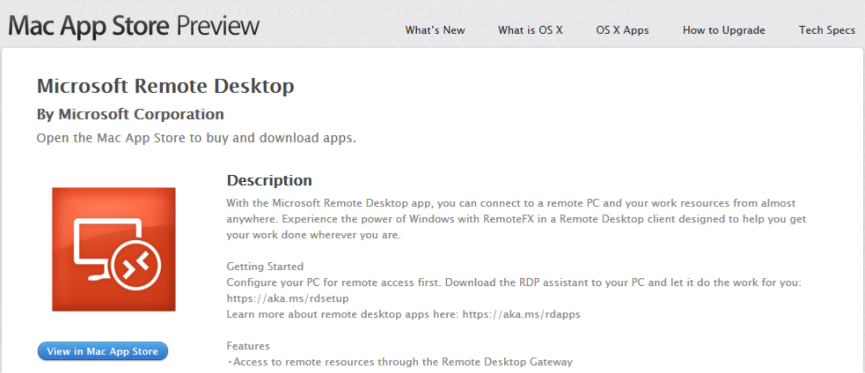
----End

5.4.8 Why Does the System Display Invalid Certificate or Associated Chain When I Log In to a Windows ECS from a Mac?

Symptom

When you use Microsoft Remote Desktop for Mac to remotely access a Windows ECS, the system displays invalid certificate or associated chain.

Figure 5-70 Microsoft Remote Desktop for Mac



Microsoft Remote Desktop

By Microsoft Corporation

Open the Mac App Store to buy and download apps.

Description

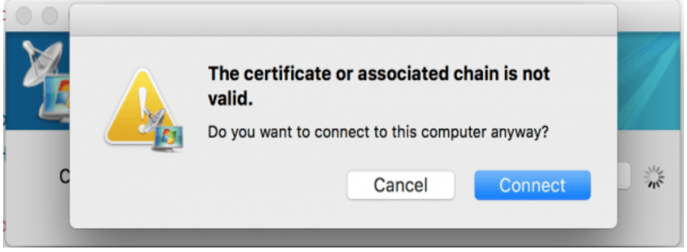
With the Microsoft Remote Desktop app, you can connect to a remote PC and your work resources from almost anywhere. Experience the power of Windows with RemoteFX in a Remote Desktop client designed to help you get your work done wherever you are.

Getting Started
Configure your PC for remote access first. Download the RDP assistant to your PC and let it do the work for you: https://aka.ms/rdsetup
Learn more about remote desktop apps here: https://aka.ms/rdapps

Features
·Access to remote resources through the Remote Desktop Gateway

Due to the particularity of the Mac system, you need to perform internal configurations on Mac and the Windows ECS to ensure successful remote connection. When you log in to the Windows ECS using Microsoft Remote Desktop for Mac, the system displays an error message indicating that the certificate or associated chain is invalid.

Figure 5-71 Invalid certificate or associated chain



The certificate or associated chain is not valid.

Do you want to connect to this computer anyway?

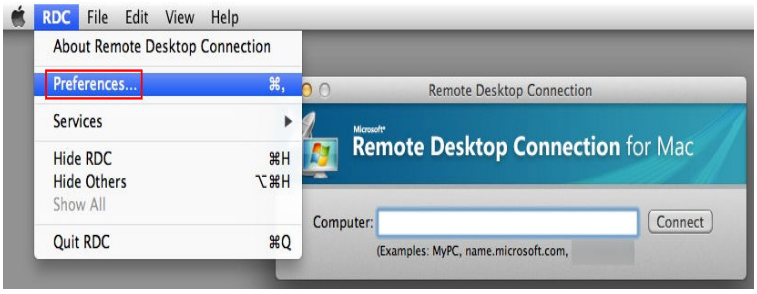
Possible Causes

The group policy setting is incorrect on the ECS.

Procedure

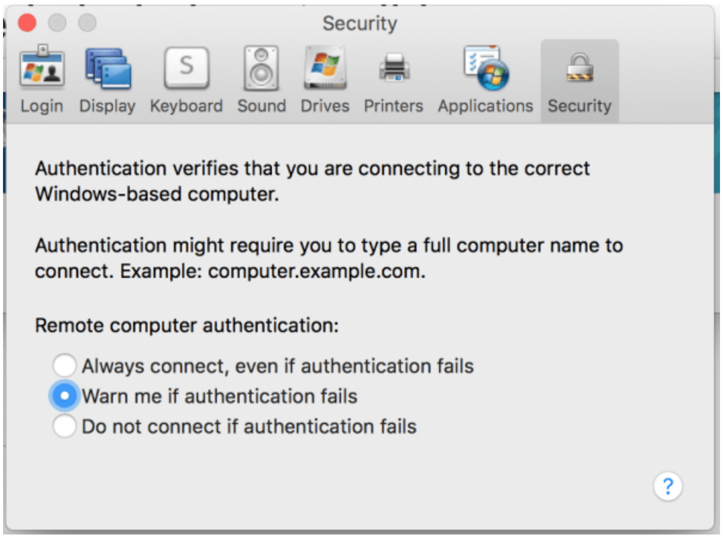
1. On the menu bar in the upper left corner, choose **RDC** > **Preferences** to open the preference setting page of the Microsoft Remote Desktop.

   Figure 5-72 Preferences setting

   
   RDC
File
Edit
View
Help
About Remote Desktop Connection
Preferences... ⌘,
Services
Hide RDC ⌘H
Hide Others ⌥⌘H
Show All
Quit RDC ⌘Q
Remote Desktop Connection
Microsoft
Remote Desktop Connection for Mac
Computer:
Connect
(Examples: MyPC, name.microsoft.com,

2. Select **Security** and modify the parameter settings according the following figure.

Figure 5-73 Security setting



Authentication verifies that you are connecting to the correct Windows-based computer.

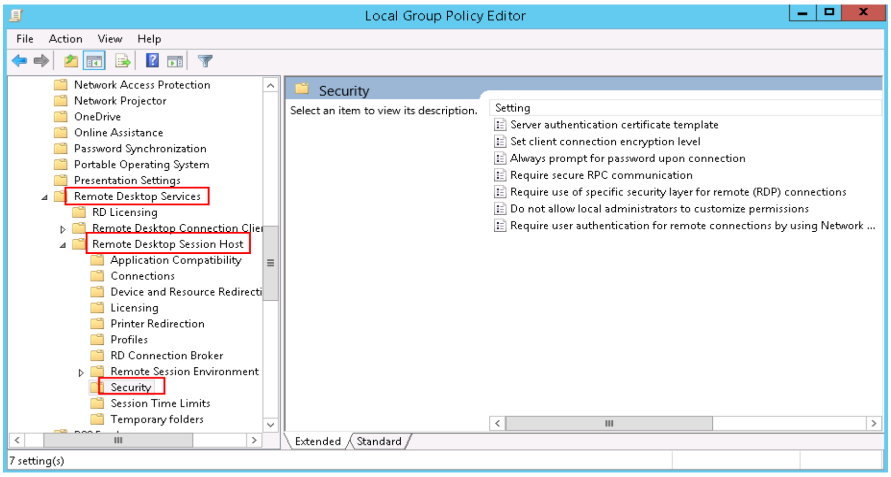
Authentication might require you to type a full computer name to connect. Example: computer.example.com.

Remote computer authentication:

○ Always connect, even if authentication fails
● Warn me if authentication fails
○ Do not connect if authentication fails

3. Remotely connect to the Windows ECS again. If the error message **Invalid certificate or associated chain** is still displayed, go to **4**.
4. Log in to the Windows ECS using VNC.
5. Press **Win+R** to start the **Open** text box.
6. Enter **gpedit.msc** to access the Local Group Policy Editor.
7. In the left navigation pane, choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Security**.

Figure 5-74 Remote Desktop Session Host



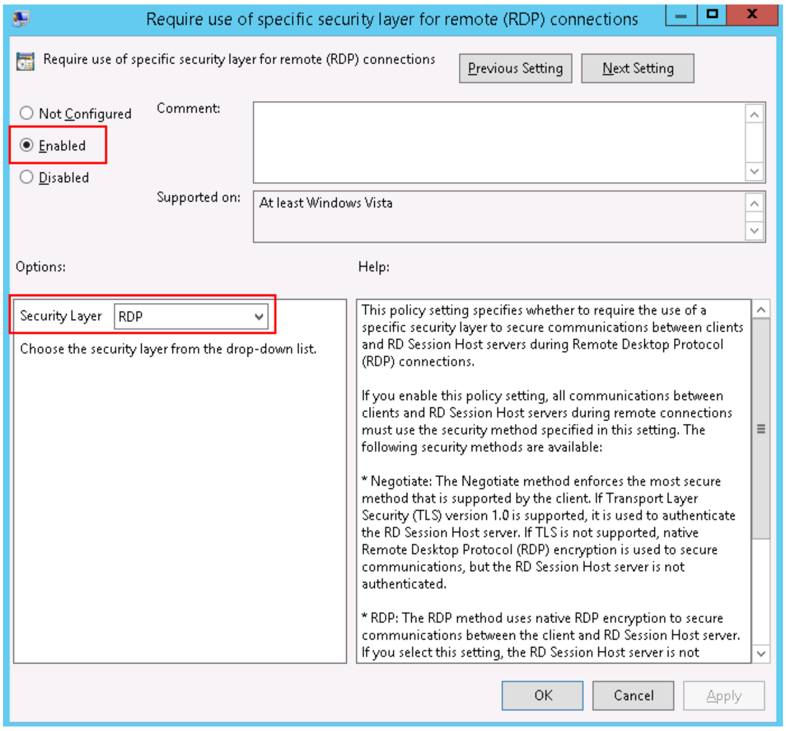
Select an item to view its description.

Setting
Server authentication certificate template
Set client connection encryption level
Always prompt for password upon connection
Require secure RPC communication
Require use of specific security layer for remote (RDP) connections
Do not allow local administrators to customize permissions
Require user authentication for remote connections by using Network ...

7 setting(s)

8. Modify the following parameters as prompted:
   - Enable **Require use of specific security layer for remote (RDP) connections**.

Figure 5-75 Require use of specific security layer for remote (RDP) connections



Require use of specific security layer for remote (RDP) connections

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Vista

Security Layer: RDP

Choose the security layer from the drop-down list.

This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

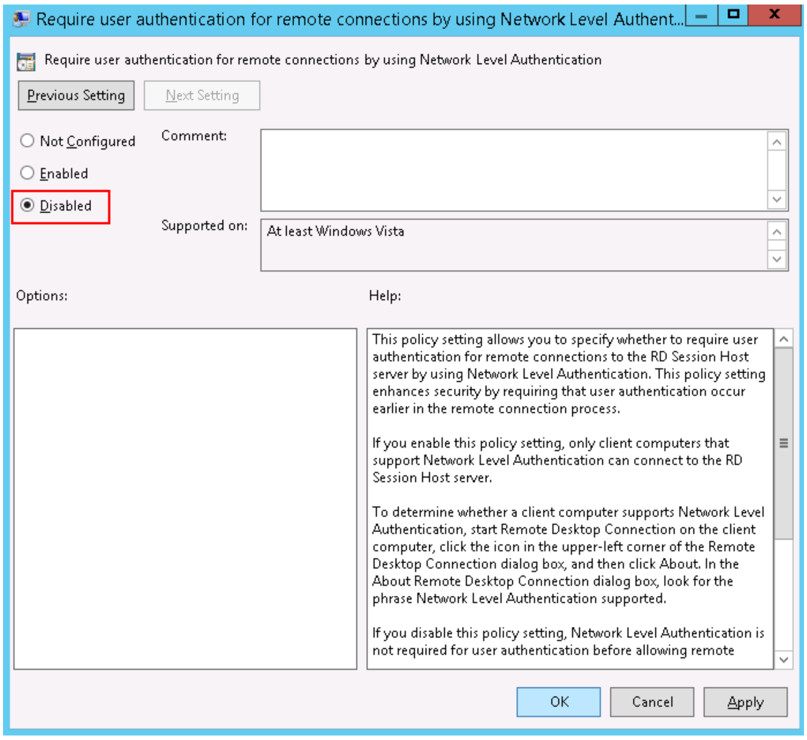
If you enable this policy setting, all communications between clients and RD Session Host servers during remote connections must use the security method specified in this setting. The following security methods are available:

* Negotiate: The Negotiate method enforces the most secure method that is supported by the client. If Transport Layer Security (TLS) version 1.0 is supported, it is used to authenticate the RD Session Host server. If TLS is not supported, native Remote Desktop Protocol (RDP) encryption is used to secure communications, but the RD Session Host server is not authenticated.

* RDP: The RDP method uses native RDP encryption to secure communications between the client and RD Session Host server. If you select this setting, the RD Session Host server is not

– Disable **Require user authentication for remote connections by using Network Level Authentication**.

Figure 5-76 Remote connection authentication



Require user authentication for remote connections by using Network Level Authent...
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

Require user authentication for remote connections by using Network Level Authentication

○ Not Configured
○ Enabled
● Disabled

Supported on: At least Windows Vista

This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process.

If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server.

To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported.

If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote

9. Close the group policy editor and restart the ECS.

5.4.9 Why Does the System Display a Message Indicating Invalid Credentials When I Attempt to Access a Windows ECS?

Symptom

When you use a local PC running Windows to access a Windows ECS using RDP (for example, MSTSC), the system displays a message indicating that the credentials are invalid.

Solution

Perform the following steps to rectify the fault. After completing each step, try to access the ECS to check whether the fault is rectified. If the fault persists, go to the next step.

Step 1: Change Network Access Policy

Step 2: Modify Credentials Delegation

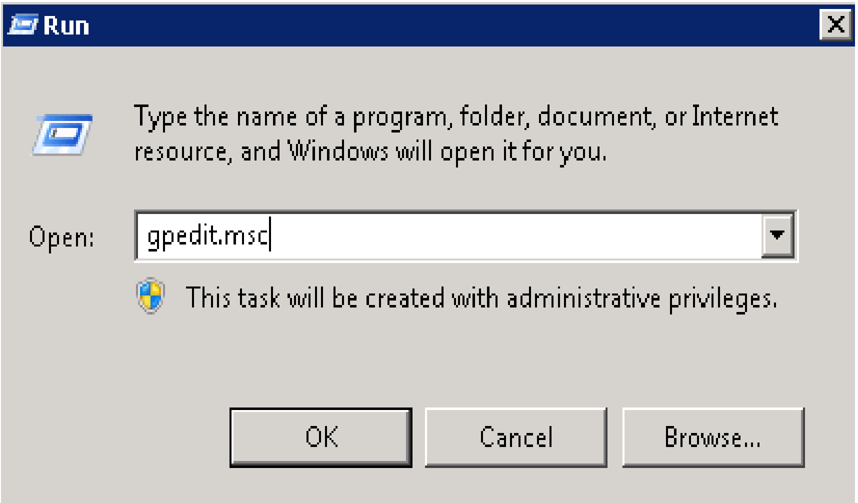
Step 3: Set the Credentials of the Local Server

Step 4: Disable Password Protected Sharing

Step 1: Change Network Access Policy

1. Log in to the ECS using VNC on the management console.
2. Choose **Start** > **Run**. In the **Run** dialog box, enter **gpedit.msc** and click **OK** to start **Local Group Policy Editor**.

Figure 5-77 gpedit.msc

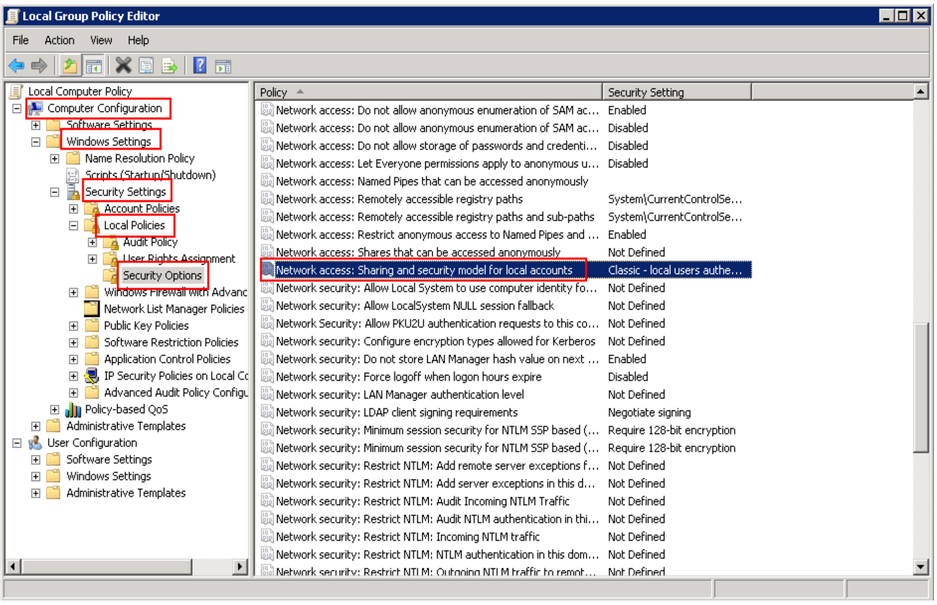


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
This task will be created with administrative privileges.
OK
Cancel
Browse...

gpedit.msc

3. Choose **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options** and click **Network access: Sharing and security model for local accounts**.

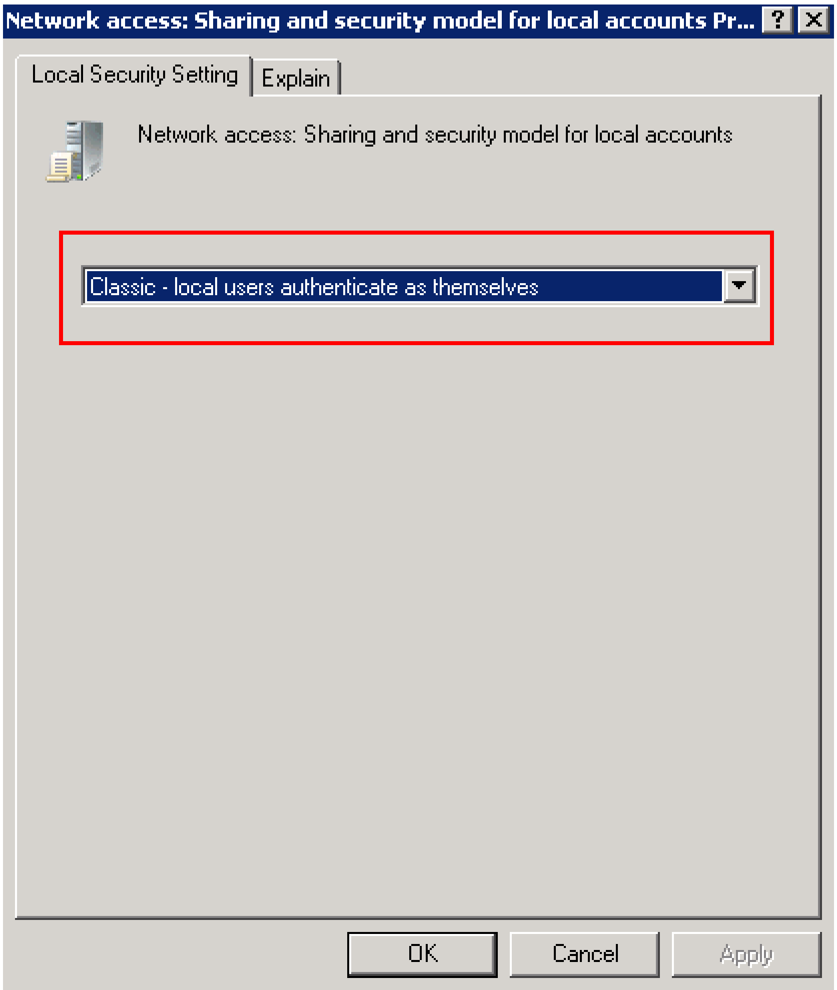
Figure 5-78 Locating the network access policy



Policy	Security Setting
Network access: Do not allow anonymous enumeration of SAM ac…	Enabled
Network access: Do not allow anonymous enumeration of SAM ac…	Disabled
Network access: Do not allow storage of passwords and credenti…	Disabled
Network access: Let Everyone permissions apply to anonymous u…	Disabled
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System\CurrentControlSe…
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSe…
Network access: Restrict anonymous access to Named Pipes and …	Enabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users authe…
Network security: Allow Local System to use computer identity fo…	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network Security: Allow PKU2U authentication requests to this co…	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next …	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (…	Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (…	Require 128-bit encryption
Network security: Restrict NTLM: Add remote server exceptions f…	Not Defined
Network security: Restrict NTLM: Add server exceptions in this d…	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in thi…	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this dom…	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remot…	Not Defined

4. Select **Classic - local users authenticate as themselves** and click **OK**.

Figure 5-79 Changing the network access policy


Network access: Sharing and security model for local accounts Pr...
?
Local Security Setting
Explain
OK
Cancel
Apply

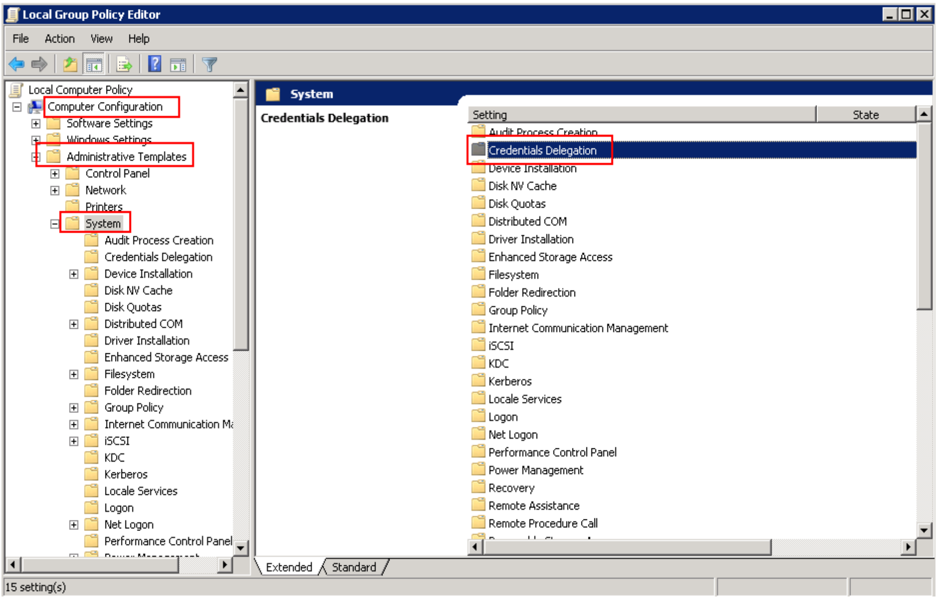
Network access: Sharing and security model for local accounts

Classic - local users authenticate as themselves

Step 2: Modify Credentials Delegation

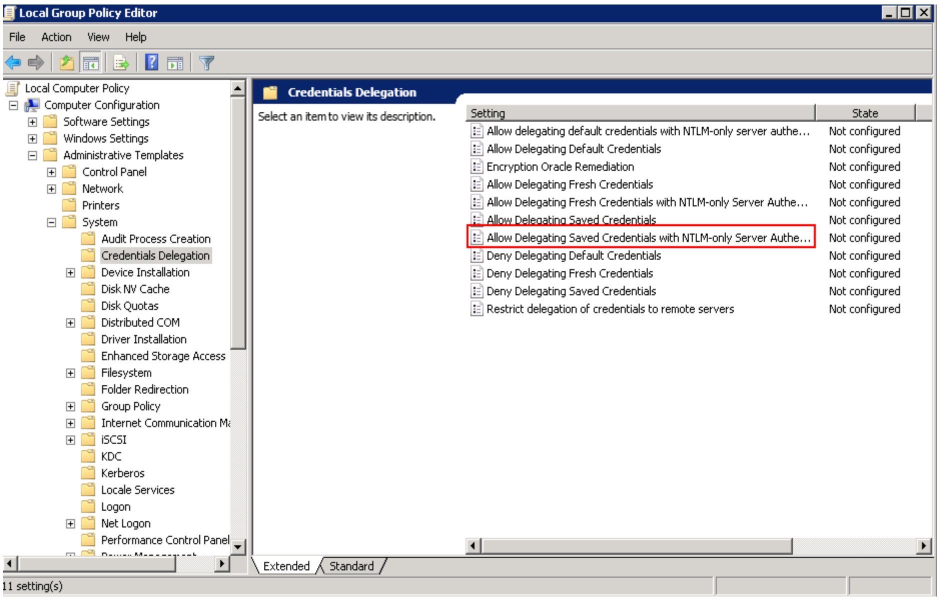
1. Log in to the ECS using VNC on the management console.
2. Choose **Start** > **Run**. In the **Run** dialog box, enter **gpedit.msc** and click **OK** to start **Local Group Policy Editor**.
3. Choose **Computer Configuration** > **Administrative Templates** > **System** and locate **Credentials Delegation**.

Figure 5-80 Locating the network access policy



4. Double-click **Allow Delegating Saved Credentials with NTLM-only Server Authentication** and click **OK**.

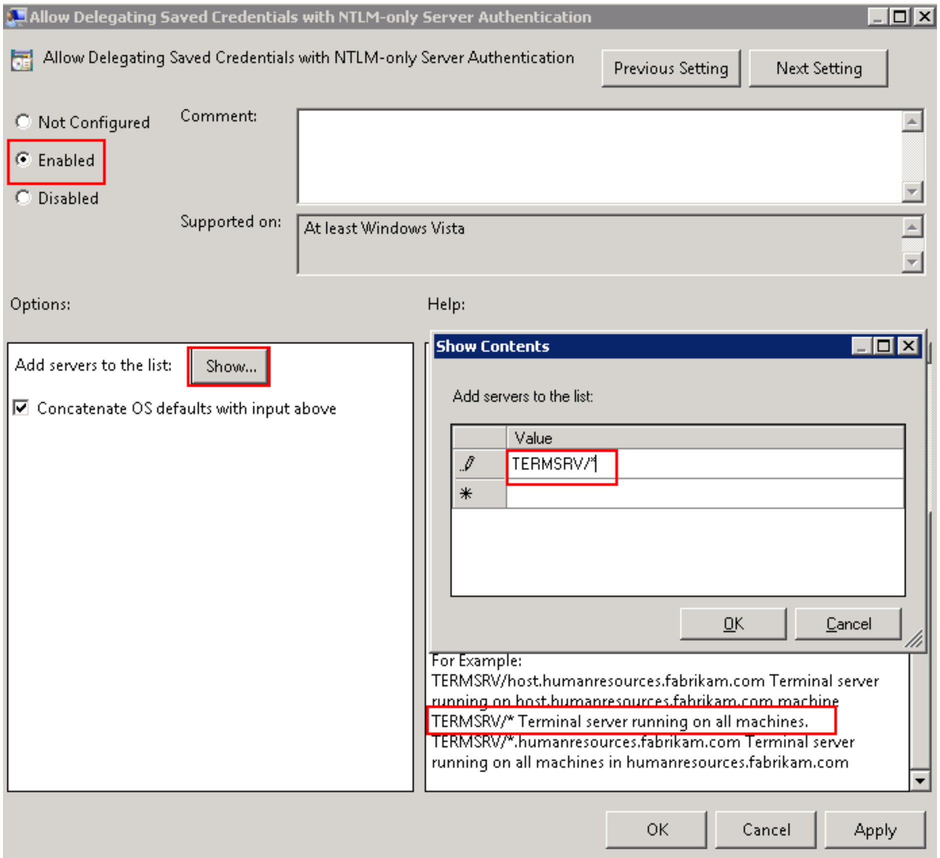
Figure 5-81 Allow Delegating Saved Credentials with NTLM-only Server Authentication



Setting	State
Allow delegating default credentials with NTLM-only server authe…	Not configured
Allow Delegating Default Credentials	Not configured
Encryption Oracle Remediation	Not configured
Allow Delegating Fresh Credentials	Not configured
Allow Delegating Fresh Credentials with NTLM-only Server Authe…	Not configured
Allow Delegating Saved Credentials	Not configured
Allow Delegating Saved Credentials with NTLM-only Server Authe…	Not configured
Deny Delegating Default Credentials	Not configured
Deny Delegating Fresh Credentials	Not configured
Deny Delegating Saved Credentials	Not configured
Restrict delegation of credentials to remote servers	Not configured

5. Select **Enabled** and enter **TERMSRV/*** in the **Show Contents** text box. **TERMSRV/*** indicates the terminal server running on all computers.

Figure 5-82 Enabled



Allow Delegating Saved Credentials with NTLM-only Server Authentication

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Vista

Add servers to the list:

☑ Concatenate OS defaults with input above

Show Contents

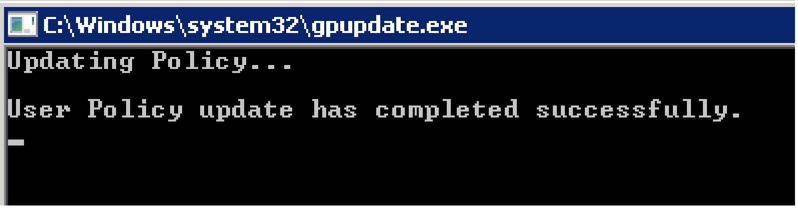
Add servers to the list:

	Value
	TERMSRV/*
*	

For Example:
TERMSRV/host.humanresources.fabrikam.com Terminal server running on host.humanresources.fabrikam.com machine
TERMSRV/* Terminal server running on all machines.
TERMSRV/*.humanresources.fabrikam.com Terminal server running on all machines in humanresources.fabrikam.com

6. Refresh the group policy for the settings to take effect.
7. Choose **Start** > **Run**. In the **Run** dialog box, enter **gpupdate /force** and press **OK** to update the group policy.

Figure 5-83 Updating the group policy

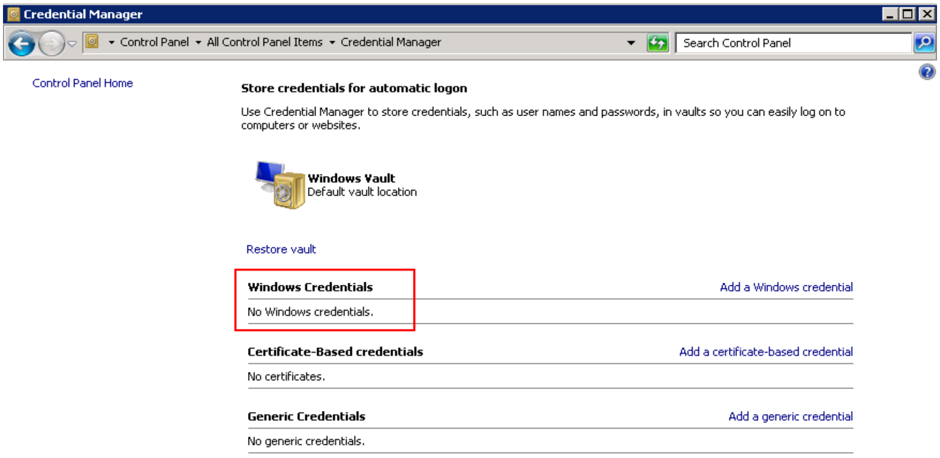


```
C:\Windows\system32\gpupdate.exe
Updating Policy...

User Policy update has completed successfully.
_
```

Step 3: Set the Credentials of the Local Server

1. Open the control panel on the local server and choose **Credential Manager** > **Windows Credentials**.

Figure 5-84 Credential Manager



Credential Manager
Control Panel ▸ All Control Panel Items ▸ Credential Manager
Search Control Panel
Control Panel Home

Store credentials for automatic logon

Use Credential Manager to store credentials, such as user names and passwords, in vaults so you can easily log on to computers or websites.

Windows Credentials Add a Windows credential

No Windows credentials.

Certificate-Based credentials Add a certificate-based credential

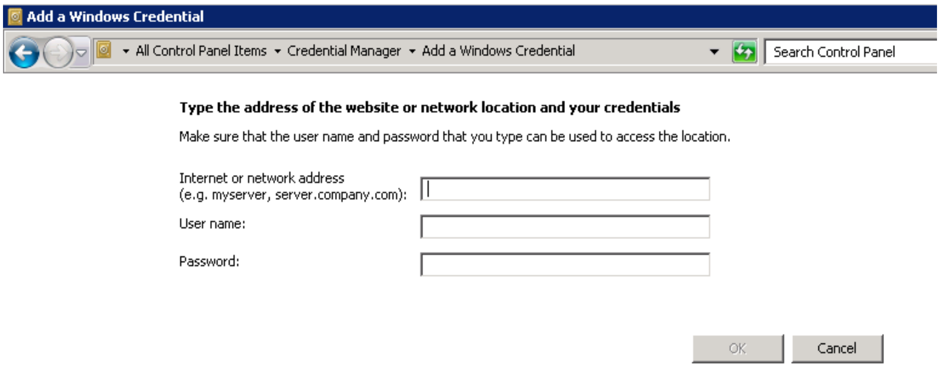
No certificates.

Generic Credentials Add a generic credential

No generic credentials.

2. Check whether the credential of the target ECS is contained in the Windows credentials. If there is no credential, add one.
   - Internet or network address: IP address of the ECS
   - **User name**: Username for logging in to the ECS
   - **Password**: Password for logging in to the ECS

Figure 5-85 Add a Windows Credential



Add a Windows Credential
All Control Panel Items ▸ Credential Manager ▸ Add a Windows Credential
Search Control Panel

Type the address of the website or network location and your credentials

Make sure that the user name and password that you type can be used to access the location.

Internet or network address
(e.g. myserver, server.company.com):

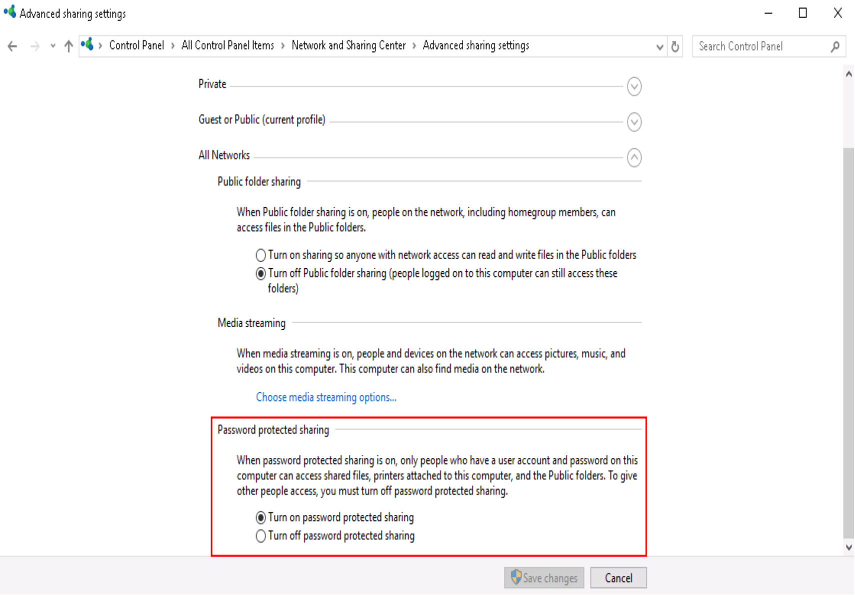
User name:

Password:

Step 4: Disable Password Protected Sharing

1. Log in to the ECS.
2. Choose **Start** > **Control Panel** > **All Control Panel Items** > **Network and Sharing Center** > **Change advanced sharing settings**.
3. In the **Password protected sharing** pane, select **Turn off password protected sharing**.

Figure 5-86 Turn off password protected sharing



Advanced sharing settings
Control Panel › All Control Panel Items › Network and Sharing Center › Advanced sharing settings
Search Control Panel
Private
Guest or Public (current profile)
All Networks
Choose media streaming options...
Save changes
Cancel

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders.

○ Turn on sharing so anyone with network access can read and write files in the Public folders
● Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.

Password protected sharing

When password protected sharing is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.

● Turn on password protected sharing
○ Turn off password protected sharing

4. Click **Save changes**.

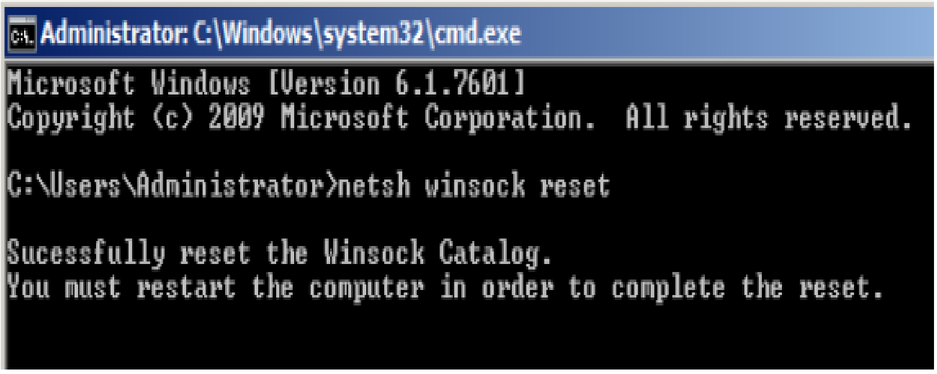
5.4.10 Why Does an Internal Error Occur When I Log In to My Windows ECS?

Symptom

When you attempt to log in to your Windows ECS using MSTSC, the system displays an error message indicating an internal error.

Solution

1. On the local server, run **cmd** as an administrator.
2. Run the **netsh winsock reset** command.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>netsh winsock reset

Sucessfully reset the Winsock Catalog.
You must restart the computer in order to complete the reset.
```

3. Restart the local server.
4. Log in to the ECS again.

   If you still cannot log in to the ECS, check your local network. Change the network (for example, use your phone's mobile data) and check whether you can log in to the ECS remotely.

If you can remotely log in to the ECS using your phone's mobile data, your local network is abnormal. Restart your local network (for example, restart the router).

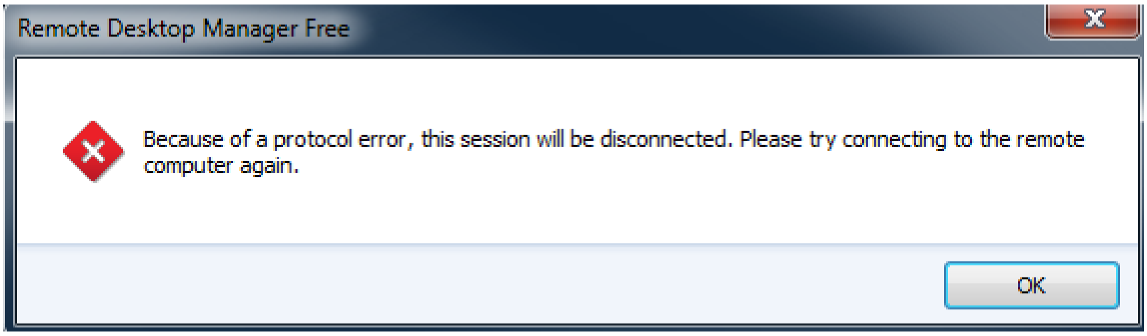
If the fault still persists, record the resource details and fault occurred time. Then, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the management console to submit a ticket.

5.4.11 Why Is My Remote Session Interrupted by a Protocol Error?

Symptom

An error message is displayed indicating that the remote session will be disconnected because of a protocol error.

Figure 5-87 Protocol error



Because of a protocol error, this session will be disconnected. Please try connecting to the remote computer again.

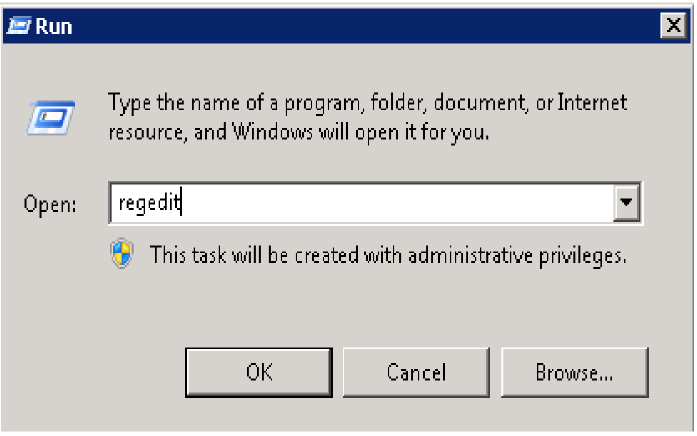
Possible Causes

The registry subkey Certificate is damaged.

Solution

1. In the **Run** dialog box, enter **regedit** and click **OK** to open the registry editor.

   Figure 5-88 Opening the registry editor

   Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

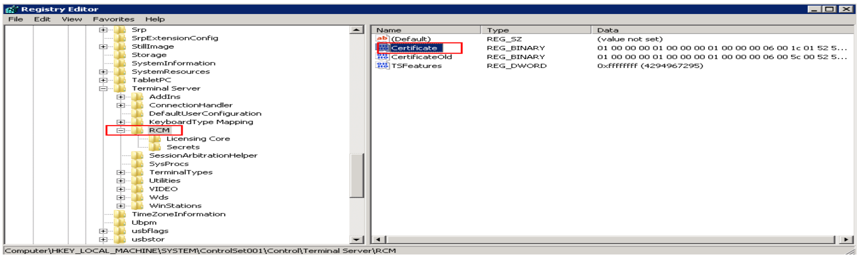
   Open: regedit

   This task will be created with administrative privileges.

2. Choose **HKEY_LOCAL_MACHINE** > **SYSTEM** > **ControlSet001** > **Control** > **Terminal Server** > **RCM**.

3. Delete **Certificate**.

Figure 5-89 Deleting Certificate



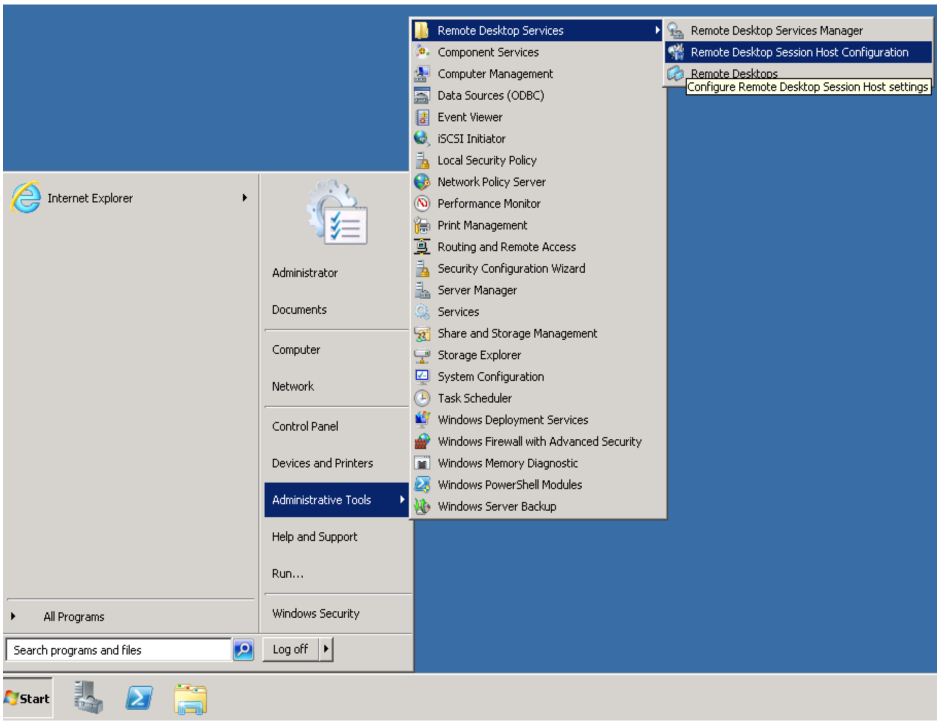
Name	Type	Data
(Default)	REG_SZ	(value not set)
Certificate	REG_BINARY	01 00 00 00 01 00 00 00 01 00 00 00 06 00 1c 01 52 5...
CertificateOld	REG_BINARY	01 00 00 00 01 00 00 00 01 00 00 00 06 00 5c 00 52 5...
TSFeatures	REG_DWORD	0xffffffff (4294967295)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server\RCM

4. Restart the ECS.

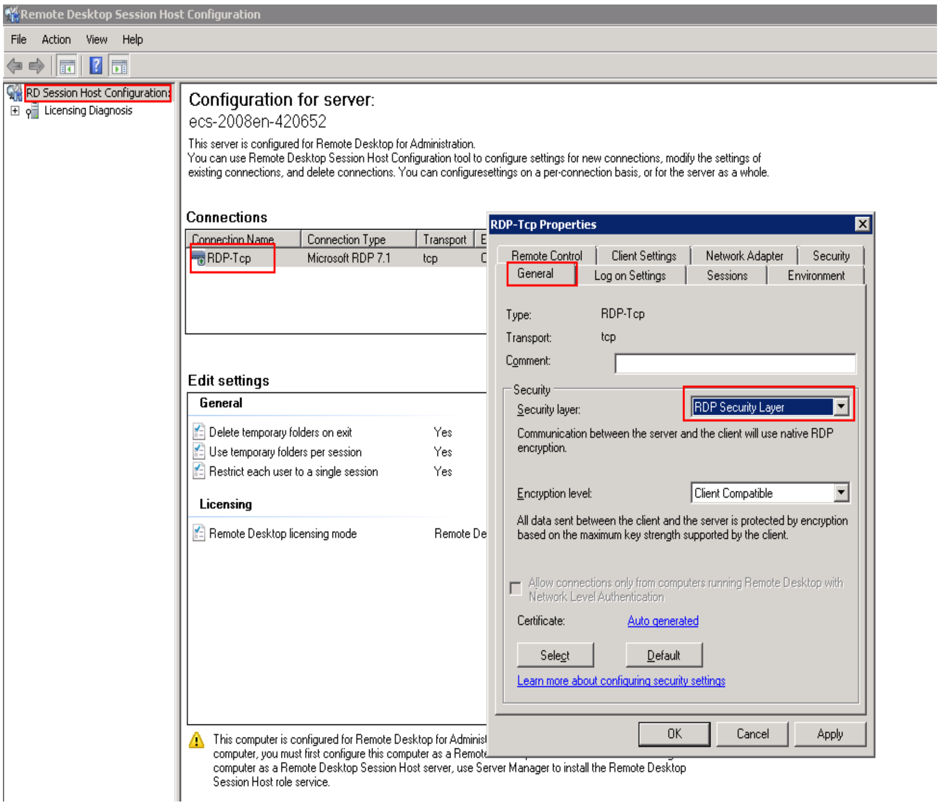
5. Choose **Start** > **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**.

Figure 5-90 Opening Remote Desktop Session Host Configuration



6. Right-click **RDP-Tcp** and choose **Properties**. In the displayed dialog box, click **General** and set **Security layer** to **RDP Security Layer**.

Figure 5-91 RDP-Tcp properties



Configuration for server:
ecs-2008en-420652

This server is configured for Remote Desktop for Administration.
You can use Remote Desktop Session Host Configuration tool to configure settings for new connections, modify the settings of existing connections, and delete connections. You can configuresettings on a per-connection basis, or for the server as a whole.

Connections

Connection Name	Connection Type	Transport
RDP-Tcp	Microsoft RDP 7.1	tcp

Edit settings

General

Delete temporary folders on exit	Yes
Use temporary folders per session	Yes
Restrict each user to a single session	Yes

Licensing

Remote Desktop licensing mode	Remote De

This computer is configured for Remote Desktop for Administ computer, you must first configure this computer as a Remote computer as a Remote Desktop Session Host server, use Server Manager to install the Remote Desktop Session Host role service.

Type: RDP-Tcp
Transport: tcp
Comment:

Security
Security layer: RDP Security Layer

Communication between the server and the client will use native RDP encryption.

Encryption level: Client Compatible

All data sent between the client and the server is protected by encryption based on the maximum key strength supported by the client.

☐ Allow connections only from computers running Remote Desktop with Network Level Authentication

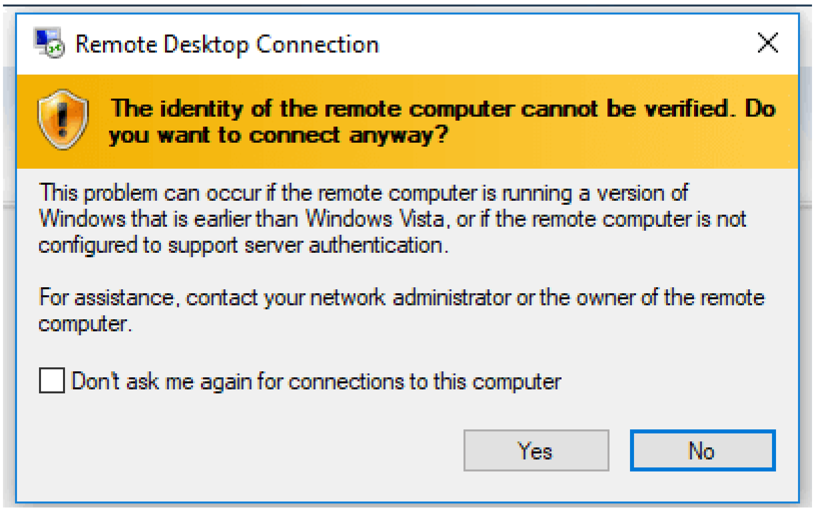
Certificate: Auto generated

5.4.12 Why Am I Seeing an Error Message That Says Identity of Remote Computer Cannot be Verified When I Log In to a Windows ECS?

Symptom

An error message is displayed indicating that the identity of the remote computer cannot be verified. You are required to enter the password and log in again.

Figure 5-92 Protocol error



The identity of the remote computer cannot be verified. Do you want to connect anyway?

This problem can occur if the remote computer is running a version of Windows that is earlier than Windows Vista, or if the remote computer is not configured to support server authentication.

For assistance, contact your network administrator or the owner of the remote computer.

☐ Don't ask me again for connections to this computer

Possible Causes

Security software installed on the ECS prevents logins from unknown IP addresses.

Solution

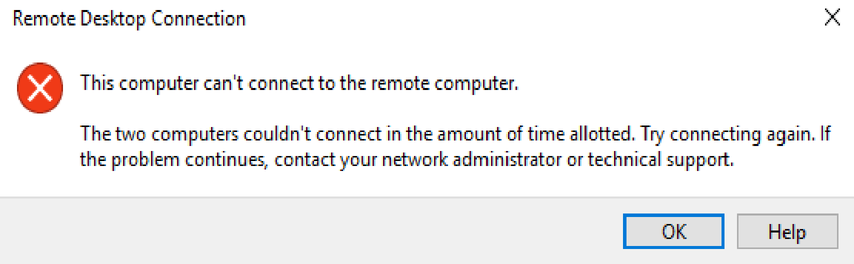
- Uninstall the security software.
- Open the security software and enable the default login mode.

5.4.13 Why Am I Seeing An Error Message That Says The Two Computers Couldn't Be Connected in the Amount of Time Allotted When I Log In to a Windows ECS?

Symptom

An error message is displayed indicating that the computer cannot connect to the remote computer in the amount of time allotted.

Figure 5-93 Error message



This computer can't connect to the remote computer.

The two computers couldn't connect in the amount of time allotted. Try connecting again. If the problem continues, contact your network administrator or technical support.

Solution

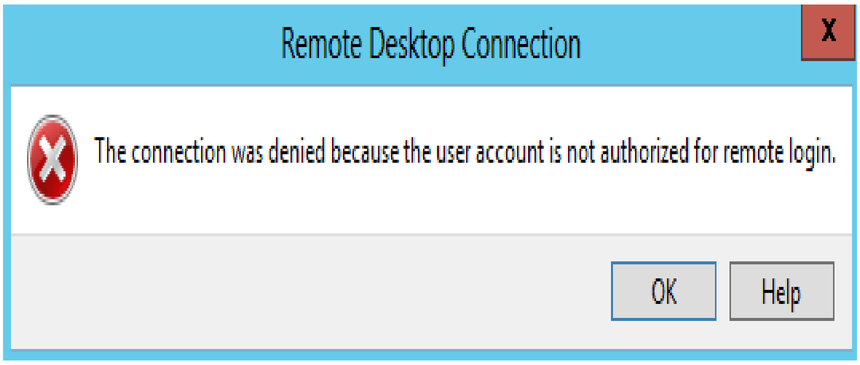
1. On the local computer, click on the **Start** icon, type **cmd** into the box, and run the command as an administrator.
2. Run the **netsh winsock reset** command.
3. Restart the local computer as prompted and reconnect to the ECS.

5.4.14 Why Am I Seeing an Error Message That Says User Account is not Authorized for Remote Login When I Log In to a Windows ECS?

Symptom

An error message is displayed indicating that the connection is denied because the user account is not authorized for remote login.

Figure 5-94 Error message



The connection was denied because the user account is not authorized for remote login.

Possible Causes

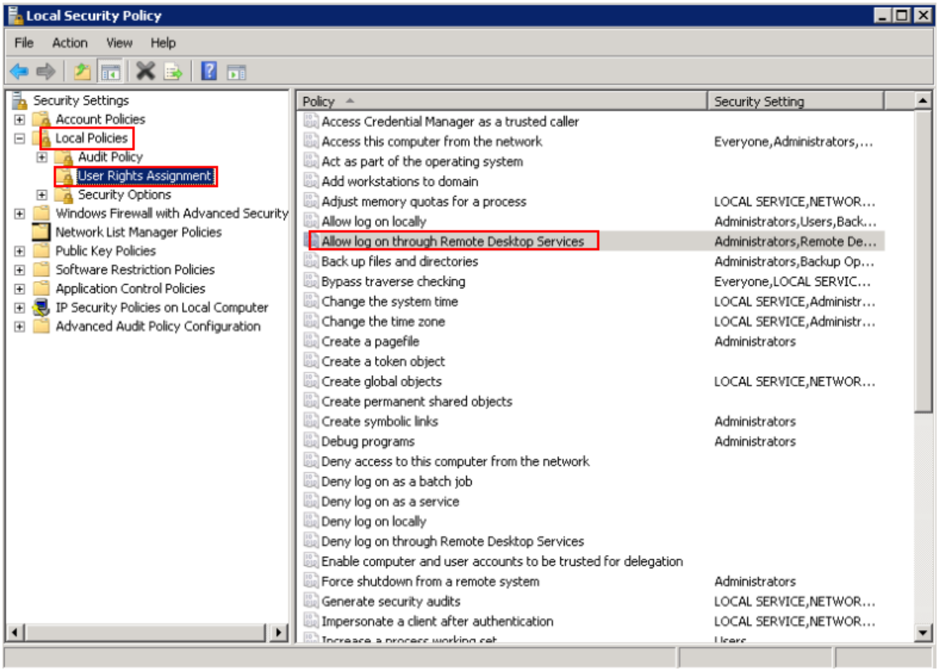
The remote desktop connection permissions have been incorrectly configured.

Solution

Step 1 Check remote desktop permissions on the ECS.

1. In the **Run** dialog box, enter **secpol.msc** and click **OK** to open **Local Security Policy**.
2. Choose **Local Policies** > **User Rights Assignment** > **Allow log on through Remote Desktop Services**.

Figure 5-95 Local security policy

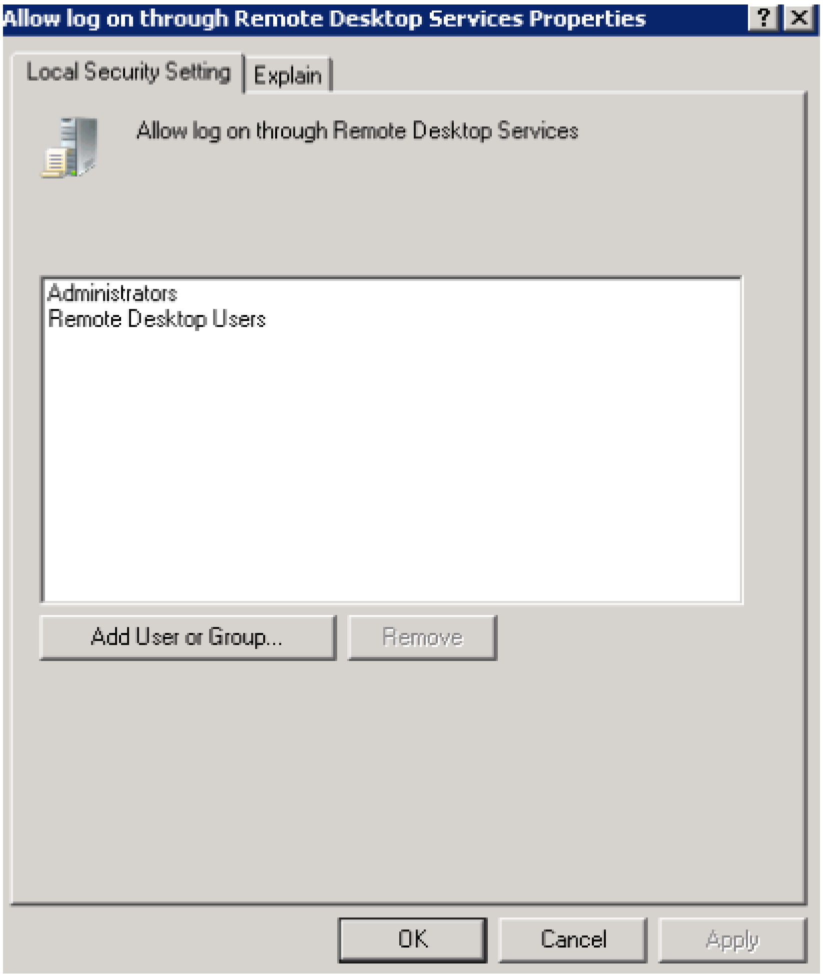

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators,...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWOR...
Allow log on locally	Administrators,Users,Back...
Allow log on through Remote Desktop Services	Administrators,Remote De...
Back up files and directories	Administrators,Backup Op...
Bypass traverse checking	Everyone,LOCAL SERVIC...
Change the system time	LOCAL SERVICE,Administr...
Change the time zone	LOCAL SERVICE,Administr...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWOR...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Deny log on through Remote Desktop Services	
Enable computer and user accounts to be trusted for delegation	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWOR...
Impersonate a client after authentication	LOCAL SERVICE,NETWOR...
Increase a process working set	Users

3. Check whether there are user groups or users that have been granted the remote login permission.

   If not, add required users or groups.

Figure 5-96 Allow log on through Remote Desktop Services properties

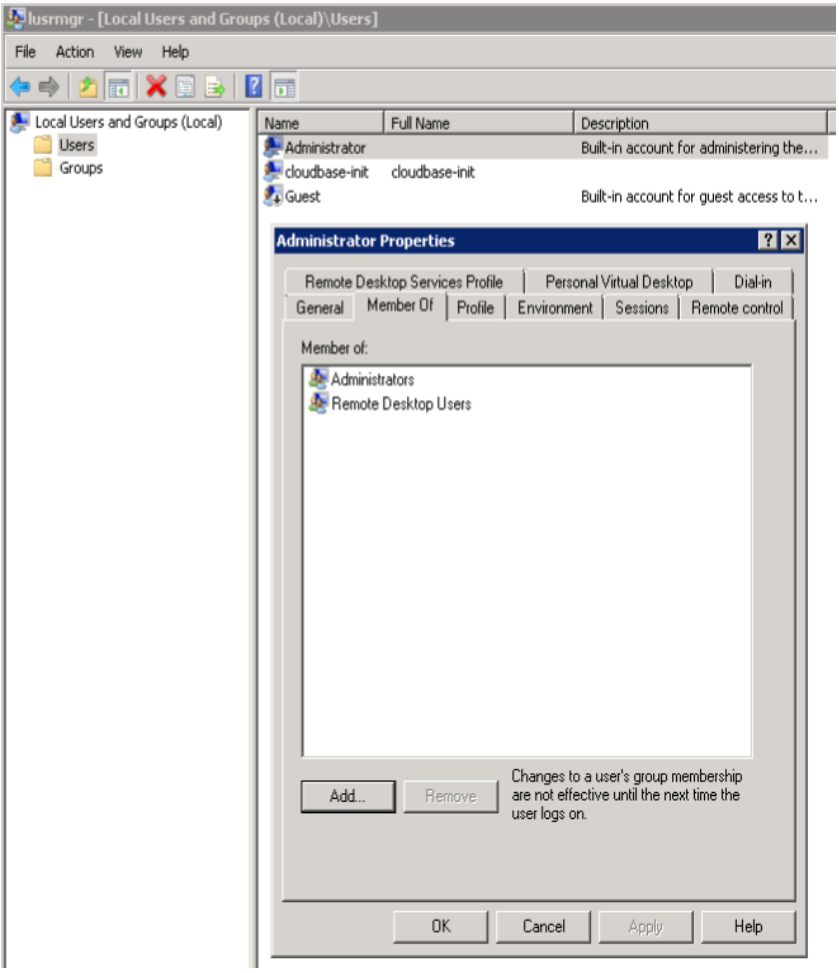

Allow log on through Remote Desktop Services Properties
Local Security Setting
Explain
Allow log on through Remote Desktop Services
Add User or Group...
Remove
OK
Cancel
Apply

Administrators
Remote Desktop Users

Step 2 Check the target user group.

1. Open the **Run** dialog box, enter **lusrmgr.msc**, and click **OK** to open **Local Users and Groups**.
2. Double-click **Users** on the left.
3. Double-click the name of the user to whom the login error message was displayed.
4. In the displayed dialog box, click the **Member Of** tab. Ensure that the user belongs to the user group that is assigned with the remote login permission in **Step 2.2**.

Figure 5-97 Checking the target user group



Name	Full Name	Description
Administrator		Built-in account for administering the...
cloudbase-init	cloudbase-init	
Guest		Built-in account for guest access to t...

Member of:

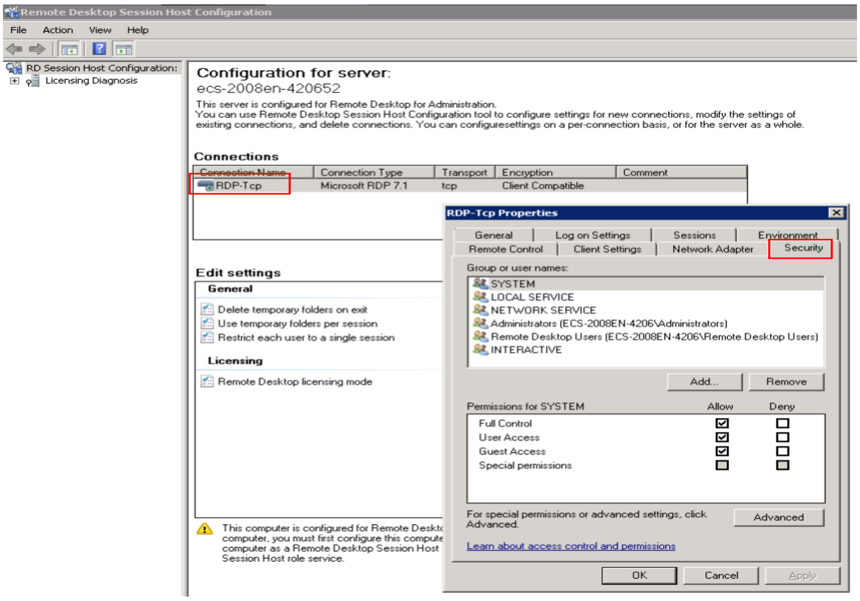
- Administrators
- Remote Desktop Users

Changes to a user's group membership are not effective until the next time the user logs on.

Step 3 Check the remote desktop session host configuration.

1. In the **Run** dialog box, enter **tsconfig.msc** and click **OK** to open **Remote Desktop Session Host Configuration**.
2. Double-click **RDP-Tcp** or other connections added by a user under **Connections** and click the **Security** tab.

Figure 5-98 Security



Configuration for server:
ecs-2008en-420652

This server is configured for Remote Desktop for Administration.
You can use Remote Desktop Session Host Configuration tool to configure settings for new connections, modify the settings of existing connections, and delete connections. You can configuresettings on a per-connection basis, or for the server as a whole.

Connections

Connection Name	Connection Type	Transport	Encryption	Comment
RDP-Tcp	Microsoft RDP 7.1	tcp	Client Compatible	

Edit settings

General

- Delete temporary folders on exit
- Use temporary folders per session
- Restrict each user to a single session

Licensing

- Remote Desktop licensing mode

This computer is configured for Remote Deskt
computer, you must first configure this compute
computer as a Remote Desktop Session Host
Session Host role service.

Group or user names:

- SYSTEM
- LOCAL SERVICE
- NETWORK SERVICE
- Administrators (ECS-2008EN-4206\Administrators)
- Remote Desktop Users (ECS-2008EN-4206\Remote Desktop Users)
- INTERACTIVE

Permissions for SYSTEM	Allow	Deny
Full Control	☑	☐
User Access	☑	☐
Guest Access	☑	☐
Special permissions	☐	☐

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

3. Check whether there are user groups or users that have been granted the remote login permission under **Group or user names**.

   If not, add required users or groups.

4. Restart the ECS or run the following commands in the CLI to restart the Remote Desktop Services:

   net stop TermService

   net start TermService

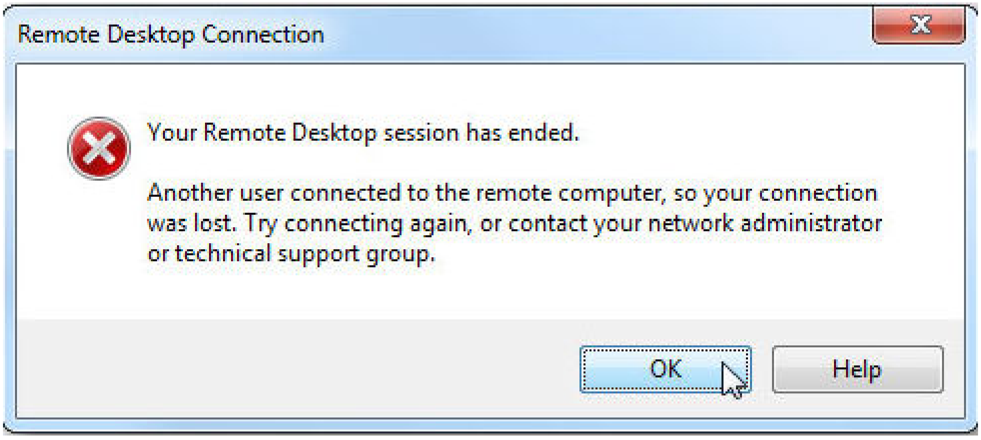
----End

5.4.15 Why Does My Remote Desktop Session End Because Another User Logs In When I Log In to a Windows ECS?

Symptom

An error message is displayed indicating that your remote desktop session has ended because another user has connected to the remote computer.

Figure 5-99 Ended remote desktop session



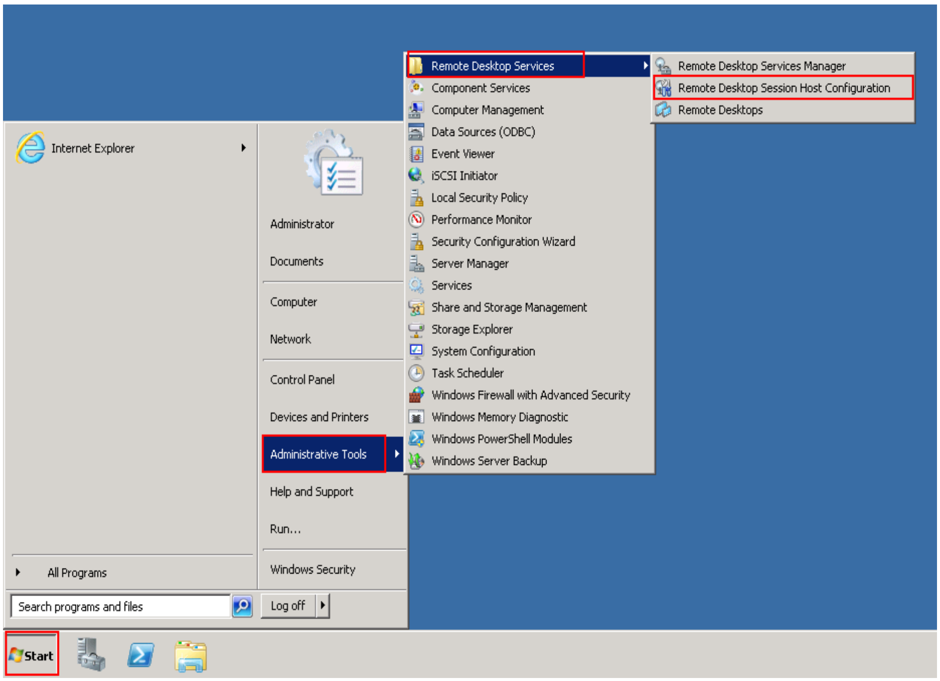
Your Remote Desktop session has ended.

Another user connected to the remote computer, so your connection was lost. Try connecting again, or contact your network administrator or technical support group.

Windows Server 2008

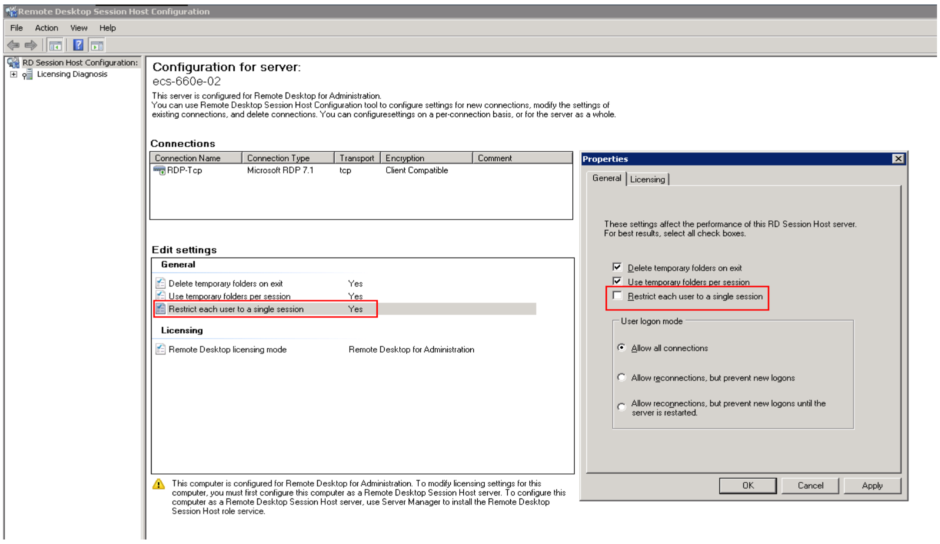
1. Choose **Start** > **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**.

Figure 5-100 Remote Desktop Session Host Configuration



2. Double-click **Restrict each user to a single session** and deselect **Restrict each user to a single session**, and click **OK**.

Figure 5-101 Modifying the configuration



Configuration for server:
ecs-660e-02

This server is configured for Remote Desktop for Administration.
You can use Remote Desktop Session Host Configuration tool to configure settings for new connections, modify the settings of existing connections, and delete connections. You can configuresettings on a per-connection basis, or for the server as a whole.

Connections

Connection Name	Connection Type	Transport	Encryption	Comment
RDP-Tcp	Microsoft RDP 7.1	tcp	Client Compatible	

Edit settings

General

Delete temporary folders on exit	Yes
Use temporary folders per session	Yes
Restrict each user to a single session	Yes

Licensing

Remote Desktop licensing mode	Remote Desktop for Administration

This computer is configured for Remote Desktop for Administration. To modify licensing settings for this computer, you must first configure this computer as a Remote Desktop Session Host server. To configure this computer as a Remote Desktop Session Host server, use Server Manager to install the Remote Desktop Session Host role service.

These settings affect the performance of this RD Session Host server.
For best results, select all check boxes.

☑ Delete temporary folders on exit
☑ Use temporary folders per session
☐ Restrict each user to a single session

User logon mode

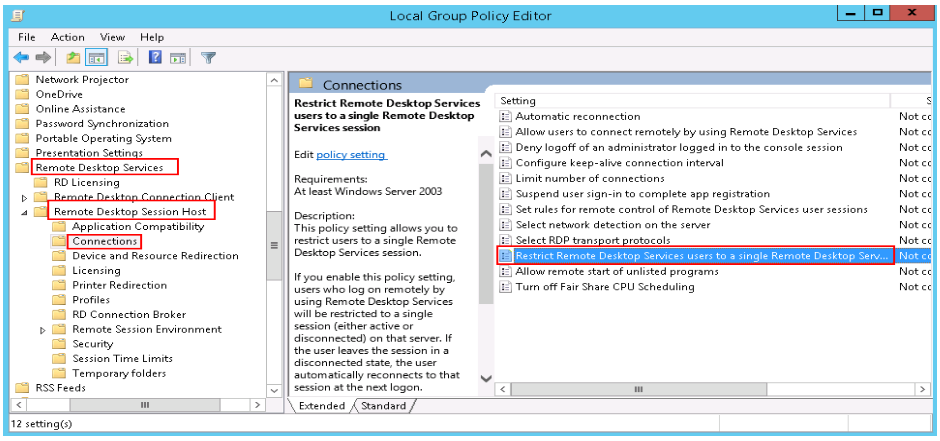
● Allow all connections
○ Allow reconnections, but prevent new logons
○ Allow reconnections, but prevent new logons until the server is restarted.

Windows Server 2012

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

2. Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**.

Figure 5-102 Connections



Restrict Remote Desktop Services users to a single Remote Desktop Services session

Edit policy setting

Requirements:
At least Windows Server 2003

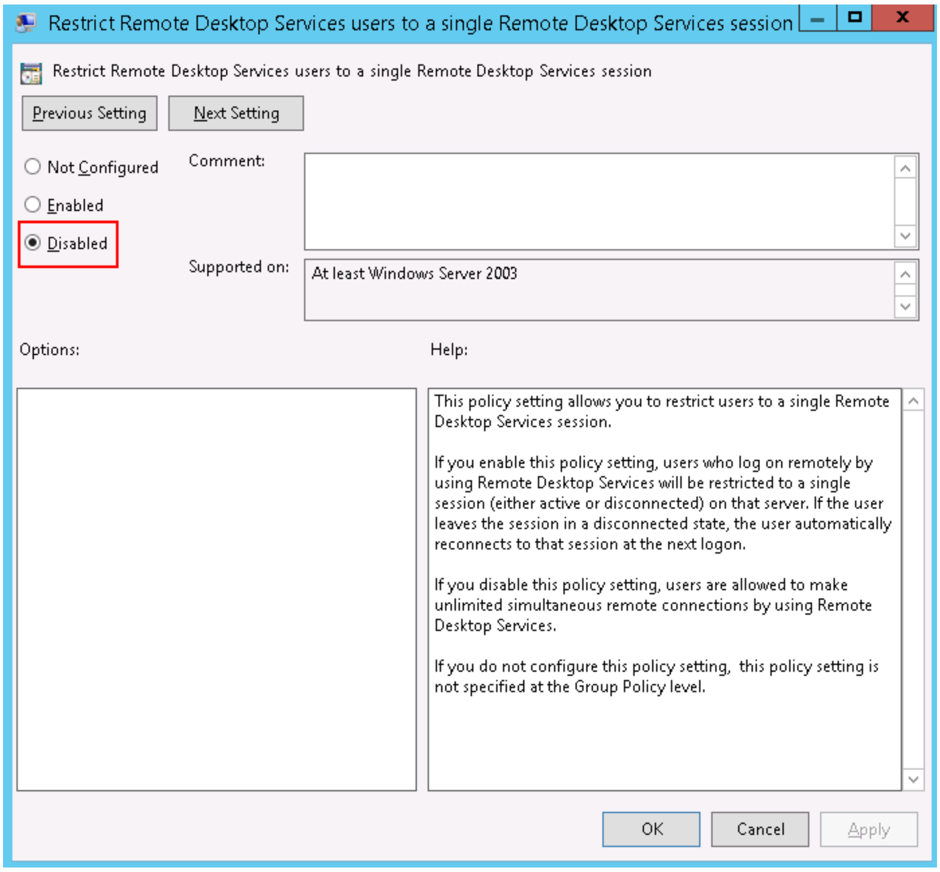
Description:
This policy setting allows you to restrict users to a single Remote Desktop Services session.

If you enable this policy setting, users who log on remotely by using Remote Desktop Services will be restricted to a single session (either active or disconnected) on that server. If the user leaves the session in a disconnected state, the user automatically reconnects to that session at the next logon.

Setting	S
Automatic reconnection	Not co
Allow users to connect remotely by using Remote Desktop Services	Not co
Deny logoff of an administrator logged in to the console session	Not co
Configure keep-alive connection interval	Not co
Limit number of connections	Not co
Suspend user sign-in to complete app registration	Not co
Set rules for remote control of Remote Desktop Services user sessions	Not co
Select network detection on the server	Not co
Select RDP transport protocols	Not co
Restrict Remote Desktop Services users to a single Remote Desktop Serv...	Not co
Allow remote start of unlisted programs	Not co
Turn off Fair Share CPU Scheduling	Not co

3. Double-click **Restrict Remote Desktop Services users to a single Remote Desktop Services session**, change the value to **Disabled**, and click **OK**.

Figure 5-103 Modifying the configuration


Restrict Remote Desktop Services users to a single Remote Desktop Services session
Previous Setting
Next Setting
Options:
Help:
OK
Cancel
Apply

Restrict Remote Desktop Services users to a single Remote Desktop Services session

○ Not Configured
○ Enabled
● Disabled

Comment:

Supported on: At least Windows Server 2003

This policy setting allows you to restrict users to a single Remote Desktop Services session.

If you enable this policy setting, users who log on remotely by using Remote Desktop Services will be restricted to a single session (either active or disconnected) on that server. If the user leaves the session in a disconnected state, the user automatically reconnects to that session at the next logon.

If you disable this policy setting, users are allowed to make unlimited simultaneous remote connections by using Remote Desktop Services.

If you do not configure this policy setting, this policy setting is not specified at the Group Policy level.

4. Run **gpupdate/force** to update the group policy.

5.4.16 Why Does BSOD Occur When I Log In to an ECS Using Remote Desktop Connection?

Symptom

When you attempt to use a remote desktop connection to log in to an ECS running Windows Server 2012 R2 from a local computer with redirected drive enabled, BSOD occurs.

Root Cause

The remote desktop connection with redirected drive enabled loads the desired rdpdr.sys drive, which leads to BSOD and error code 0x18, 0x50, 0xa, 0x27, or 0x133.

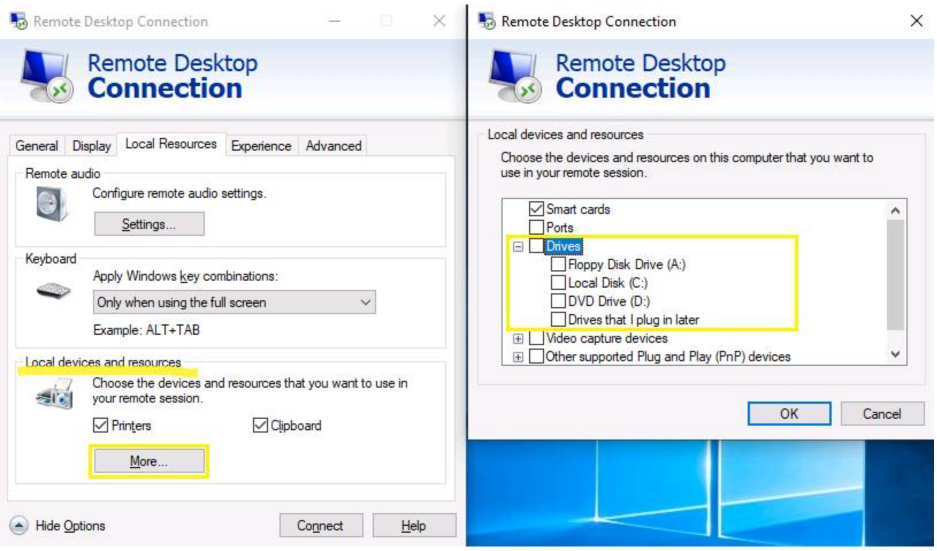
Solution

After you enable the remote desktop connection, disable redirect local drives.

1. Start the **Run** dialog box.
2. Enter **mstsc** and click **OK**.

   The **Remote Desktop Connection** window is displayed.
3. Click **Options** in the lower left corner and click the **Local Resources** tab.
4. In the **Local devices and resources** pane, click **More**.
5. Deselect **Drives**.
6. Click **OK**.

Figure 5-104 Disabling redirect local drives


Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Experience
Advanced
Remote audio
Settings...
Keyboard
Local devices and resources
More...
Hide Options
Connect
Help
Remote Desktop Connection
Remote Desktop Connection
Local devices and resources
OK
Cancel

Configure remote audio settings.

Apply Windows key combinations: Only when using the full screen

Example: ALT+TAB

Choose the devices and resources that you want to use in your remote session.

☑ Printers ☑ Clipboard

Choose the devices and resources on this computer that you want to use in your remote session.

☑ Smart cards
☐ Ports
☐ Drives
  ☐ Floppy Disk Drive (A:)
  ☐ Local Disk (C:)
  ☐ DVD Drive (D:)
  ☐ Drives that I plug in later
☐ Video capture devices
☐ Other supported Plug and Play (PnP) devices

5.4.17 Why Does an ECS Fail to Be Remotely Connected Using RDP and Internal Error Code 4 Is Displayed?

Symptom

An internal error is displayed when you log in to a Windows ECS and you fail to connect to the ECS remotely. Generally, this problem occurs because the Remote Desktop Services is busy.

Possible Causes

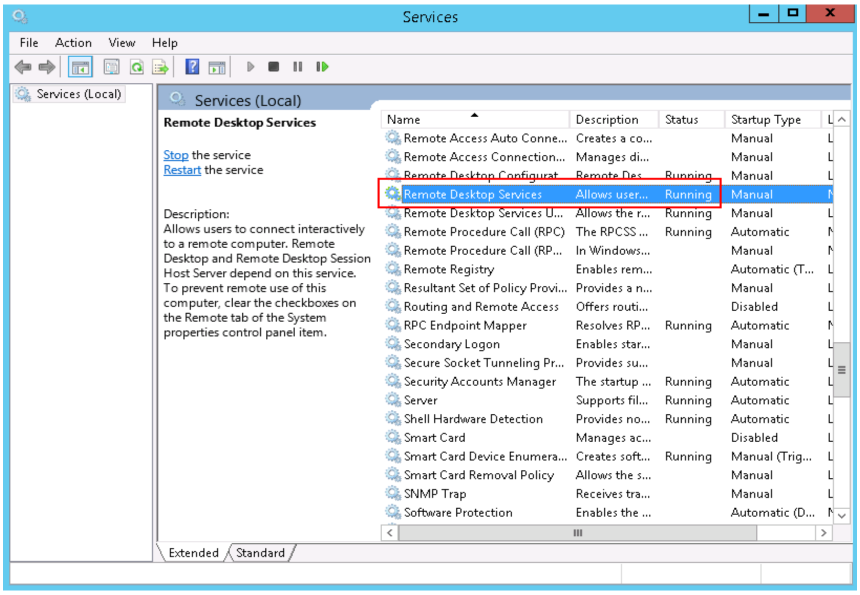
The Remote Desktop Services is busy.

The remote desktop is disconnected after login but is not logged out. To prevent this problem, log out of the ECS if you do not need to remotely connect to it.

Solution

1. Use VNC provided by the management console to remotely log in to the ECS.
2. Open the Windows search box, enter **services**, and select **Services**.
3. In the **Services** window, restart **Remote Desktop Services**. Ensure that **Remote Desktop Services** is in the **Running** status.

Figure 5-105 Remote Desktop Services



Description:
Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service. To prevent remote use of this computer, clear the checkboxes on the Remote tab of the System properties control panel item.

Name	Description	Status	Startup Type	L
Remote Access Auto Conne...	Creates a co...		Manual	L
Remote Access Connection...	Manages di...		Manual	L
Remote Desktop Configurat...	Remote Des...	Running	Manual	L
Remote Desktop Services	Allows user...	Running	Manual	N
Remote Desktop Services U...	Allows the r...	Running	Manual	L
Remote Procedure Call (RPC)	The RPCSS ...	Running	Automatic	N
Remote Procedure Call (RP...	In Windows...		Manual	N
Remote Registry	Enables rem...		Automatic (T...	L
Resultant Set of Policy Provi...	Provides a n...		Manual	L
Routing and Remote Access	Offers routi...		Disabled	L
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	N
Secondary Logon	Enables star...		Manual	L
Secure Socket Tunneling Pr...	Provides su...		Manual	L
Security Accounts Manager	The startup ...	Running	Automatic	L
Server	Supports fil...	Running	Automatic	L
Shell Hardware Detection	Provides no...	Running	Automatic	L
Smart Card	Manages ac...		Disabled	L
Smart Card Device Enumera...	Creates soft...	Running	Manual (Trig...	L
Smart Card Removal Policy	Allows the s...		Manual	L
SNMP Trap	Receives tra...		Manual	L
Software Protection	Enables the ...		Automatic (D...	N

4. Remotely connect to the ECS again.

   If the connection still fails, run the cmd command on the local server as the administrator, run the **netsh winsock reset** command to restore the default network connection configurations, and then retry the remote connection.

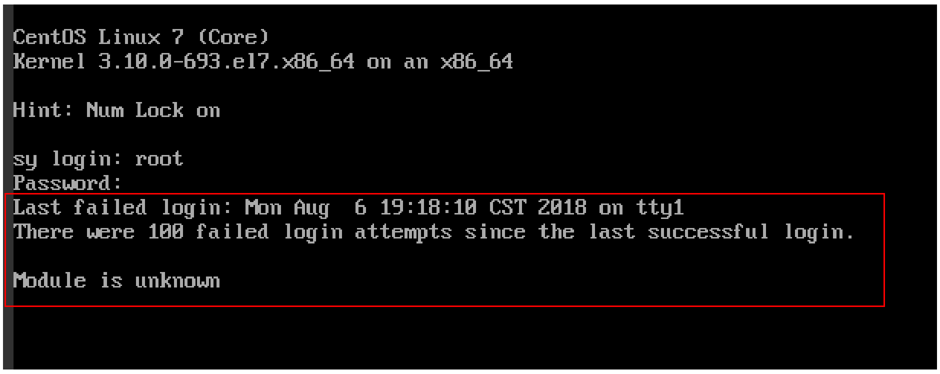
5.5 Remote Login Errors on Linux

5.5.1 Why Am I Seeing the Error Message "Module is unknown" When I Remotely Log In to a Linux ECS?

Symptom

When you attempt to remotely log in to a Linux ECS, the system displays the error message "Module is unknown".

Figure 5-106 Module is unknown



```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.el7.x86_64 on an x86_64

Hint: Num Lock on

sy login: root
Password:
Last failed login: Mon Aug  6 19:18:10 CST 2018 on tty1
There were 100 failed login attempts since the last successful login.

Module is unknown
```

NOTE

- To resolve this issue, restart the ECS and enter the rescue mode.
- Restarting the ECS may interrupt services. Exercise caution when performing this operation.

Root Cause

The file in the **/etc/pam.d/** directory was modified by mistake.

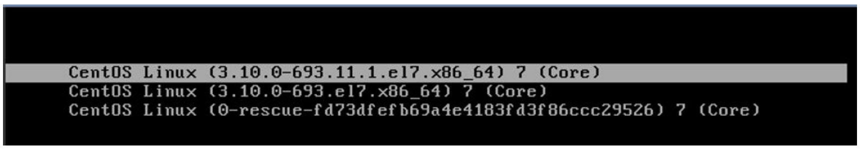
Solution

1. Enter single-user mode.

   The following uses CentOS 7 as an example:

   a. Restart the ECS and click **Remote Login**.
   b. Click **Ctrl+Alt+Del** in the upper part of the remote login panel to restart the ECS.
   c. Press the up arrow key to prevent automatic system startup. When the kernels are displayed, press **e** to enter the editing mode.

   Figure 5-107 Entering the kernel editing mode



```
        CentOS Linux (3.10.0-693.11.1.el7.x86_64) 7 (Core)
        CentOS Linux (3.10.0-693.el7.x86_64) 7 (Core)
        CentOS Linux (0-rescue-fd73dfefb69a4e4183fd3f86ccc29526) 7 (Core)
```

NOTE

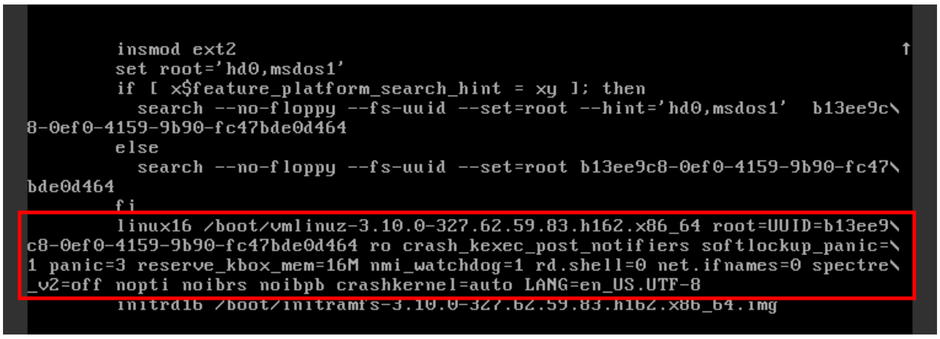
The grub file is encrypted by Euler images by default. Before entering the edit mode, you need to contact customer service to obtain username and password.

d. Locate the row containing **linux16** and delete the parameters you do not require.

e. Change **ro** to **rw** for mounting the root partition with read-write permissions.

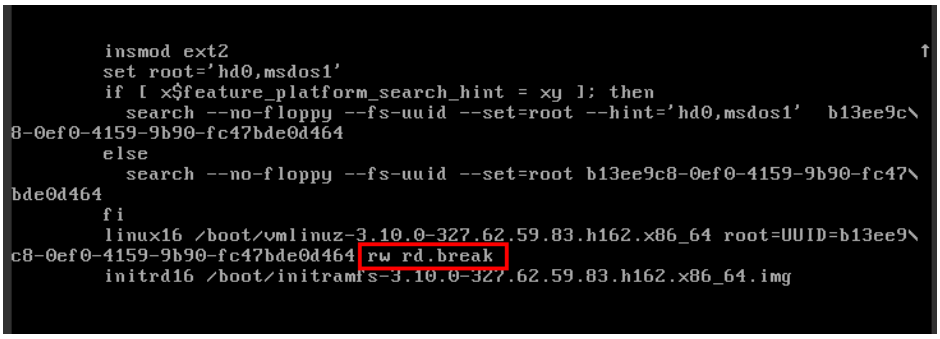
f. Add **rd.break** and press **Ctrl+X**.

Figure 5-108 Before the modification



```
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  b13ee9c\
8-0ef0-4159-9b90-fc47bde0d464
        else
          search --no-floppy --fs-uuid --set=root b13ee9c8-0ef0-4159-9b90-fc47\
bde0d464
        fi
        linux16 /boot/vmlinuz-3.10.0-327.62.59.83.h162.x86_64 root=UUID=b13ee9\
c8-0ef0-4159-9b90-fc47bde0d464 ro crash_kexec_post_notifiers softlockup_panic=\
1 panic=3 reserve_kbox_mem=16M nmi_watchdog=1 rd.shell=0 net.ifnames=0 spectre\
_v2=off nopti noibrs noibpb crashkernel=auto LANG=en_US.UTF-8
        initrd16 /boot/initramfs-3.10.0-327.62.59.83.h162.x86_64.img
```

Figure 5-109 After the modification



```
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  b13ee9c\
8-0ef0-4159-9b90-fc47bde0d464
        else
          search --no-floppy --fs-uuid --set=root b13ee9c8-0ef0-4159-9b90-fc47\
bde0d464
        fi
        linux16 /boot/vmlinuz-3.10.0-327.62.59.83.h162.x86_64 root=UUID=b13ee9\
c8-0ef0-4159-9b90-fc47bde0d464 rw rd.break
        initrd16 /boot/initramfs-3.10.0-327.62.59.83.h162.x86_64.img
```

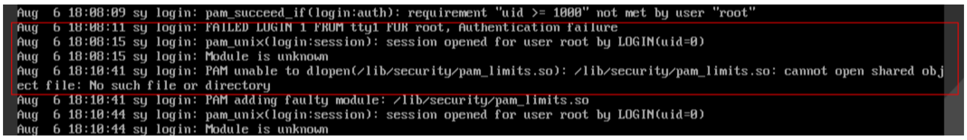
g. Run the following command to go to the **/sysroot** directory:

chroot /sysroot

2. Run the following command to view the system log for error files:

grep Module /var/log/messages

Figure 5-110 System log

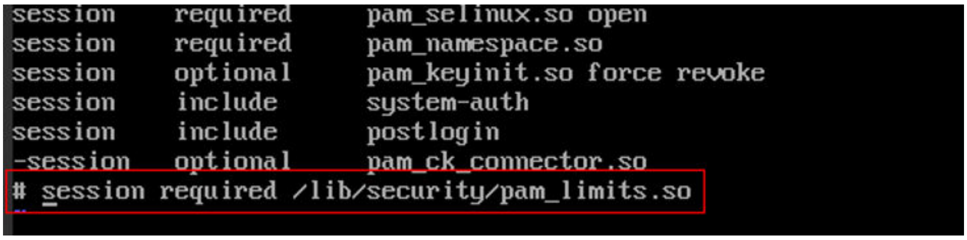


```
Aug  6 18:08:09 sy login: pam_succeed_if(login:auth): requirement "uid >= 1000" not met by user "root"
Aug  6 18:08:11 sy login: FAILED LOGIN 1 FROM tty1 FOR root, Authentication failure
Aug  6 18:08:15 sy login: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Aug  6 18:08:15 sy login: Module is unknown
Aug  6 18:10:41 sy login: PAM unable to dlopen(/lib/security/pam_limits.so): /lib/security/pam_limits.so: cannot open shared obj
ect file: No such file or directory
Aug  6 18:10:41 sy login: PAM adding faulty module: /lib/security/pam_limits.so
Aug  6 18:10:44 sy login: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Aug  6 18:10:44 sy login: Module is unknown
```

3. Comment out or modify the error line in the error files displayed in the system log.

vi /etc/pam.d/login

Figure 5-111 Modifying the error information



```
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      system-auth
session    include      postlogin
-session   optional     pam_ck_connector.so
# session required /lib/security/pam_limits.so
```

4. Restart the ECS and try to log in to it again.

NOTE

- To view the modification records and check whether the modification is caused by unintended actions, run the following command:

  vi /root/.bash_history

  Search for the keyword **vi** or **login**.
- Do not modify the files in the **/etc/pam.d/** directory. Run the following command for details about pam:

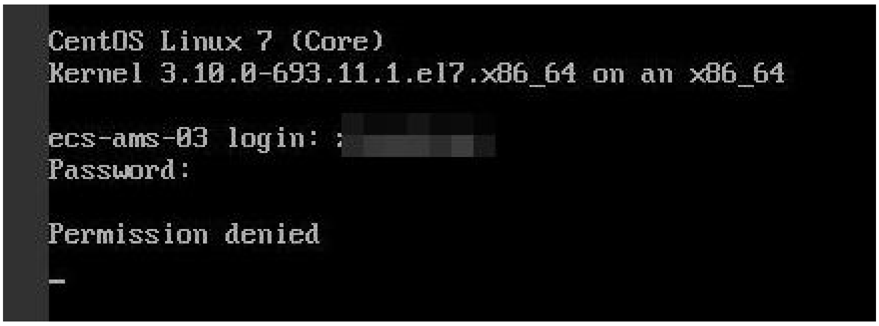
  man pam.d

5.5.2 What Should I Do If Error Message "Permission denied" Is Displayed When I Remotely Log In to a Linux ECS?

Symptom

When I attempted to remotely log in to a Linux ECS, the system displayed error Message "Permission denied".

Figure 5-112 Permission denied



```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.11.1.el7.x86_64 on an x86_64

ecs-ams-03 login: [redacted]
Password:

Permission denied

_
```

NOTE

- To resolve this issue, you are required to restart the ECS and enter the rescue mode.
- Restarting the ECS may interrupt services. Exercise caution when performing this operation.

Root Cause

The **nofile** parameter in **/etc/security/limits.conf** is used to set the maximum number of files that can be opened in the system. If the value is greater than the **fs.nr_open** value (**1048576** by default) set in **PermissionDenied.png**, a login verification error will occur, leading to "Permission denied".

Solution

1. Enter single-user mode.

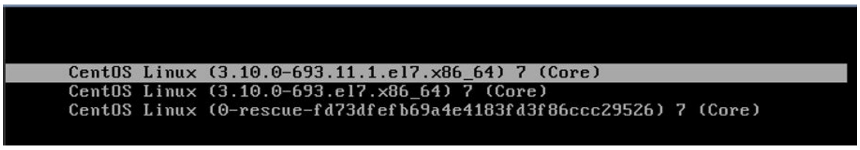
   The following uses CentOS 7 as an example:

   a. Restart the ECS and click **Remote Login**.

   b. Click **Ctrl+Alt+Del** in the upper part of the remote login panel to restart the ECS.

   c. Press the up arrow key to prevent automatic system startup. When the kernels are displayed, press **e** to enter the editing mode.

Figure 5-113 Entering the kernel editing mode



```
    CentOS Linux (3.10.0-693.11.1.el7.x86_64) 7 (Core)
    CentOS Linux (3.10.0-693.el7.x86_64) 7 (Core)
    CentOS Linux (0-rescue-fd73dfefb69a4e4183fd3f86ccc29526) 7 (Core)
```

NOTE

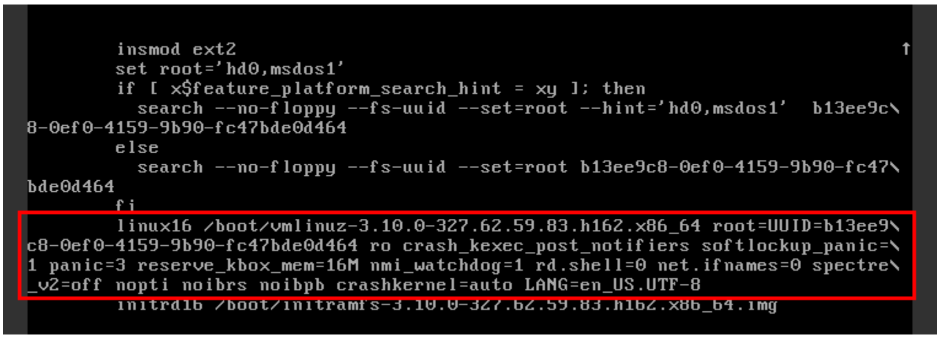
The grub file is encrypted by Euler images by default. Before entering the edit mode, you need to contact customer service to obtain username and password.

   d. Locate the row containing **linux16** and delete the parameters you do not require.

   e. Change **ro** to **rw** for mounting the root partition with read-write permissions.

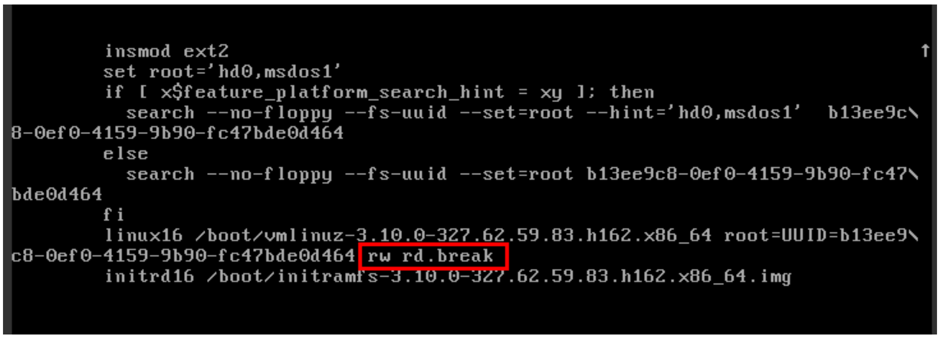
   f. Add **rd.break** and press **Ctrl+X**.

Figure 5-114 Before the modification



```
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  b13ee9c\
8-0ef0-4159-9b90-fc47bde0d464
        else
          search --no-floppy --fs-uuid --set=root b13ee9c8-0ef0-4159-9b90-fc47\
bde0d464
        fi
        linux16 /boot/vmlinuz-3.10.0-327.62.59.83.h162.x86_64 root=UUID=b13ee9\
c8-0ef0-4159-9b90-fc47bde0d464 ro crash_kexec_post_notifiers softlockup_panic=\
1 panic=3 reserve_kbox_mem=16M nmi_watchdog=1 rd.shell=0 net.ifnames=0 spectre\
_v2=off nopti noibrs noibpb crashkernel=auto LANG=en_US.UTF-8
        initrd16 /boot/initramfs-3.10.0-327.62.59.83.h162.x86_64.img
```

Figure 5-115 After the modification



```
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  b13ee9c\
8-0ef0-4159-9b90-fc47bde0d464
        else
          search --no-floppy --fs-uuid --set=root b13ee9c8-0ef0-4159-9b90-fc47\
bde0d464
        fi
        linux16 /boot/vmlinuz-3.10.0-327.62.59.83.h162.x86_64 root=UUID=b13ee9\
c8-0ef0-4159-9b90-fc47bde0d464 rw rd.break
        initrd16 /boot/initramfs-3.10.0-327.62.59.83.h162.x86_64.img
```

   g. Run the following command to go to the **/sysroot** directory:

      chroot /sysroot

2. Run the following command to view the **fs.nr_open** value:

   sysctl fs.nr_open

3. Change the **nofile** value in **/etc/security/limits.conf** so that the value is smaller than the **fs.nr_open** value obtained in 2.

   vi /etc/security/limits.conf

   NOTE

   limits.conf is the **pam_limits.so** configuration file of Linux Pluggable Authentication Module (PAM). For more details, run the following command:

   man limits.conf

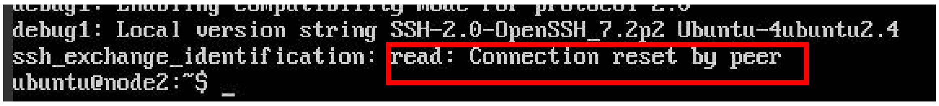
4. Restart the ECS and try to log in to it again.

5.5.3 What Should I Do If Error Message "read: Connection reset by peer" Is Displayed When I Remotely Log In to a Linux ECS?

Symptom

When I attempted to remotely log in to a Linux ECS, the system displayed error message "read: Connection reset by peer".

Figure 5-116 read: Connection reset by peer



```
debug1: Local version string SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4
ssh_exchange_identification: read: Connection reset by peer
ubuntu@node2:~$ _
```

Possible Causes

- The remote login port is not permitted in the security group.
- The firewall is enabled on the ECS, but the remote login port is blocked by the firewall.

Solution

Perform the following operations for troubleshooting:

- **Check security group rules.**
  - Inbound: Add the remote login port. The default port 22 is used as an example.
  - Outbound: Outbound rules allow network traffic to be out of specified ports.
- **Add a port to the ECS firewall exception.**

  The following uses Ubuntu as an example:

  a. Run the following command to view the firewall status:

     sudo ufw status

The following information is displayed:

```
Status: active
```

b. Add a port to the firewall exception, taking the default port 22 as an example.

```
ufw allow 22
Rule added
Rule added (v6)
```

c. Run following command to check the firewall status again:

```
sudo ufw status
```

```
Status: active
To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
```

Try to remotely log in to the ECS again.

5.5.4 Why Am I Seeing the Error Message "Access denied" When I Remotely Log In to a Linux ECS?

Symptom

When you attempt to remotely log in to a Linux ECS, the system displays the error message "Access denied".

Possible Causes

- Incorrect username or password.
- A policy that denies logins from user **root** is enabled on the SSH server.

Solution

- The username or password is incorrect.

  Check the username and password.

  The default username for logging in to a Linux ECS is **root**. If the password is incorrect, reset it on the management console.

  To reset a password, locate the row containing the target ECS, click **More** in the **Operation** column, and select **Reset Password** from the drop-down list.

- A policy that denies logins from user **root** is enabled on the SSH server.

  a. Edit the **/etc/ssh/sshd_config** file and check the following settings to ensure that the SSH logins from user **root** are allowed:

  ```
  PermitRootLogin yes
  ```

  b. Restart SSH.

  - CentOS 6

    ```
    service sshd restart
    ```

  - CentOS 7

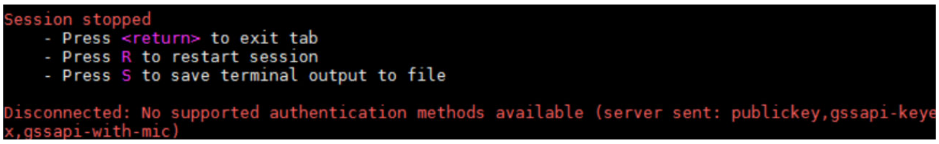
    ```
    systemctl restart sshd
    ```

5.5.5 What Should I Do If Error Message "Disconnected: No supported authentication methods available" Is Displayed When I Remotely Log In to a Linux ECS?

Symptom

When I attempted to remotely log in to a Linux ECS, the system displayed error message "Disconnected: No supported authentication methods available".

Figure 5-117 No supported authentication methods available



```
Session stopped
    - Press <return> to exit tab
    - Press R to restart session
    - Press S to save terminal output to file

Disconnected: No supported authentication methods available (server sent: publickey,gssapi-keye
x,gssapi-with-mic)
```

Possible Causes

A policy that denies password-authenticated logins is enabled on the SSH server.

Solution

1. Open the **/etc/ssh/sshd_config** file and check the following settings:

   vi /etc/ssh/sshd_config

2. Modify the following settings:

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

   Alternatively, delete the comment tag (#) before **PasswordAuthentication yes**.

3. Restart SSH.
   - CentOS 6

     service sshd restart
   - CentOS 7

     systemctl restart sshd

6 Billing

6.1 What Are the Differences Between Yearly/Monthly and Pay-per-Use Billing Modes?

Yearly/Monthly

Yearly/Monthly is a prepaid billing mode and is cost-effective for long-term use.

Note the following when using a yearly/monthly ECS:

1. A created yearly/monthly ECS cannot be deleted. If such an ECS is not required anymore, unsubscribe from it. To do so, switch to the **Elastic Cloud Server** page, locate the target ECS, and choose **More** > **Unsubscribe** in the **Operation** column.
2. A detached system disk can be used as a data disk for any ECSs, but can only be used as a system disk for the ECS where it was attached before.
3. A detached data disk that is purchased together with an ECS can only be used as a data disk for this ECS.

Pay-per-Use

Pay-per-use billing is a postpaid billing mode in which an ECS will be billed based on usage frequency and duration. ECSs are billed by the second. The system generates a bill every hour based on the usage duration and deducts the billed amount from the account balance. A pay-per-use ECS can be provisioned and deleted at any time.

In the pay-per-use billing mode, ECSs are billed by the second. The price per second of each type of ECS can be obtained by dividing their hourly price by 3600. Obtain the hourly price on the **Product Pricing Details** page.

For example, if you purchase a pay-per-use ECS priced $0.68 USD/hour, the ECS will be billed based on the usage duration by the second. The prices are examples only. The actual prices are those displayed on **ECS Pricing Details**.

- If you use the ECS for 30 minutes, you need to pay $0.34 USD (0.68/3,600 × 30 × 60).

- If you use the ECS for 1 hour and 30 minutes, you need to pay $1.02 USD (0.68/3,600 × 90 × 60).

NOTE

If a pay-per-use ECS is stopped and then restarted, the startup may fail due to insufficient resources. In such a case, change the ECS flavor or wait several minutes before attempting another restart.

Which One Is More Cost-Effective?

The yearly/monthly payment is more cost-effective than the pay-per-use payment for a longer usage duration. Yearly/Monthly is ideal when your resource usage duration is predictable. Pay-per-use is recommended when you want more flexibility and control on ECS usage. Pay-per-use ECSs can be provisioned or deleted at any time.

6.2 Will I Be Billed After ECSs Are Stopped?

ECSs support multiple billing modes. Whether you will continue to be billed after ECSs are stopped depend on the billing mode of the stopped ECSs.

- Yearly/Monthly: a prepaid billing mode. You are billed based on the subscription term you purchase. Stopping ECSs does not affect the billing.
- Spot pricing (for spot block): a postpaid billing mode. You are billed based on the usage duration and predefined duration. After ECSs are stopped, you will continue to be billed.
- Pay-per-use and spot pricing (for spot instances): a postpaid billing mode. You are billed based on the usage duration. Whether you are billed after ECSs are stopped depends on the instance type. For details about the billing policy for stopped ECSs, see **Table 6-1**.

Table 6-1 Billing for a stopped ECS

Instance Type	Description	Billing Item	Billed or Not	Action on Resources
Common instances	Common instances include: - Non-bare-metal instance - Instances without local disks - Instances without FPGA cards	ECS (compute resources including vCPUs and memory)	No	- If ECSs are created from public resource pools, basic resources (vCPUs and memory) are no longer retained. The ECS may fail to be started due to insufficient resources. Wait patiently and try again later. - If ECSs are created on a DeH or in an edge AZ, basic resources (vCPUs and memory) will be retained.
		Image	No	Resources are retained but are not billed.
		GPU	No	After GPU-accelerated ECSs without local disks attached are stopped, GPU resources are no longer retained.
		EVS disks (system and data disks)	Yes	The resources are still billed based on the billing rules.
		EIP bandwidth	Yes	The resources are still billed based on the billing rules. - EIP bandwidth price: pay-per-use EIPs (by bandwidth) - Shared bandwidth price For details, see **EIP Billing**.

Instance Type	Description	Billing Item	Billed or Not	Action on Resources
Special instances	Special instances include: • Bare metal instances • Instances with local disks such as disk-intensive, ultra-high I/O ECSs. • ECSs with FPGA cards	ECS (compute resources including vCPUs and memory)	Yes	The ECS resources are still billed based on the billing rules. To stop the billing, you need to delete the instance and its associated resources.
		Image	Yes	
		GPU	Yes	
		EVS disks (system and data disks)	Yes	
		EIP bandwidth	Yes	

NOTE

For a stopped pay-per-use ECS, the startup may fail due to insufficient resources. Please wait for several minutes before attempting another restart or changing the ECS specifications.

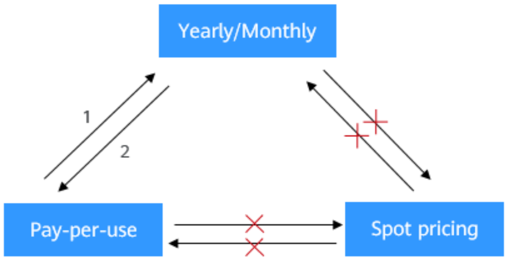
For details, see **How Can I Stop an ECS from Being Billed?**

If you want to use an ECS for a long time, you can change its billing mode from pay-per-use to yearly/monthly to reduce cost. For details, see **Changing Pay-per-Use to Yearly/Monthly**.

6.3 Can I Switch Between Yearly/Monthly and Pay-per-Use Billing Modes?

Yes, you can switch between yearly/monthly and pay-per-use payments.

Figure 6-1 ECS billing mode changes



1. After the order is paid, the yearly/monthly billing mode takes effect immediately.
2. After the change is successful, the pay-per-use billing mode takes effect immediately.
×: The billing mode cannot be changed.

- Changing pay-per-use to yearly/monthly

  Pay-per-use is a postpaid billing mode in which your ECS is billed by usage duration. You can create or delete such an ECS at any time.

  If you want to use an ECS for a long time, you can change its billing mode from pay-per-use to yearly/monthly to reduce cost. For details, see **Changing Pay-per-Use to Yearly/Monthly**.
- Changing yearly/monthly to pay-per-use

  Yearly/Monthly is a prepaid billing mode in which your ECS will be billed based on service duration. This cost-effective mode is ideal when the duration of ECS usage is predictable.

  If you require a more flexible billing mode, in which your ECS will be billed based on the actual usage, you can change the billing mode from yearly/monthly to pay-per-use. This billing mode change (from yearly/monthly to pay-per-use) takes effect immediately. For details, see **Changing Yearly/Monthly to Pay-per-Use**.

  NOTE

  - You have passed real-name authentication.
  - You can change the billing mode from yearly/monthly to pay-per-use only for ECSs whose status is **Provisioned** on the **Renewals** page.
  - The billing modes of products in a solution portfolio cannot be changed from yearly/monthly to pay-per-use.

6.4 FAQs About ECS Frozen, Deletion, and Unsubscription

Why Are My ECSs Released?

After you purchase ECSs but you do not complete the payment or renewal, the purchased ECSs will enter a grace period. If you still do not complete the payment or renewal after the grace period is ended, your ECS will enter a retention period. The ECS cannot provide services during the retention period. If you still do not complete the payment or renewal after the retention period is ended, your data stored in the ECS will be deleted and the ECS will be released. For details, see **Resource Suspension and Release**.

Can I Back Up My Data on the ECS When It Is Frozen?

No. If your ECS is frozen due to arrears, you can back up data only after you top up your account.

How Do I Unfreeze a Frozen ECS?

- Frozen due to arrears: You can renew or top up your account to unfreeze your ECS. You can renew or delete the ECSs that are frozen due to arrears. Only yearly/monthly ECSs that have not expired can be unsubscribed.
- Frozen due to violation detected by Huawei Cloud: You can renew or delete such ECSs. Only yearly/monthly ECSs that have not expired can be unsubscribed.
- Frozen due to violation detected by the public security department: You can renew such ECSs, but cannot delete them. Such frozen ECSs cannot be unsubscribed although they are displayed on the unsubscription page.

What Is the Impact on Services When Resources Are Frozen, Unfrozen, or Released?

- When resources are frozen, resource access and usage are restricted, which will interrupt your services. For example, if a server is frozen, it will be automatically stopped.
- When resources are unfrozen, constraints on resources are removed, but you need to check and restore your services. For example, after a yearly/monthly ECS is unfrozen, it will be automatically started. After a pay-per-use ECS is unfrozen, you need to start it manually.
- When resources are released, data stored on the resources will be deleted and cannot be retrieved.

How Do I Renew an ECS?

After an ECS billed on a yearly/monthly basis expires, renew it on the **Renewals** page of the management console. For details, see **Renewal Management**.

How Do I Restore an Unsubscribed or Deleted ECS?

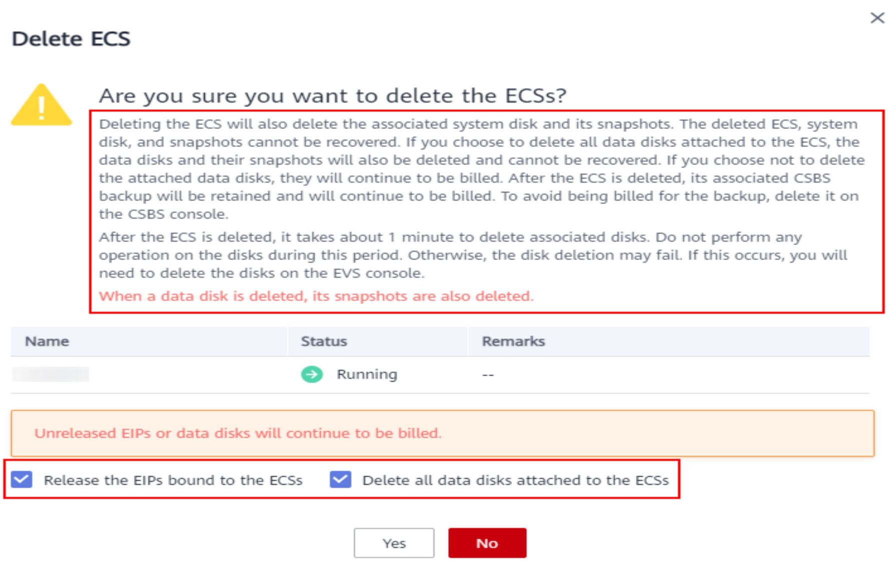
After an unsubscription is complete, the ECS will be permanently deleted and cannot be restored. You are advised to purchase a new ECS if you still want to use ECSs.

How Do I Delete an ECS?

- Pay-per-use ECS: On the ECS list page, select the target ECS, click **More** in the **Operation** column, and choose **Delete**.
  - Read details about deleting ECSs carefully.

   - Choose to delete the unneeded EIP and attached data disks together with the ECS to avoid generating costs.

Figure 6-2 Deleting pay-per-use ECSs



Delete ECS

Are you sure you want to delete the ECSs?

Deleting the ECS will also delete the associated system disk and its snapshots. The deleted ECS, system disk, and snapshots cannot be recovered. If you choose to delete all data disks attached to the ECS, the data disks and their snapshots will also be deleted and cannot be recovered. If you choose not to delete the attached data disks, they will continue to be billed. After the ECS is deleted, its associated CSBS backup will be retained and will continue to be billed. To avoid being billed for the backup, delete it on the CSBS console.

After the ECS is deleted, it takes about 1 minute to delete associated disks. Do not perform any operation on the disks during this period. Otherwise, the disk deletion may fail. If this occurs, you will need to delete the disks on the EVS console.

When a data disk is deleted, its snapshots are also deleted.

Name	Status	Remarks
[redacted]	Running	--

Unreleased EIPs or data disks will continue to be billed.

☑ Release the EIPs bound to the ECSs ☑ Delete all data disks attached to the ECSs

- Yearly/Monthly ECS: On the ECS list page, select the target ECS, click **More** in the **Operation** column, and choose **Unsubscribe**.

  For details about unsubscription rules and procedure, see **How Do I Unsubscribe from ECSs?**

How Do I Restore a Released ECS or EVS Disk?

Data cannot be restored if an ECS or EVS disk was not backed up before it is released.

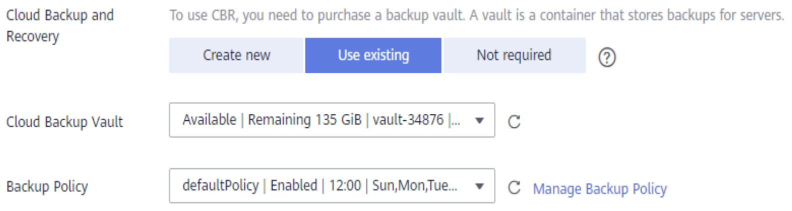
For details about how to back up an ECS and restore data using a backup, see **Backing Up ECS Data**.

How Do I Configure CBR and HSS for My ECS?

You can choose to purchase CBR and HSS together with your ECSs during the purchase process. They are not configured by default.

You can view the backup policy on the CBR console and associate the policy with your ECS. HSS takes effect only after the agent is installed on an ECS.

Figure 6-3 Cloud Backup and Recovery

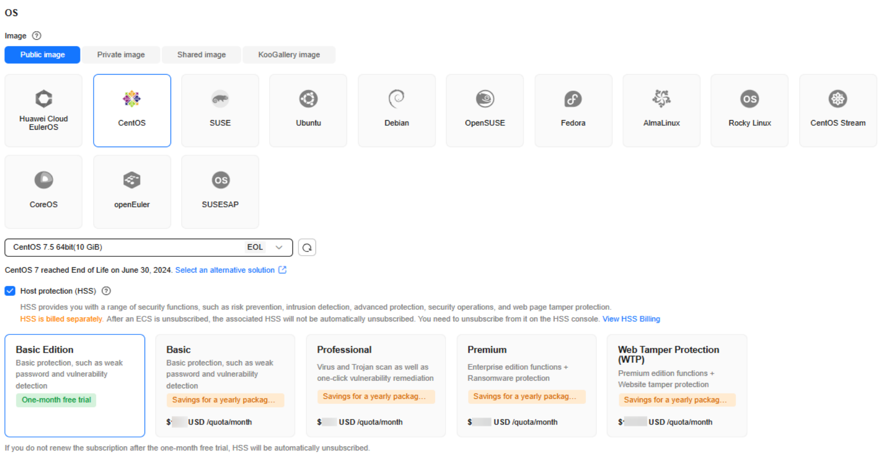


Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.

Cloud Backup Vault: Available | Remaining 135 GiB | vault-34876 |...

Backup Policy: defaultPolicy | Enabled | 12:00 | Sun,Mon,Tue...

Figure 6-4 Enabling HSS



CentOS 7.5 64bit(10 GiB)

CentOS 7 reached End of Life on June 30, 2024. Select an alternative solution

☑ Host protection (HSS)

HSS provides you with a range of security functions, such as risk prevention, intrusion detection, advanced protection, security operations, and web page tamper protection.

HSS is billed separately. After an ECS is unsubscribed, the associated HSS will not be automatically unsubscribed. You need to unsubscribe from it on the HSS console. View HSS Billing

Basic Edition	Basic	Professional	Premium	Web Tamper Protection (WTP)
Basic protection, such as weak password and vulnerability detection	Basic protection, such as weak password and vulnerability detection	Virus and Trojan scan as well as one-click vulnerability remediation	Enterprise edition functions + Ransomware protection	Premium edition functions + Website tamper protection
One-month free trial	Savings for a yearly packag...	Savings for a yearly packag...	Savings for a yearly packag...	Savings for a yearly packag...
	$[redacted] USD /quota/month	$[redacted] USD /quota/month	$[redacted] USD /quota/month	$[redacted] USD /quota/month

If you do not renew the subscription after the one-month free trial, HSS will be automatically unsubscribed.

6.5 How Can I Stop an ECS from Being Billed?

- After a pay-per-use or spot ECS is stopped (excluding bare metal ECSs or ECSs with local disks or FPGAs attached), its basic resources (vCPUs, memory, image, and GPUs) will no longer be billed, but its associated resources such as EVS disks (system and data disks), EIPs, and bandwidth will continue to be billed separately.

  To stop the ECS from being billed, delete it and its associated resources.
- Spot block ECSs, pay-per-use or spot ECSs with local disks attached (such as disk-intensive, ultra-high I/O, H2, P1, and P2 ECSs), pay-per-use or spot FPGA-based ECSs (such as Fp1 and Fp1c ECSs), and pay-per-use or spot bare metal ECSs will continue to be billed after they are stopped. To prevent such ECSs from being billed, delete them and their associated resources.
- For yearly/monthly resources such as yearly/monthly ECSs or EVS disks, your pay for them when you are purchasing them. The billing automatically stops when the subscription expires. If you stop using the resource before the subscription expires, you will not be eligible for a refund.

This section uses a pay-per-use ECS as an example to describe how you are billed after the ECS is deleted. **Table 6-2** lists the resources associated with the ECS.

Table 6-2 Billing example of a pay-per-use ECS

Resources	Description	Billing Mode
ECS basic resources	vCPUs, memory, image, and GPUs	Pay-per-use
EVS disks	System disk	Pay-per-use
	Data disk	Pay-per-use
EIP	N/A	Pay-per-use

After the ECS is deleted, it is billed as follows:

- ECS basic resources: no longer billed
- EVS disks
  - System disk: no longer billed
  - Data disks: no longer billed if you have selected **Delete the data disks attached to the following ECSs** when you were deleting the ECS. Otherwise, the data disks will continue to be billed.
- EIP: If you select **Release the EIPs bound to the ECSs** when deleting the ECS, the EIP will no longer be billed. Otherwise, the EIP will continue to be billed.

6.6 FAQs About Spot ECSs

About Spot ECSs

1. Why is my spot ECS released even when I have sufficient account balance?

   A spot ECS may be released at any time based on the changes in market price or supply and demand. For example, if the market price at a certain time is higher than the maximum price you are willing to pay, or if there are a large number of demands that the ECS resource supply cannot meet, the system automatically reclaims your spot ECS.
2. Can I change a spot ECS to a pay-per-use or yearly/monthly ECS?

   No.
3. Which resources are included in the price discount of a spot ECS?

   The price discount applies only to the vCPUs and memory of a spot ECS. The prices of other resources, such as the system disk, data disk, and bandwidth, are the same as those of ECSs billed on a pay-per-use basis.
4. How can I bid for a spot ECS?

   When you purchase a spot ECS, you are required to set the maximum price you are willing to pay. If the maximum price is higher than the market price and inventory resources are sufficient, you can purchase your spot ECS. The spot ECS is billed depending on the market price.
5. What is the relationship between the maximum price I am willing to pay for a spot ECS and the market price?

   Your spot ECS will run only if the maximum price you are willing to pay is higher than the market price. If the maximum price is lower than the market price, purchasing the spot will ECS fail, or the spot ECS that you have already purchased will be reclaimed. A spot ECS is billed based on market price, regardless of the maximum price you set.
6. If I have multiple spot ECSs and all the ECSs start to run at the same time, will the billing be the same for all of them?

   The billing will be the same for spot ECSs of the same series with the same specifications.
7. Can I obtain the market price before purchasing the spot ECS?

   Yes. When you purchase a spot ECS on the management console, you can view the market price range and historical prices of the ECS after you select an ECS flavor.
8. How is a spot ECS billed?

Spot ECSs are billed by the second, and the billing period is 1 hour.

9. When does the billing duration for a spot ECS start and end?

   The duration starts from the time when the spot ECS is purchased to the time when it is released either manually or automatically.

10. Will a stopped spot ECS continue to be billed?

    For details, see **Table 6-3**.

Table 6-3 Billing of stopped spot ECSs

Item	Spot Pricing
Spot ECSs without local disks or FPGAs attached, or non-bare metal ECSs	After the ECS is stopped, basic resources including vCPUs, memory, image, and GPUs are no longer billed. The resources associated with the ECS, such as EVS disks (including system and data disks), EIPs, and bandwidth, are separately billed.
Spot ECSs with local disks attached, FPGA-based ECSs, or bare metal ECSs	The ECS will continue to be billed after it is stopped. To stop the ECS from being billed, delete it and its associated resources.

6.7 How Can I Renew ECSs?

Yearly/monthly ECSs are unavailable after the subscription expires. If you want to continue using them, you need to renew the ECS subscription within a specified period. Otherwise, resources, such as vCPUs, memory, and EVS disks, will be automatically released, and data will be lost and cannot be restored.

On the ECS console, locate the ECS you want to renew and choose **More** > **Renew** in the **Operation** column. You can renew the subscription manually or automatically.

For details, see **Overview**.

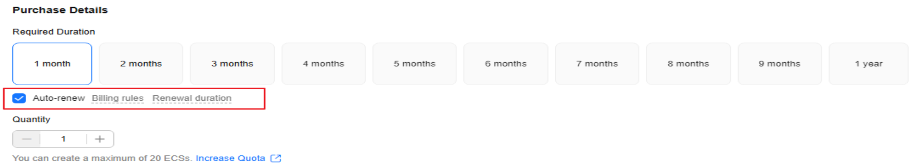
6.8 How Can I Automatically Renew a Yearly/Monthly ECS?

Solution

1. Select **Auto renew** when purchasing a yearly/monthly ECS.

   On the **Buy ECS** page, select **Auto renew** under **Required Duration**.

Figure 6-5 Auto renew



☑ Auto-renew

Quantity 1

You can create a maximum of 20 ECSs.

2. Select the EIP bound to the target ECS for automatic renewal.

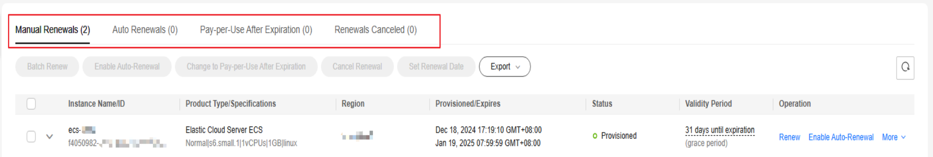
   Auto renew is provided for the ECSs and EVS disks when you purchase them. To enable automatic renewal for EIPs, perform the following operations:

   a. Log in to the management console and click **Billing** > **Renewal** in the upper right corner.

      The **Renewals** page is displayed.

   b. Select the EIP for automatic renewal.

Figure 6-6 Enable Auto-Renew



☐	Instance Name/ID	Product Type/Specifications	Region	Provisioned/Expires	Status	Validity Period	Operation
☐	ecs-[redacted] f4050982-[redacted]	Elastic Cloud Server ECS Normal|s6.small.1|1vCPUs|1GB|linux	[redacted]	Dec 18, 2024 17:19:10 GMT+08:00 Jan 19, 2025 07:59:59 GMT+08:00	○ Provisioned	31 days until expiration (grace period)	Renew Enable Auto-Renewal More

6.9 Will I Receive a Notification If My Account Balance Is Insufficient?

You can set the balance alert function in the Billing Center. The system checks your account balance and sends a notification if your balance is less than or equal to your set threshold. Set the alert threshold based on your resource usage.

1. Log in to the management console and click **Billing** in the upper right corner.

   The **Overview** page of the Billing Center is displayed.

2. In the **Available Credit** area on the **Overview** page, toggle on or off **Balance Alert** to enable or disable the balance alert function.
3. In the displayed **Enable Balance Alerts** dialog box, set **Threshold**.
4. Click **OK** to complete the setting of the balance alert function.

   After the setting, you can click **Modify** next to **Alert Threshold** to modify the alert threshold.

5. With balance alert enabled, when the sum of your account balance, cash coupons, and flexi-purchase coupons goes below the threshold, the recipients will receive a notification for 1-3 days by SMS and email.

   You can modify the recipients that receive the balance alerts at **SMS & Email Settings** > **Finance** > **Account balance** in the Message Center.

   After receiving a balance alert, top up your account or disable unnecessary resources in a timely manner to avoid affecting the normal use of cloud resources or to stop unnecessary fees from being generated.

6.10 Will I Receive a Notification of Account Balance Changes?

Yes. You will receive a notification of account balance changes via emails or SMS messages, such as account top-ups or balance adjustment.

For details about the notification scenarios and types, see **Message Receiving and Management**.

You can manage message receiving. For details, see **How Do I Manage Message Receiving?**

7 Region and AZ

7.1 What Is AZ and How Can I Select and View an AZ?

What Is an AZ?

An availability zone (AZ) is a physical region where resources use independent power supplies and networks. AZs are physically isolated but interconnected through an internal network.

There are multiple AZs in each region. If one AZ becomes faulty, other AZs in the same region continue to provide services.

AZs in the same region can communicate with each other through an internal network.

How Do I Select an AZ

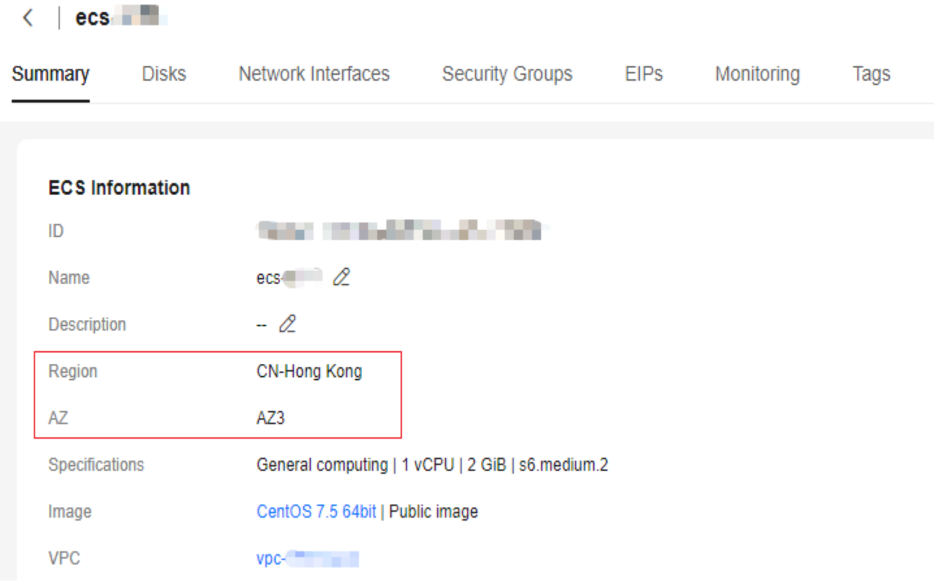
You can select an AZ when you are purchasing an ECS. After the ECS is created, the AZ cannot be changed. If there is only one AZ displayed in a region, it means the region only provides one AZ.

How Do I View the AZ of an ECS?

After purchasing an ECS, you can view the AZ which the ECS belongs to on the ECS details page.

1. Go to the **ECS console**.
2. In the ECS list, click the name of the target ECS to go to the details page.
3. On the **Summary** tab, view the AZ which the ECS belongs to.

Figure 7-1 Viewing the AZ of an ECS



ecs[redacted]

ECS Information

ID [redacted]

Name ecs[redacted]

Description --

Region CN-Hong Kong

AZ AZ3

Specifications General computing | 1 vCPU | 2 GiB | s6.medium.2

Image CentOS 7.5 64bit | Public image

VPC vpc-[redacted]

7.2 What Is a Region?

Regions are geographic areas isolated from each other. ECSs are region-specific and cannot be used across regions through internal network connections.

When you buy an ECS, select the nearest region for low network latency and quick resource access.

7.3 Are Products Different in Different Regions?

Yes. Currently, each region contains different products. Certain products are available for trial release in certain regions only.

7.4 Is Data Transmission Between AZs Billed?

Data transmission between AZs in the same region is free of charge. However, data transmission between AZs in different regions will be billed.

7.5 Can I Change the Region or AZ After an ECS Is Purchased?

Sorry, you cannot change the region after the ECS is purchased. During the ECS purchase, you are advised to select the region nearest to your services for lower network latency and quick resource access.

If you need to change the region or AZ for a purchased ECS, you can use Image Management Service (IMS) to migrate the ECS data across regions or AZs.

Example 1:

ecs01 in a region needs to be migrated to another region.

1. In the original region, create a full-ECS image image01 for ecs01.
2. Replicate image01 from the original region to the target region and name the new image image01-copy.
3. In the target region, use image01-copy to create an ECS named ecs02.

   In this way, data on ecs01 is migrated from the original region to ecs02 in the target region.

Example 2:

In a region, ecs01 in an AZ needs to be migrated to another AZ.

1. In the original AZ, create full-ECS image image01 from ecs01.
2. In the target AZ, use image image01 to create an ECS named ecs02.

   In this way, data on ECS ecs01 is migrated from the original AZ to the target AZ.

For more migration methods and background information, see **Can I Migrate an ECS to Another Region, AZ, or Account?**

7.6 Can I Migrate an ECS to Another Region, AZ, or Account?

After an ECS is created, it cannot be directly migrated to another region, AZ, or account.

To migrate an ECS across accounts or regions, create an image using the ECS and migrate the image to the target accounts or regions.

For details about common server migration scenarios and methods, see **Common Server Migration Scenarios**.

For details about how to migrate an ECS across accounts or regions, see **Migrating ECSs Across Accounts and Regions Through Image Replication**.

Common Server Migration Scenarios

Common server migration scenarios include migration from physical servers to cloud servers, from virtualization platforms (such as VMware) to Huawei Cloud, between cloud servers on Huawei Cloud (across accounts, regions, or AZs), from cloud servers on a third-party cloud platform to cloud servers on Huawei Cloud, and installation disk imaging. For details about the recommended migration methods, see **Table 7-1**.

Table 7-1 Common server migration scenarios

Scenario	Condition	Recommended Solution	Remarks
From x86 physical servers to Huawei Cloud servers For example, P2V	The servers can access the Internet.	Server Migration Service For details, see **Best Practices - Server Migration Service**.	N/A
From VMs (such as VMware) on a virtualization platform to Huawei Cloud servers	The VMs can access the Internet.	Server Migration Service For details, see **Best Practices - Server Migration Service**.	N/A
	The VMs cannot access the Internet.	1. Export the VM image files from the VMware virtualization platform. 2. **Import the image files to Huawei Cloud.**	If the image file format is not vhd, vmdk, qcow2, raw, vhdx, qcow, vdi, qed, zvhd, or zvhd2, convert the file format.
Between cloud servers on Huawei Cloud (across accounts, regions, or AZs) For example, migrating the cloud servers of account A in the CN North-Beijing4 region to account B in the CN East-Shanghai1 region	The cloud servers can access the Internet.	Server Migration Service For details, see **Best Practices - Server Migration Service**.	N/A

Scenario	Condition	Recommended Solution	Remarks
	The cloud servers cannot access the Internet.	**Recommended** - Migration across accounts: **Sharing Images**. Use the source cloud server's system disk to create a system disk image and the data disk to create a data disk image, or use the source cloud server to create a full-server image. Then, share the images with other accounts. - Migration across regions: **Replicating images across regions.** Use the source cloud server's system disk to create a system disk image and the data disk to create a data disk image, or use the source cloud server to create a full-server image. Then, replicate the images to other regions. - Migration across accounts and regions: **Sharing Images** and **Replicating**	Only the full-server images created using CBR can be shared. The size of images to be replicated across regions cannot be greater than 128 GiB.

Scenario	Condition	Recommended Solution	Remarks
		Images Across Regions. - Migration across AZs: **Creating an ECS from an Image**. Use the source cloud server's system disk to create a system disk image and the data disk to create a data disk image, or use the source cloud server to create a full-server image. Then, use the **Apply for Server** function of the image to create a cloud server in the target AZ.	
From a third-party cloud platform to Huawei Cloud For example, from Alibaba Cloud or Tencent Cloud to Huawei Cloud	The cloud servers can access the Internet.	Server Migration Service For details, see **Best Practices - Server Migration Service**.	N/A
	The cloud servers cannot access the Internet.	1. Export the image from the source cloud platform. 2. **Import the image files to Huawei Cloud.**	If the image file format is not vhd, vmdk, qcow2, raw, vhdx, qcow, vdi, qed, zvhd, or zvhd2, convert the file format.

Scenario	Condition	Recommended Solution	Remarks
Installation disk imaging For example, create an image file offline and import it to Huawei Cloud.	The ISO installation disk image of the required OS is available.	**Create a Windows image using VirtualBox and upload the image to Huawei Cloud.** Or **Create an image using an ISO file imported to Huawei Cloud.**	N/A

7.7 Can a Load Balancer Distribute Traffic to ECSs in Different Regions?

Only dedicated load balancers support this. Backend servers can be from VPCs in different regions.

For details, see **Creating a Dedicated Load Balancer**.

7.8 Is Application Disaster Recovery Available in Different Regions?

Yes.

You can deploy active and standby application nodes in different regions. If the active application node is faulty, the standby application node continues to provide services.

7.9 Are There Any Services Provided for Application Disaster Recovery?

No. Currently, the standard application disaster recovery service is unavailable now. If you have such a requirement, please contact us. We will customize an application disaster recovery solution based on your application scenarios.

7.10 Can Components Contained in an Application Be Distributed to Different Regions?

Yes. However, such a deployment mode is not recommended.

You are advised to deploy the components contained in an application in the same region. In this manner, these components can communicate with each other over an internal network, reducing bandwidth costs of using public networks and ensuring communication quality between the components.

8 OS

8.1 How Do I Use BYOL?

What Is BYOL?

Bring your own license (BYOL) allows you to use your existing OS license. In such a case, you do not need to apply for a license again.

How Do I Use BYOL?

If you select the BYOL license type, you are required to manage licenses by yourself. If you have obtained an OS license, you do not need to apply for a license.

For details, see **License Types**.

8.2 Do ECSs Support GUI?

Windows ECSs are managed through a GUI but Linux ECSs are managed through the CLI. You can configure a GUI if required.

Before installing a GUI on an ECS, ensure that the idle memory is greater than or equal to 2 GiB. Otherwise, the GUI installation may fail or the ECS cannot be started after the installation.

For details about how to install a Linux OS on the GUI, see the following:

- **How Can I Install a GUI on an ECS Running CentOS 6?**
- **How Can I Install a GUI on an ECS Running CentOS 7?**
- **How Can I Install a GUI on an ECS Running Ubuntu?**
- **How Can I Install a GUI on an ECS Running Debian?**

8.3 How Can I Install a GUI on an ECS Running CentOS 6?

Scenarios

To provide a pure system, the ECSs running CentOS 6 do not have a GUI installed by default. You can install a GUI on such ECSs as needed.

Constraints

- Before installing a GUI on an ECS, ensure that the idle memory is greater than or equal to 2 GB. Otherwise, the GUI installation may fail or the ECS cannot be started after the installation.

Procedure

1. Run the following command to obtain the installation component provided by the OS:

   ```
   yum groupinstall "Desktop"
   ```

2. Run the following command to set the default startup level to **5** (GUI):

   ```
   sed -i 's/id:3:initdefault:/id:5:initdefault:/' /etc/inittab
   ```

3. Run the following command:

   ```
   startx
   ```

8.4 How Can I Install a GUI on an ECS Running CentOS 7?

Scenarios

You want to install a GUI on an ECS running CentOS 7 series.

Constraints

- Before installing a GUI on an ECS, ensure that the idle memory is greater than or equal to 2 GB. Otherwise, the GUI installation may fail or the ECS cannot be started after the installation.

Procedure

1. Run the following command to install the GUI desktop component:

   ```
   yum groupinstall "Server with GUI"
   ```

NOTE

If the following message is displayed after the installation is complete:

Failed : python -urllibs3.noarch 0:1.10.2-7.e17

Run the following command:

```
mv /usr/lib/python2.7/site-packages/urllib3/packages/ssl_match_hostname /usr/lib/python2.7/site-packages/urllib3/packages/ssl_match_hostname.bak
```

```
yum install python-urllib3 -y
```

2. After the installation is complete, run the following command to set the default startup level to **graphical.target**:

   ```
   systemctl set-default graphical.target
   ```

3. Run the following command to start **graphical.target**:

   ```
   systemctl start graphical.target
   ```

4. Restart the ECS.
5. Log in to the ECS using VNC provided on the management console. Set the language, time zone, username, and password as prompted.

8.5 How Can I Install a GUI on an ECS Running Ubuntu?

Scenarios

To provide a pure system, the ECSs running Ubuntu do not have a GUI installed by default. You can install a GUI on such ECSs as needed.

For GPU-accelerated ECSs, after installing a GUI, you need to configure X Server, x11vnc, and lightdm to make sure that:

- The graphics system and VNC server are automatically started upon the ECS startup.
- Applications can invoke GPUs properly after a remote login using VNC.

You can perform the following steps to install a GUI on an Ubuntu ECS:

- **Installing a GUI**
- **(Optional) Configuring X Server, x11vnc, and lightdm**: required only for GPU-accelerated ECSs.
- **(Optional) Verifying Drivers on GPU-accelerated ECSs**: required only for GPU-accelerated ECSs.

Constraints

- This section applies to ECSs running Ubuntu 16.04, 18.04, 20.04, 22.04, and 24.04.
- The Ubuntu ECS must have an EIP bound or have an intranet image source configured.
- Before installing a GUI on an ECS, ensure that the idle memory is greater than or equal to 2 GB. Otherwise, the GUI installation may fail or the ECS cannot be started after the installation.

- GPU-accelerated ECSs must have a correct GPU driver installed. For details, see **GPU Driver**.

Installing a GUI

1. Log in to the ECS and install a GUI desktop environment.
   a. Run the following command to update the software library:

      apt-get update

   b. Run the following command to install the Ubuntu GUI desktop component:
      - For Ubuntu 16.04, run the following command:

        apt-get install -y scite xorg xubuntu-desktop

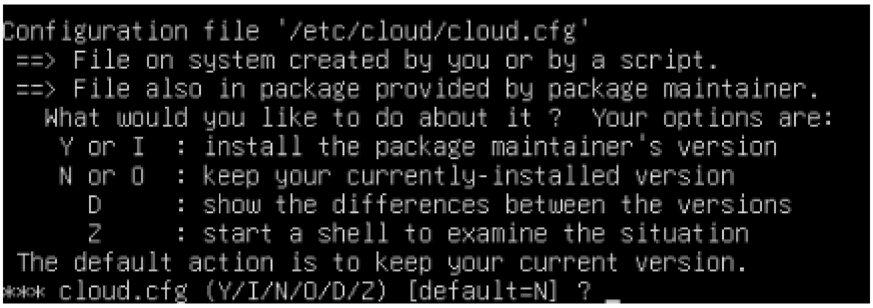
      - For Ubuntu 18.04 and later versions, run the following command:

        apt-get install -y ubuntu-desktop

2. Set the configuration file version (mandatory for Ubuntu 24.04).

   In Ubuntu 24.04, after the installation command is executed, you need to set the configuration file as prompted or press **Enter** to use the default value.

   Figure 8-1 Example configuration file



```
Configuration file '/etc/cloud/cloud.cfg'
 ==> File on system created by you or by a script.
 ==> File also in package provided by package maintainer.
   What would you like to do about it ?  Your options are:
    Y or I  : install the package maintainer's version
    N or O  : keep your currently-installed version
      D     : show the differences between the versions
      Z     : start a shell to examine the situation
 The default action is to keep your current version.
*** cloud.cfg (Y/I/N/O/D/Z) [default=N] ? _
```

3. Run the following command to edit the **/root/.profile** file:

   vim /root/.profile

   Press **i** to enter the editing mode and change **mesg n || true** in the last line to **tty -s && mesg n || true**. After the modification, the file content is as follows:

```
# ~/.profile: executed by Bourne-compatible login shells.

if [ "$BASH" ]; then
  if [ -f ~/.bashrc ]; then
    . ~/.bashrc
  fi
fi
tty -s && mesg n || true
```

4. Press **Esc** to exit editing mode.
5. Run the following command to save and exit the configuration file:

   :wq

6. Add a member account (mandatory for Ubuntu 20.04).

   After the GUI desktop component is installed on the ECS, you cannot log in to the Ubuntu 20.04 OS as user **root**. You need to add a member account for logging in to the GUI desktop.

   Run the following command to add user **user01**:

adduser user01

Set a password for **user01** as prompted.

```
Adding user `user01' ...
Adding new group `user01' (1001) ...
Adding new user `user01' (1001) with group `user01' ...
Creating home directory `/home/user01' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
```

Set information about **user01**. You can press **Enter** to skip the setting. Then the system prompts you to check whether the entered information is correct.

Enter **Y**.

```
Changing the user information for user01
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

7. Run the reboot command to restart the ECS.
8. Log in to the ECS using VNC provided on the management console and log in to the GUI desktop using the member account created in step **6** or the **root** account.
    - For Ubuntu 20.04 OS, you need to use the member account to log in to the GUI desktop.
    - For GPU-accelerated ECSs, you also need to **configure X Server, x11vnc, and lightdm**.

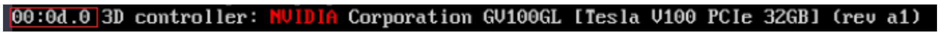
(Optional) Configuring X Server, x11vnc, and lightdm

For GPU-accelerated ECSs, you need to configure X Server, x11vnc, and lightdm when installing a GUI.

1. Remotely log in to the ECS.
2. Query the BusID of the GPU.

    lspci | grep -i nvidia

    Figure 8-2 GPU's BusID

    ```
    00:0d.0 3D controller: NVIDIA Corporation GV100GL [Tesla V100 PCIe 32GB] (rev a1)
    ```

3. Generate the X Server configuration.

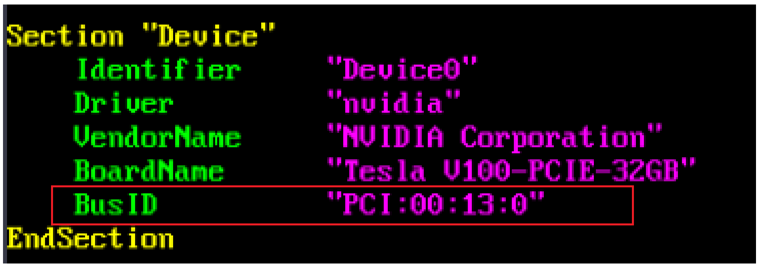
    nvidia-xconfig --enable-all-gpus --separate-x-screens

4. Configure the GPU's BusID in "Section Device" in the generated **/etc/X11/xorg.conf**.
    a. Edit **/etc/X11/xorg.conf**.

       vi /etc/X11/xorg.conf

    b. Press **i** to enter editing mode.
    c. Add the GPU's BusID in "Section "Device".

Figure 8-3 Adding the GPU's BusID



```
Section "Device"
    Identifier      "Device0"
    Driver          "nvidia"
    VendorName      "NVIDIA Corporation"
    BoardName       "Tesla V100-PCIE-32GB"
    BusID           "PCI:00:13:0"
EndSection
```

NOTE

The BusID queried in step 2 is a hexadecimal number. You need to convert it to a decimal number before adding it to "Section Device" in **/etc/X11/xorg.conf**.

1. For example, the queried BusID is **00.0d.0** (a hexadecimal number) and needs to be converted to **PCI:00:13:0** (a decimal number).

   d. Press **Esc** to exit editing mode.

   e. Run the following command to save and exit the configuration file:

   :wq

5. Install x11vnc.

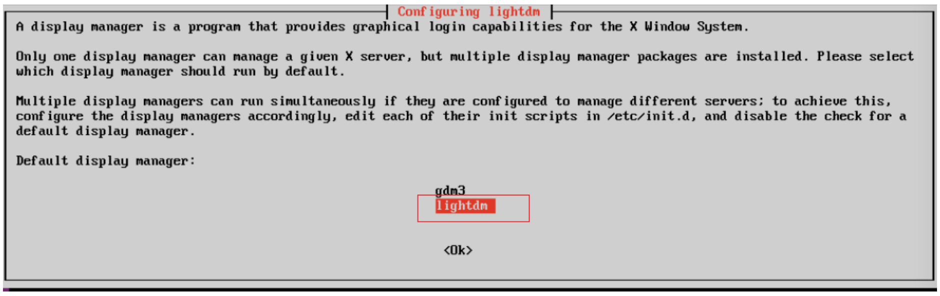
   apt-get -y install x11vnc

6. Install lightdm.

   apt-get -y install lightdm

7. Select **lightdm** as the default display manager.

Figure 8-4 Selecting a display manager



```
Configuring lightdm
A display manager is a program that provides graphical login capabilities for the X Window System.

Only one display manager can manage a given X server, but multiple display manager packages are installed. Please select
which display manager should run by default.

Multiple display managers can run simultaneously if they are configured to manage different servers; to achieve this,
configure the display managers accordingly, edit each of their init scripts in /etc/init.d, and disable the check for a
default display manager.

Default display manager:

                                        gdm3
                                        lightdm

                                         <Ok>
```

8. Configure the GUI desktop environment to automatically start upon ECS startup.

   systemctl set-default graphical.target

9. (Optional) Configure the x11vnc to automatically start upon ECS startup.

   a. Add the **/lib/systemd/system/myservice.service** file.

   vi /lib/systemd/system/myservice.service

   b. Press **i** to enter editing mode.

   c. Add the following content to the file:

```
[Unit]
Description=My Service
After=network.target lightdm.service

[Service]
Type=oneshot
```

```
ExecStart=/usr/bin/x11vnc -forever -loop -noxdamage -repeat -rfbport 5902 -shared -bg -auth
guess -o /var/log/vnc.log

[Install]
WantedBy=multi-user.target
Alias=myservice.service
```

   d. Press **Esc** to exit editing mode.
   e. Run the following command to save and exit the configuration file:

      :wq

10. Load configuration files.

    systemctl daemon-reload

    systemctl enable myservice.service

11. Run the reboot command to restart the ECS.

(Optional) Verifying Drivers on GPU-accelerated ECSs

After installing a GUI on a GPU-accelerated ECS, perform the following operations to check whether the driver is working properly:

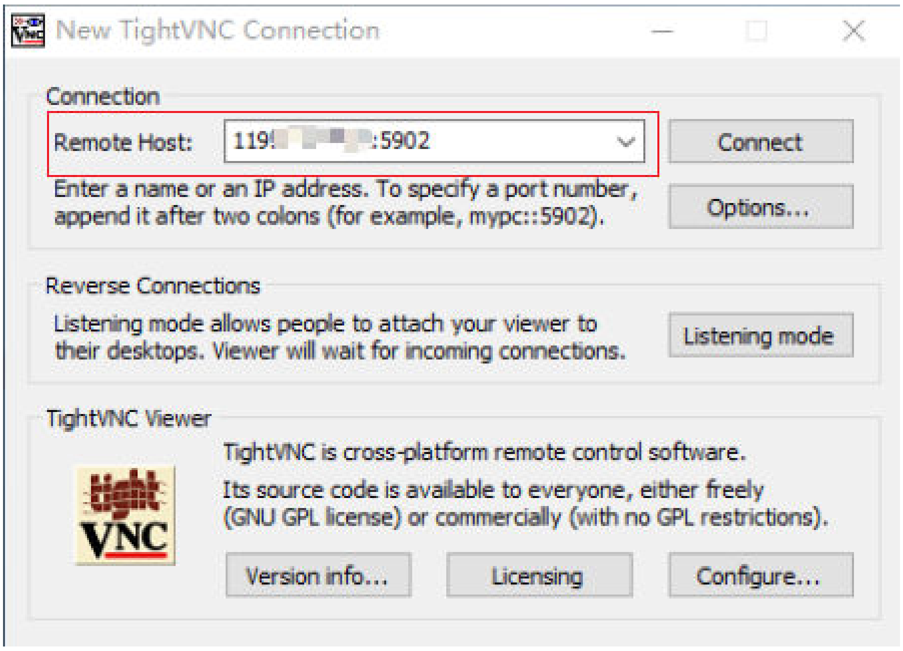
1. Log in to the **management console**.
2. Configure a security group for the ECS.
   a. On the ECS list, click the name of an ECS for which you want to configure the security group rule. On the ECS details page, click **Security Groups**.
   b. Expand the security group and in the upper right corner of the security group rule list, click **Modify Security Group Rule**.
   c. On the **Inbound Rules** page, click **Add Rule**.
   d. In the **Add Inbound Rule** dialog box, follow the prompts to add the following security group rule:

      Allow inbound access through TCP port *5902*. The port number is determined by the **rfbport** parameter in step **9.c**.

3. Log in to the ECS using VNC.

   The following uses TightVNC as an example.

Figure 8-5 TightVNC client



Remote Host: 119[redacted]:5902

Enter a name or an IP address. To specify a port number, append it after two colons (for example, mypc::5902).

Listening mode allows people to attach your viewer to their desktops. Viewer will wait for incoming connections.

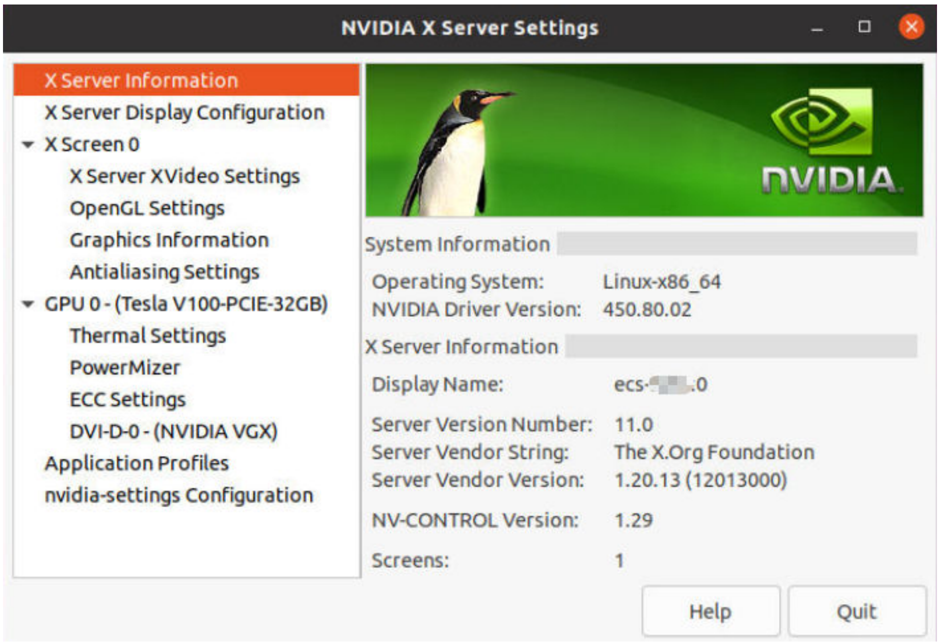
TightVNC is cross-platform remote control software.

Its source code is available to everyone, either freely (GNU GPL license) or commercially (with no GPL restrictions).

4. Right-click on the blank area and choose **Open in Terminal** from the shortcut menu.
5. Run the following command on the terminal. If the graphics card information is displayed as follows, the driver is working properly.

   nvidia-settings

Figure 8-6 Graphics card information



Operating System: Linux-x86_64
NVIDIA Driver Version: 450.80.02

Display Name: ecs-[redacted].0
Server Version Number: 11.0
Server Vendor String: The X.Org Foundation
Server Vendor Version: 1.20.13 (12013000)
NV-CONTROL Version: 1.29
Screens: 1

NOTE

If a GPU-accelerated ECS has a GRID driver installed, you need to configure a license to use the GPU rendering capability. For details, see **Manually Installing a GRID Driver on a GPU-accelerated ECS**.

8.6 How Can I Install a GUI on an ECS Running Debian?

Scenarios

To provide a pure system, the ECSs running Debian do not have a GUI installed by default. You can install a GUI on such ECSs as needed.

Constraints

- The operations described in this section apply to ECSs running Debian 8, Debian 9, or Debian 10 only.
- Before installing a GUI on an ECS, ensure that the idle memory is greater than or equal to 2 GB. Otherwise, the GUI installation may fail or the ECS cannot be started after the installation.

Procedure

1. Log in to the ECS and run the following command to update the software library:

   apt update

2. Run the following command to upgrade the software library:

   apt upgrade

3. Run the following command to install tasksel:

   apt install tasksel

4. Run the following command to use tasksel to install the GNOME GUI:

   tasksel install desktop gnome-desktop

   The installation takes a long time. Please wait.

5. Run the following command to set the GUI as the default startup target:

   systemctl set-default graphical.target

6. Create a member account.

   After the GUI desktop component is installed on the ECS, you cannot log in to the Debian OS as user root **user**. Therefore, you need to add a member account for logging in to the GUI desktop.

   Run the following command to add user **user01**:

   adduser user01

   Set a password for **user01** as prompted.

   ```
   Adding user `user01' ...
   Adding new group `user01' (1001) ...
   Adding new user `user01' (1001) with group `user01' ...
   Creating home directory `/home/user01' ...
   Copying files from `/etc/skel' ...
   New password:
   ```

```
Retype new password:
passwd: password updated successfully
```

Set information about **user01**. You can press **Enter** to skip the setting. Then the system prompts you to check whether the entered information is correct.

Enter **Y**.

```
Changing the user information for user01
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

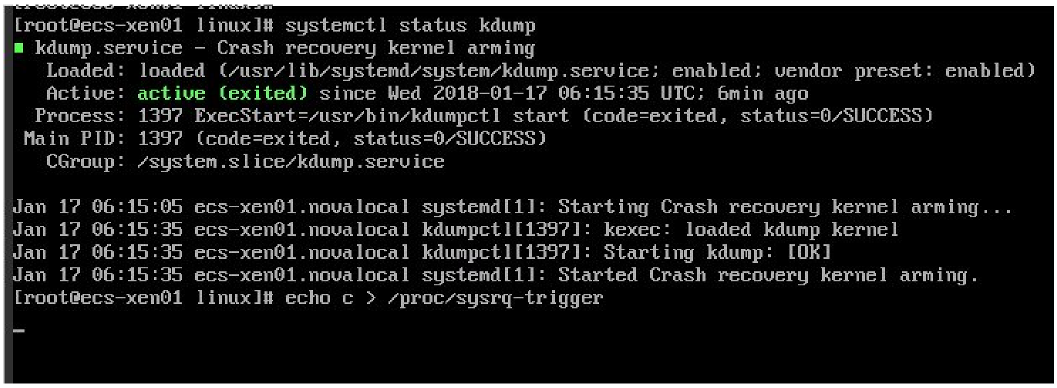
7. Run the reboot command to restart the ECS.
8. Log in to the ECS using VNC provided on the management console and log in to the GUI desktop using the member account added in 6.

8.7 Why Does the OS Fail to Respond When kdump Occurs on a Linux ECS?

Symptom

When kdump occurs on a Xen Linux ECS, the OS fails to respond and cannot be automatically recovered. For example, if you run the **echo c>/proc/sysrq-trigger** command to trigger kdump, this fault occurs.

Figure 8-7 Triggering kdump



```
[root@ecs-xen01 linux]# systemctl status kdump
■ kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset: enabled)
   Active: active (exited) since Wed 2018-01-17 06:15:35 UTC; 6min ago
  Process: 1397 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
 Main PID: 1397 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/kdump.service

Jan 17 06:15:05 ecs-xen01.novalocal systemd[1]: Starting Crash recovery kernel arming...
Jan 17 06:15:35 ecs-xen01.novalocal kdumpctl[1397]: kexec: loaded kdump kernel
Jan 17 06:15:35 ecs-xen01.novalocal kdumpctl[1397]: Starting kdump: [OK]
Jan 17 06:15:35 ecs-xen01.novalocal systemd[1]: Started Crash recovery kernel arming.
[root@ecs-xen01 linux]# echo c > /proc/sysrq-trigger

_
```

NOTE

Generally, kdump is disabled for public images. This issue does not occur on the ECSs created using public images.

Possible Causes

- Certain Linux kernel versions are incompatible with Xen virtualization.
- If kdump is enabled in the ECS with the kernel not supporting soft_rest, the ECS stops responding during dump.

Solution

Method 1: Disable kdump.

CentOS 7.5 is used as an example in the following.

1. Forcibly restart the ECS.
   a. Log in to the **management console**.
   b. Choose **Compute** > **Elastic Cloud Server**.
   c. In the ECS list, select the target ECS and click **Restart**.
   d. Select **Forcibly restart the preceding ECSs** or **Forcibly stop the preceding ECSs**.
   e. Click **OK**.
2. Disable kdump.
   a. Log in to the forcibly restarted ECS as user **root**.
   b. Run the following command to disable kdump:

      service kdump stop

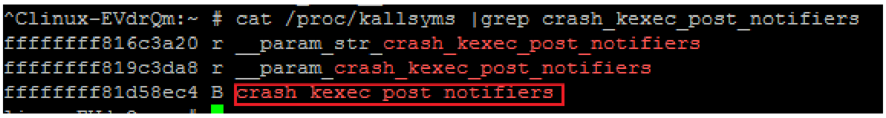
Solution 2:

If the target ECS supports the **crash_kexec_post_notifiers** function, add the function to the ECS startup configuration file (**menu.lst** or **grub.cfg**). To do so, perform the following operations:

1. Run the following command to check whether the ECS supports the **crash_kexec_post_notifiers** function:

   cat /proc/kallsyms |grep crash_kexec_post_notifiers

   Figure 8-8 Support for the **crash_kexec_post_notifiers** function

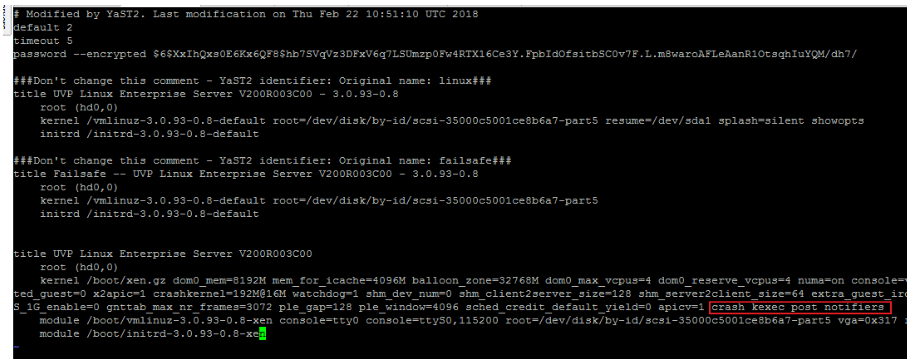
```
^Clinux-EVdrQm:~ # cat /proc/kallsyms |grep crash_kexec_post_notifiers
ffffffff816c3a20 r __param_str_crash_kexec_post_notifiers
ffffffff819c3da8 r __param_crash_kexec_post_notifiers
ffffffff81d58ec4 B crash_kexec_post_notifiers
```

   - If yes, go to step 2.
   - If no, use method 1.
2. Add the **crash_kexec_post_notifiers** function to the startup configuration file **menu.lst** or **grub.cfg**.

   Take **menu.lst** as an example.
   a. Run the following command to open the **menu.lst** file:

      vi /boot/grub/menu.lst
   b. Add the **crash_kexec_post_notifiers** function to the startup item.

Figure 8-9 Editing the **menu.lst** file



```
# Modified by YaST2. Last modification on Thu Feb 22 10:51:10 UTC 2018
default 2
timeout 5
password --encrypted $6$XxIhQxs0E6Kx6QF8$hb7SVqVz3DFxV6q7LSUmzp0Fw4RTX16Ce3Y.FpbIdOfsitbSC0v7F.L.m8waroAFLeAanR1OtsqhIuYQM/dh7/

###Don't change this comment - YaST2 identifier: Original name: linux###
title UVP Linux Enterprise Server V200R003C00 - 3.0.93-0.8
    root (hd0,0)
    kernel /vmlinuz-3.0.93-0.8-default root=/dev/disk/by-id/scsi-35000c5001ce8b6a7-part5 resume=/dev/sda1 splash=silent showopts
    initrd /initrd-3.0.93-0.8-default

###Don't change this comment - YaST2 identifier: Original name: failsafe###
title Failsafe -- UVP Linux Enterprise Server V200R003C00 - 3.0.93-0.8
    root (hd0,0)
    kernel /vmlinuz-3.0.93-0.8-default root=/dev/disk/by-id/scsi-35000c5001ce8b6a7-part5
    initrd /initrd-3.0.93-0.8-default


title UVP Linux Enterprise Server V200R003C00
    root (hd0,0)
    kernel /boot/xen.gz dom0_mem=8192M mem_for_icache=4096M balloon_zone=32768M dom0_max_vcpus=4 dom0_reserve_vcpus=4 numa=on console=
ted_guest=0 x2apic=1 crashkernel=192M@16M watchdog=1 shm_dev_num=0 shm_client2server_size=128 shm_server2client_size=64 extra_guest_ir
S_1G_enable=0 gnttab_max_nr_frames=3072 ple_gap=128 ple_window=4096 sched_credit_default_yield=0 apicv=1 crash kexec post notifiers
    module /boot/vmlinuz-3.0.93-0.8-xen console=tty0 console=ttyS0,115200 root=/dev/disk/by-id/scsi-35000c5001ce8b6a7-part5 vga=0x317
    module /boot/initrd-3.0.93-0.8-xen
~
```

c. Run the following command to restart the ECS for the modification to take effect:

reboot

8.8 How Can I Upgrade the Kernel of a Linux ECS?

Scenarios

If the kernel of a Linux ECS has stability or performance issues such as system breakdown, freezing, and memory leakage, or new kernel functions are required, you can upgrade the OS kernel.

Constraints

⚠ CAUTION

Upgrading the OS kernel may cause system instability or compatibility issues. Before the upgrade, you should know the problems that may occur during the upgrade, back up important data, and perform the upgrade with caution.

For details about how to back up the ECS, see **Backup Overview**.

- After the OS kernel is upgraded, the Linux ECS may not be able to identify the network interfaces. This will lead to network access failure.
- After the OS kernel is upgraded, the Linux ECS may not be able to identify data disks. As a result, starting system mount points fails, and the ECS cannot start.

Procedure

This section uses the Huawei Cloud EulerOS, CentOS, Ubuntu, and Debian as examples to describe how to update the OS kernel.

Upgrading the Kernel (Huawei Cloud EulerOS or CentOS)

1. Log in to the ECS.
2. Run the following command to query the OS kernel version:

uname -r

3. Run the following command to check whether there is any OS kernel that can be upgraded:

   sudo yum list kernel

   - If no OS kernel can be upgraded:

     You are advised to change the OS to Huawei Cloud EulerOS 2.0. For details, see **Changing the OS**.

     NOTE

     CentOS 6, CentOS 7, and CentOS 8 are no longer maintained and will not be supported by Huawei Cloud. For details, see **What Do I Do If CentOS Linux Is No Longer Maintained?**

   - If there is an OS kernel that can be upgraded:

     i. Run the following command to check whether the **initrd** or **initramfs** file contains the virtio-blk or xen-blkfront driver:

        sudo lsinitrd /boot/initramfs-`uname -r`.img | grep -E 'virtio|xen'

        If information similar to the following is displayed, the virtio-blk or xen-blkfront driver is contained. Otherwise, the driver is not included. Go to the next step.

```
-rwxr--r--   1 root     root       23888 Feb 10  2022 lib/modules/2.6.32-754.35.1.el6.x86_64/
kernel/drivers/block/virtio_blk.ko
-rwxr--r--   1 root     root       55064 Feb 10  2022 lib/modules/2.6.32-754.35.1.el6.x86_64/
kernel/drivers/block/xen-blkfront.ko
```

     ii. (Optional) Run the following command to add the virtio-blk or xen-blkfront driver to the **initrd** or **initramfs** file.

        Perform this step only when the **initrd** or **initramfs** file does not contain the virtio-blk or xen-blkfront driver.

        sudo sh -c 'echo 'add_drivers+="xen-blkfront virtio_blk"' >> /etc/dracut.conf.d/virt-drivers.conf'

4. Run the following command to upgrade the OS kernel version:

   sudo yum update -y

5. Run the following command to update the GRUB file so that the ECS can select the target kernel version during startup:

   sudo grub2-mkconfig -o /boot/grub2/grub.cfg

6. Run the following command to restart the ECS:

   sudo reboot

7. Run the following command to check whether the kernel version has been upgraded:

   uname -r

   If the new kernel version is returned, the kernel has been upgraded.

Upgrading the Kernel (Ubuntu or Debian)

1. Log in to the ECS.
2. Run the following command to query the OS kernel version:

   uname -r

3. Run the following commands to update the system software package list and check whether the OS kernel can be upgraded:

   sudo apt update

   apt-cache search linux-image

   – If no OS kernel can be upgraded:

     You are advised to change the OS to a later version. For details, see **Changing the OS**.

   – If there is an OS kernel that can be upgraded:

     i. Run the following command to upgrade the OS kernel version:

        sudo apt-get install linux-image-*<target-kernel-package-name>*

     ii. (Optional) Upgrade the additional modules of the OS kernel.

        For an ECS running Ubuntu, you need to upgrade additional modules after the OS kernel is upgraded.

        sudo apt-get install linux-modules-extra-*<target-kernel-package-name>*

        For example, to update the kernel of Ubuntu 20.04 to 5.15.0, run the following commands:

        sudo apt update

        apt-cache search linux-image | grep '5.15' | grep generic

        sudo apt-get install linux-image-5.15.0-122-generic

        sudo apt-get install linux-modules-extra-5.15.0-122-generic

4. Run the following command to update the GRUB file so that the ECS can select the target kernel version during startup:

   sudo update-grub

5. Run the following command to restart the ECS:

   sudo reboot

6. Run the following command to check whether the kernel version has been upgraded:

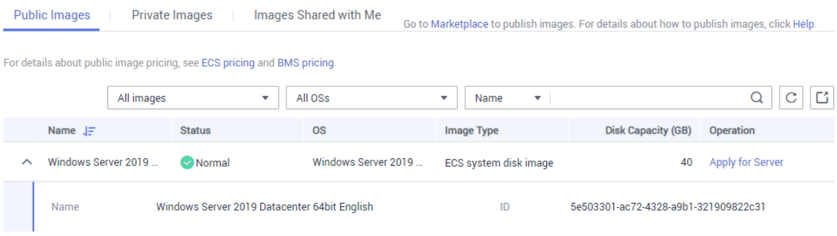
   uname -r

   If the new kernel version is returned, the kernel has been upgraded.

8.9 Why Cannot My ECS OS Start Properly?

1. Check the image based on which the ECS was created. If the image is a public one, this issue is not caused by private image sources.

   Figure 8-10 Image type



Go to Marketplace to publish images. For details about how to publish images, click Help.

For details about public image pricing, see ECS pricing and BMS pricing.

Name	Status	OS	Image Type	Disk Capacity (GB)	Operation
Windows Server 2019 ...	Normal	Windows Server 2019 ...	ECS system disk image	40	Apply for Server

Name: Windows Server 2019 Datacenter 64bit English
ID: 5e503301-ac72-4328-a9b1-321909822c31

2. Click **Apply for Server** and check whether the same ECS can be created. If not, this image may have been canceled.
3. Change the ECS OS to one that is available on the management console.

8.10 How Can I Fix the Meltdown and Spectre Security Vulnerabilities on Intel Processor Chips?

Symptom

On January 3, 2018 (Beijing time), severe security vulnerabilities Meltdown and Spectre were found on Intel processor chips. The details are as follows:

Vulnerability name: Severe chip-level vulnerabilities on Intel processor chips

Vulnerability IDs: CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

Severity: High risk

Vulnerability description: High-risk CPU kernel vulnerabilities Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5715 and CVE-2017-5753) exposed. Attackers can use these vulnerabilities to bypass the memory security isolation mechanism and access the core data of the OS and other programs without authorization, leading to sensitive information disclosure.

Impact

These vulnerabilities will not cause attacks between ECSs but may introduce attacks between:

- Applications on an ECS
- Accounts for logging in to an ECS

If your ECSs are created using a public image, the cloud platform will automatically fix the vulnerabilities, which will not affect your services.

If your ECSs are created using a private image, determine whether to install a patch described in this section in the private image based on the impact of the vulnerabilities.

Background

For details about the official patch release of affected OSs, see **Huawei Cloud Security Notices**.

Prerequisites

Tests have been fully verified and ECS data has been backed up.

Installing a Patch on Windows ECSs

Step 1 Log in to the ECS.

Step 2 Use either of the following methods to install the patch:

- Method 1: Use Windows Update to install the patch.
  a. Open Windows Update and click **Check for Updates**.
  b. Download and install the required patch.
- Method 2: Manually download and install the patch.

  Download the official patch and install it. For details, see **Background**.

Step 3 Restart the ECS for the patch to take effect.

Step 4 Check whether the patch has been installed.

1. Check whether the ECS is running properly.
2. Check whether the requirements specified in the **Verification** column of **Background** are met.

----End

Installing a Patch on Linux ECSs

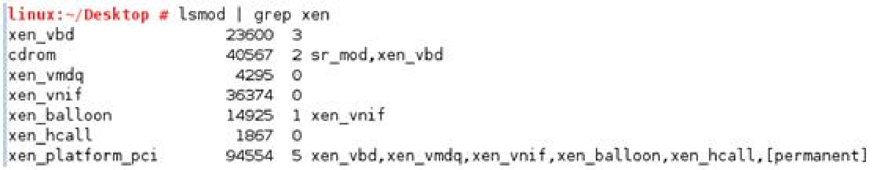
Step 1 Log in to the ECS.

Step 2 Check whether Tools has been installed on the Linux ECS (SUSE Linux Enterprise Server 11 SP1 is used as an example).

1. Run the following command on any directory to view the ECS driver:

   lsmod | grep xen

   Figure 8-11 Viewing the ECS driver

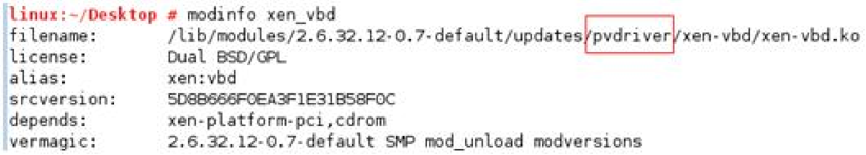


```
linux:~/Desktop # lsmod | grep xen
xen_vbd                23600  3
cdrom                  40567  2 sr_mod,xen_vbd
xen_vmdq                4295  0
xen_vnif               36374  0
xen_balloon            14925  1 xen_vnif
xen_hcall               1867  0
xen_platform_pci       94554  5 xen_vbd,xen_vmdq,xen_vnif,xen_balloon,xen_hcall,[permanent]
```

2. Run the following command to view the driver path (a disk driver is used as an example):

   modinfo xen_vbd

   Figure 8-12 Viewing the driver path



```
linux:~/Desktop # modinfo xen_vbd
filename:       /lib/modules/2.6.32.12-0.7-default/updates/pvdriver/xen-vbd/xen-vbd.ko
license:        Dual BSD/GPL
alias:          xen:vbd
srcversion:     5D8B666F0EA3F1E31B58F0C
depends:        xen-platform-pci,cdrom
vermagic:       2.6.32.12-0.7-default SMP mod_unload modversions
```

3. Check whether **pvdriver** is contained in the driver path.
   - If so, Tools have been installed in the ECS. Then, go to step **Step 3**.
   - If no, go to step **Step 4**.

Step 3 Uninstall Tools.

1. Run the following command to switch to user **root**:

   su root

2. Run the following command to uninstall Tools in the root directory:

   /etc/.uvp-monitor/uninstall

3. Run the following command to restart the ECS:

   reboot

Step 4 Install the patch to upgrade the kernel. For details, see **Background**.

NOTE

After updating the kernel, run the **reboot** command to restart the ECS.

Step 5 Check whether the patch has been installed.

1. Check whether the ECS is running properly.
2. Check whether the requirements specified in the **Verification** column of **Background** are met.

NOTE

After the patch is installed, the ECS uses the driver delivered with the OS. In this event, the memory usage and disk usage of Linux ECSs will not be monitored. The other features and functions are not affected. If the memory usage and disk usage must be monitored, contact customer service.

----End

Checking Whether Security Vulnerabilities Have Been Fixed on Linux

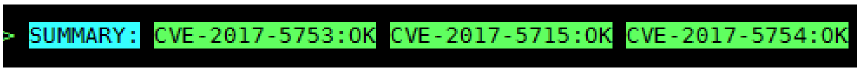
1. Click **spectre-meltdown-checker** to obtain **spectre-meltdown-checker.sh**.
2. Upload the script to the ECS.
3. Run the following commands on the ECS and check whether the Meltdown or Spectre vulnerability has been fixed based on the script prompt:

   chmod +x spectre-meltdown-checker.sh

   sudo bash spectre-meltdown-checker.sh

   Figure 8-13 shows the command output.

   Figure 8-13 Command output after the script is executed



```
> SUMMARY: CVE-2017-5753:OK CVE-2017-5715:OK CVE-2017-5754:OK
```

   OK indicates that the vulnerability has been fixed, and **KO** indicates that the vulnerability has not been fixed. The information shown in **Figure 8-13** indicates that the CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754 vulnerabilities have been fixed.

Enabling or Disabling the Security Vulnerability Patch on Linux

CPU speculative execution optimizes performance. Therefore, fixing the Meltdown or Spectre vulnerability may deteriorate performance under specific workloads.

If the impact on the system performance is unacceptable or a better protection solution is available, you can disable certain or all security protection policies.

Determine the optimal security policy based on application scenarios:

- Meltdown vulnerability

  Page Table Isolation (PTI) takes effect on the kernel. This function is suitable for CVE-2017-5754.
- Spectre vulnerability

  Indirect Branch Restricted Speculation (IBRS) takes effect on specified registers (MSR) in SPEC_CTRL model. Working with retpoline, IBRS controls Indirect Branch Prediction Barriers (IBPBs) on specified registers (MSR) in PRED_CMD model. This function is suitable for CVE-2017-5715.

  NOTE

  The CVE-2017-5753 vulnerability is fixed by a kernel patch and cannot be disabled. No obvious impact was detected for the patch in Red Hat performance tests.
- **Disabling the Meltdown Vulnerability Patch**

  To prevent the enabling of PTI from deteriorating the system performance, or a better protection solution is available, perform the following operations to disable the patch:

  a. Modify kernel parameters based on OSs:
     - CentOS, EulerOS, Ubuntu, Fedora, and Red Hat: Add the kernel parameter **nopti**.
     - Debian and OpenSUSE: Add the kernel parameter **pti=off**.

  b. Restart the ECS.
- **Disabling the Spectre Vulnerability Patch**

  To prevent the Spectre vulnerability fixing from deteriorating the system performance, or a better protection solution is available, perform the following operations to disable the patch:

  a. Modify kernel parameters based on OSs:
     - CentOS, EulerOS, Fedora, Debian, Red Hat, and OpenSUSE: Add the kernel parameter **spectre_v2=off**.
     - Ubuntu: Add the kernel parameter **nospectre_v2=off**.

  b. Restart the ECS.

If you are using one of the following OSs, visit their official website for more details.

Red Hat: **https://access.redhat.com/articles/3311301?spm=a2c4g.11186623.2.20.42b49d4aJuKYx2**

SUSE: **https://www.suse.com/support/kb/doc/?spm=a2c4g.11186623.2.21.42b49d4avOXw7d&id=7022512**

Ubuntu: **https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown**

8.11 How Can I Enable SELinux on an ECS Running CentOS?

Symptom

SELinux is disabled on ECSs running CentOS 7.5 by default. After I enable SELinux by running **/etc/selinux/config** and enter the login password, the login failed.

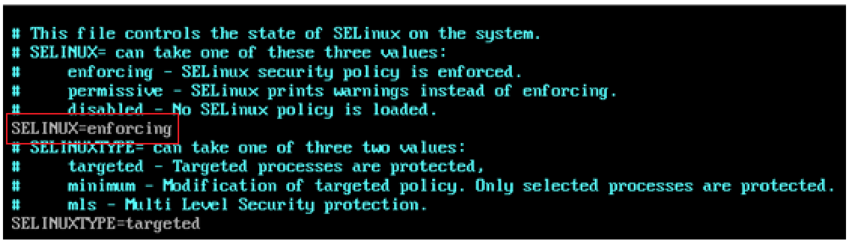
This section describes how to resolve this issue based on enabled SELinux.

Solution

The operations described in this section are performed on ECSs running CentOS 7.5.

1. Run the following command to change **SELINUX=disabled** in the SELinux configuration file to **SELINUX=enforcing**:

   vim /etc/selinux/config

   ```
   # This file controls the state of SELinux on the system.
   # SELINUX= can take one of these three values:
   #     enforcing - SELinux security policy is enforced.
   #     permissive - SELinux prints warnings instead of enforcing.
   #     disabled - No SELinux policy is loaded.
   SELINUX=enforcing
   # SELINUXTYPE= can take one of three two values:
   #     targeted - Targeted processes are protected,
   #     minimum - Modification of targeted policy. Only selected processes are protected.
   #     mls - Multi Level Security protection.
   SELINUXTYPE=targeted
   ```

2. Run the following command to automatically enable SELINUX on the file system upon ECS restarting:

   touch /.autorelabel

3. Run the following command to restart the ECS for the configuration to take effect:

   reboot

   NOTE

   After the preceding command is executed, the system automatically restarts twice.

8.12 What Should I Do If the Cursor Is Unavailable After a GNOME GUI Is Installed on a Kunpeng ECS Running CentOS 7 or NeoKylin NKASV 7?

Symptom

After a GNOME GUI is installed on a Kunpeng ECS running CentOS 7 or NeoKylin NKASV 7, the cursor is unavailable in remote logins.

Possible Causes

x86 ECSs use Cirrus GPUs, and Kunpeng ECSs use Virtio GPUs. The cursor can be a software cursor or a hardware cursor.

By default, Virtio GPUs use the hardware cursor. The position and shape of the hardware cursor rely on the VNC client. If the function of "Let remote server deal with cursor" is enabled on the hardware cursor, the VNC client ignores cursor requests. In such a case, the cursor is not displayed when you remotely log in to the ECS.

Solution

Disable the hardware cursor. This section uses a Kunpeng ECS running CentOS 7.5 64bit as an example.

For instructions about how to install a GUI on an ECS running CentOS 7.5, see **How Can I Install a GUI on an ECS Running CentOS 7?**

1. Run the following commands to add the **20-virtio.conf** configuration file in the **/etc/X11/xorg.conf.d/** directory:

   cd /etc/X11/xorg.conf.d

   touch 20-virtio.conf

2. Run the following command to obtain the **xorg.conf** configuration template:

   Xorg :0 -configure

   The generated file is stored in **/root/xorg.conf.new**.

   NOTE

   If a GUI has been installed, run the following command:

   Xorg :2 -configure

   The generated file is stored in **/root/xorg.conf.new**.

3. Copy the description of the GUI in **/root/xorg.conf.new** to **20-virtio.conf**.

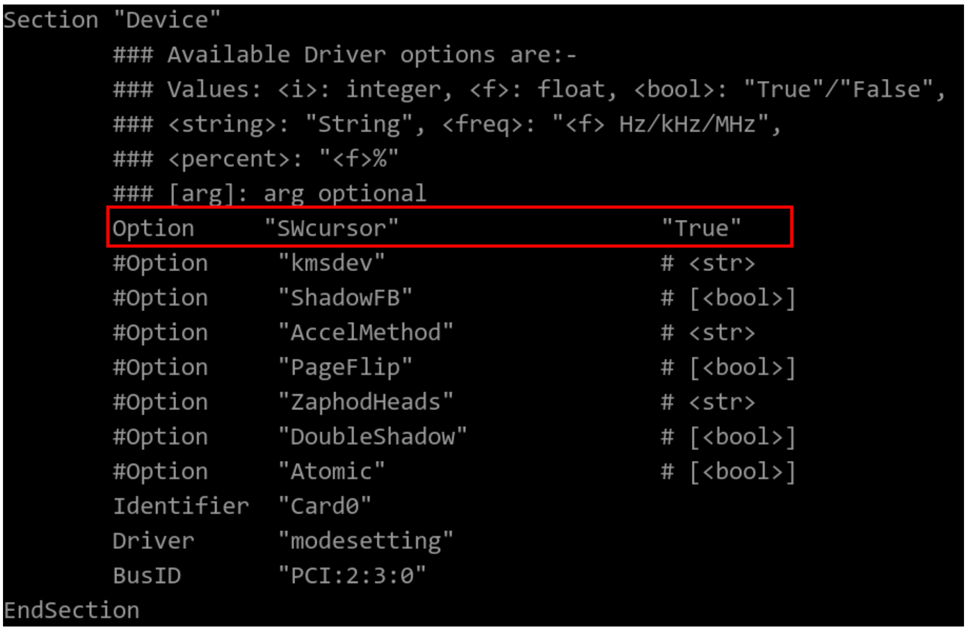
   cp /root/xorg.conf.new /etc/X11/xorg.conf.d/20-virtio.conf

4. Add a line for the Option description.

   ```
   Option    "SWcursor"    "True"
   ```

   Figure 8-14 shows **20-virtio.conf** with the added information.

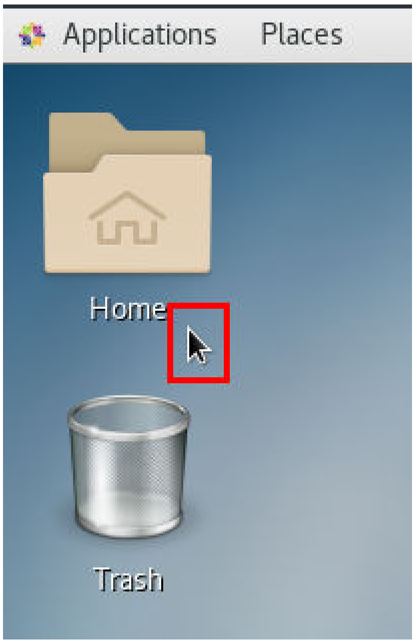
Figure 8-14 20-virtio.conf



```
Section "Device"
        ### Available Driver options are:-
        ### Values: <i>: integer, <f>: float, <bool>: "True"/"False",
        ### <string>: "String", <freq>: "<f> Hz/kHz/MHz",
        ### <percent>: "<f>%"
        ### [arg]: arg optional
        Option     "SWcursor"                   "True"
        #Option     "kmsdev"                    # <str>
        #Option     "ShadowFB"                  # [<bool>]
        #Option     "AccelMethod"               # <str>
        #Option     "PageFlip"                  # [<bool>]
        #Option     "ZaphodHeads"               # <str>
        #Option     "DoubleShadow"              # [<bool>]
        #Option     "Atomic"                    # [<bool>]
        Identifier  "Card0"
        Driver      "modesetting"
        BusID       "PCI:2:3:0"
EndSection
```

5. Restart the ECS. The cursor is displayed on the GUI.

Figure 8-15 Cursor displayed on the GUI



8.13 How Do I View the GPU Usage of a GPU-accelerated ECS?

Symptom

The GPU usage of GPU-accelerated ECSs running Windows Server 2012 and Windows Server 2016 cannot be viewed in Task Manager.

This section provides two methods for you to view the GPU usage. One is to run a command in the command-line interface, and the other is to install the GPU-Z tool.

Prerequisites

The NVIDIA driver has been installed on the GPU-accelerated ECS.

Method 1

1. Log in to the GPU-accelerated ECS.
2. Start the **Run** dialog box. Enter **cmd** and press **Enter**.
3. Run the following commands to check the GPU usage:

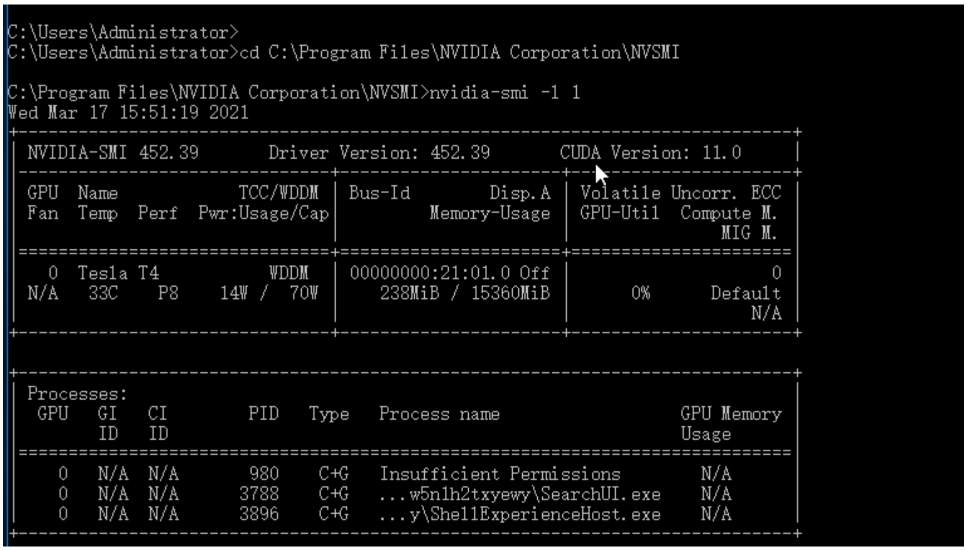
   cd C:\Program Files\NVIDIA Corporation\NVSMI

   nvidia-smi

   To continuously observe the GPU usage, run the following command:

   nvidia-smi -l 1

Figure 8-16 GPU usage



```
C:\Users\Administrator>
C:\Users\Administrator>cd C:\Program Files\NVIDIA Corporation\NVSMI

C:\Program Files\NVIDIA Corporation\NVSMI>nvidia-smi -l 1
Wed Mar 17 15:51:19 2021
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 452.39       Driver Version: 452.39       CUDA Version: 11.0     |
|-------------------------------+----------------------+----------------------+
| GPU  Name            TCC/WDDM | Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|                               |                      |               MIG M. |
|===============================+======================+======================|
|   0  Tesla T4            WDDM | 00000000:21:01.0 Off |                    0 |
| N/A   33C    P8    14W /  70W |    238MiB / 15360MiB |      0%      Default |
|                               |                      |                  N/A |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|    0   N/A  N/A       980    C+G   Insufficient Permissions        N/A      |
|    0   N/A  N/A      3788    C+G   ...w5n1h2txyewy\SearchUI.exe    N/A      |
|    0   N/A  N/A      3896    C+G   ...y\ShellExperienceHost.exe    N/A      |
+-----------------------------------------------------------------------------+
```

NOTE

NVIDIA GPUs can work in Tesla Compute Cluster (TCC) or Windows Display Driver Model (WDDM) mode.

- In TCC mode, the GPU is completely used for computing.
- In WDDM mode, the GPU supports both compute and graphics workloads.

The WDDM mode can be used only when GRID drivers are installed on GPU-accelerated ECSs.

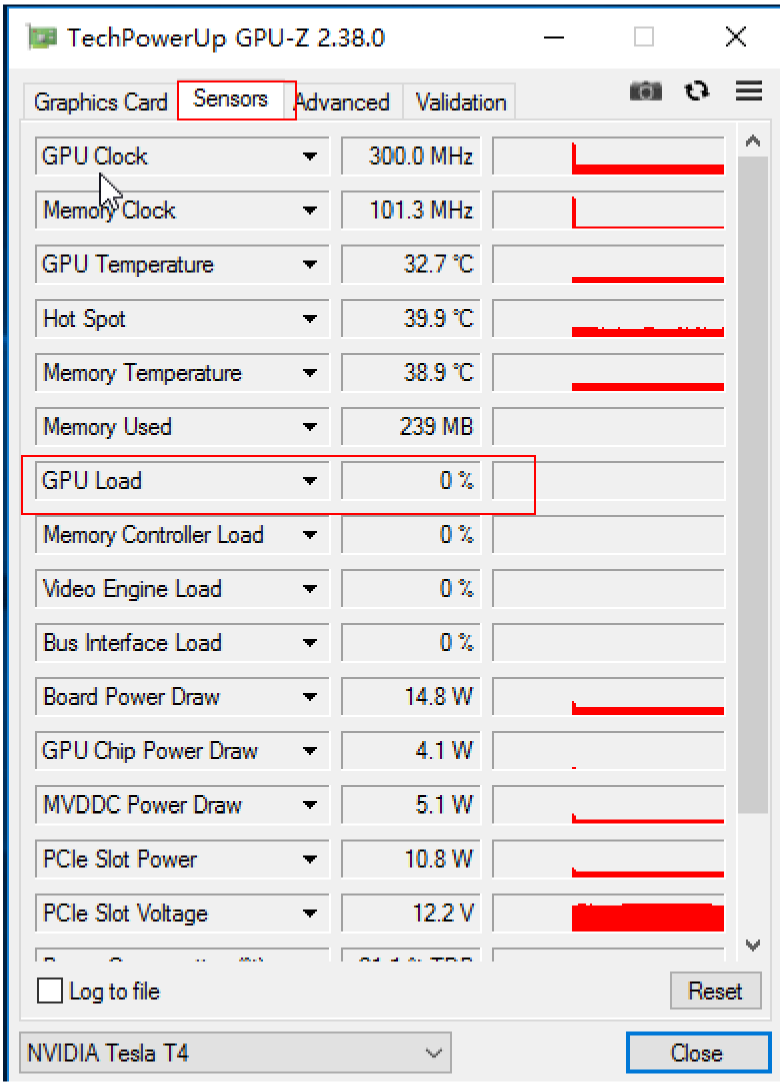
Learn more about TCC and WDDM.

Method 2

1. Log in to the GPU-accelerated ECS.

2. **Download GPU-Z** and install it.
3. Open GPU-Z and click **Sensors** to view the GPU usage.

Figure 8-17 GPU usage



GPU Clock	300.0 MHz
Memory Clock	101.3 MHz
GPU Temperature	32.7 °C
Hot Spot	39.9 °C
Memory Temperature	38.9 °C
Memory Used	239 MB
GPU Load	0 %
Memory Controller Load	0 %
Video Engine Load	0 %
Bus Interface Load	0 %
Board Power Draw	14.8 W
GPU Chip Power Draw	4.1 W
MVDDC Power Draw	5.1 W
PCIe Slot Power	10.8 W
PCIe Slot Voltage	12.2 V

☐ Log to file

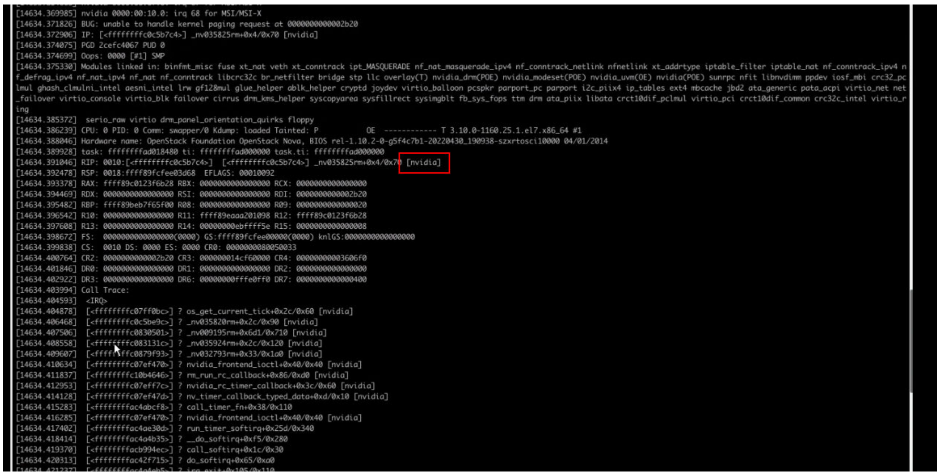
NVIDIA Tesla T4

8.14 Why Does the NVIDIA Kernel Crashes on a GPU-accelerated ECS?

Symptom

A GPU-accelerated ECS crashed during running. After the ECS was restarted, no NVIDIA driver stack logs were recorded.

Figure 8-18 Stack log information



```
[14634.369985] nvidia 0000:00:10.0: irq 68 for MSI/MSI-X
[14634.371826] BUG: unable to handle kernel paging request at 0000000000002b20
[14634.372906] IP: [<ffffffffc0c5b7c4>] _nv035825rm+0x4/0x70 [nvidia]
[14634.374075] PGD 2cefc4067 PUD 0
[14634.374699] Oops: 0000 [#1] SMP
[14634.375330] Modules linked in: binfmt_misc fuse xt_nat veth xt_conntrack ipt_MASQUERADE nf_nat_masquerade_ipv4 nf_conntrack_netlink nfnetlink xt_addrtype iptable_filter iptable_nat nf_conntrack_ipv4 n
f_defrag_ipv4 nf_nat_ipv4 nf_nat nf_conntrack libcrc32c br_netfilter bridge stp llc overlay(T) nvidia_drm(POE) nvidia_modeset(POE) nvidia_uvm(OE) nvidia(POE) sunrpc nfit libnvdimm ppdev iosf_mbi crc32_pc
lmul ghash_clmulni_intel aesni_intel lrw gf128mul glue_helper ablk_helper cryptd joydev virtio_balloon pcspkr parport_pc parport i2c_piix4 ip_tables ext4 mbcache jbd2 ata_generic pata_acpi virtio_net net
_failover virtio_console virtio_blk failover cirrus drm_kms_helper syscopyarea sysfillrect sysimgblt fb_sys_fops ttm drm ata_piix libata crct10dif_pclmul virtio_pci crct10dif_common crc32c_intel virtio_r
ing
[14634.385372]  serio_raw virtio drm_panel_orientation_quirks floppy
[14634.386239] CPU: 0 PID: 0 Comm: swapper/0 Kdump: loaded Tainted: P           OE  ------------ T 3.10.0-1160.25.1.el7.x86_64 #1
[14634.388046] Hardware name: OpenStack Foundation OpenStack Nova, BIOS rel-1.10.2-0-g5f4c7b1-20220430_190938-szxrtosci10000 04/01/2014
[14634.389928] task: ffffffffad018480 ti: ffffffffad000000 task.ti: ffffffffad000000
[14634.391046] RIP: 0010:[<ffffffffc0c5b7c4>]  [<ffffffffc0c5b7c4>] _nv035825rm+0x4/0x70 [nvidia]
[14634.392478] RSP: 0018:ffff89fcfee03d68  EFLAGS: 00010092
[14634.393378] RAX: ffff89c0123f6b28 RBX: 0000000000000000 RCX: 0000000000000000
[14634.394469] RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000002b20
[14634.395482] RBP: ffff89beb7f65f00 R08: 0000000000000000 R09: 0000000000000020
[14634.396542] R10: 0000000000000000 R11: ffff89eaaa201098 R12: ffff89c0123f6b28
[14634.397608] R13: 0000000000000000 R14: 00000000ebffff5e R15: 0000000000000008
[14634.398672] FS:  0000000000000000(0000) GS:ffff89fcfee00000(0000) knlGS:0000000000000000
[14634.399838] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[14634.400764] CR2: 0000000000002b20 CR3: 000000014cf60000 CR4: 00000000003606f0
[14634.401846] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[14634.402922] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
[14634.403994] Call Trace:
[14634.404593]  <IRQ>
[14634.404878]  [<ffffffffc07ff0bc>] ? os_get_current_tick+0x2c/0x60 [nvidia]
[14634.406468]  [<ffffffffc0c5be9c>] ? _nv035820rm+0x2c/0x90 [nvidia]
[14634.407506]  [<ffffffffc0830501>] ? _nv009195rm+0x6d1/0x710 [nvidia]
[14634.408558]  [<ffffffffc083131c>] ? _nv035924rm+0x2c/0x120 [nvidia]
[14634.409607]  [<ffffffffc0879f93>] ? _nv032793rm+0x33/0x1a0 [nvidia]
[14634.410634]  [<ffffffffc07ef470>] ? nvidia_frontend_ioctl+0x40/0x40 [nvidia]
[14634.411837]  [<ffffffffc10b4646>] ? rm_run_rc_callback+0x86/0xd0 [nvidia]
[14634.412953]  [<ffffffffc07eff7c>] ? nvidia_rc_timer_callback+0x3c/0x60 [nvidia]
[14634.414128]  [<ffffffffc07ef47d>] ? nv_timer_callback_typed_data+0xd/0x10 [nvidia]
[14634.415283]  [<ffffffffac4abcf8>] ? call_timer_fn+0x38/0x110
[14634.416285]  [<ffffffffc07ef470>] ? nvidia_frontend_ioctl+0x40/0x40 [nvidia]
[14634.417402]  [<ffffffffac4ae30d>] ? run_timer_softirq+0x25d/0x340
[14634.418414]  [<ffffffffac4a4b35>] ? __do_softirq+0xf5/0x280
[14634.419370]  [<ffffffffacb994ec>] ? call_softirq+0x1c/0x30
[14634.420313]  [<ffffffffac42f715>] ? do_softirq+0x65/0xa0
```

Possible Causes

The ECS kernel crashed due to an official NVIDIA driver bug.

Solutions

- Method 1: Restart the ECS.

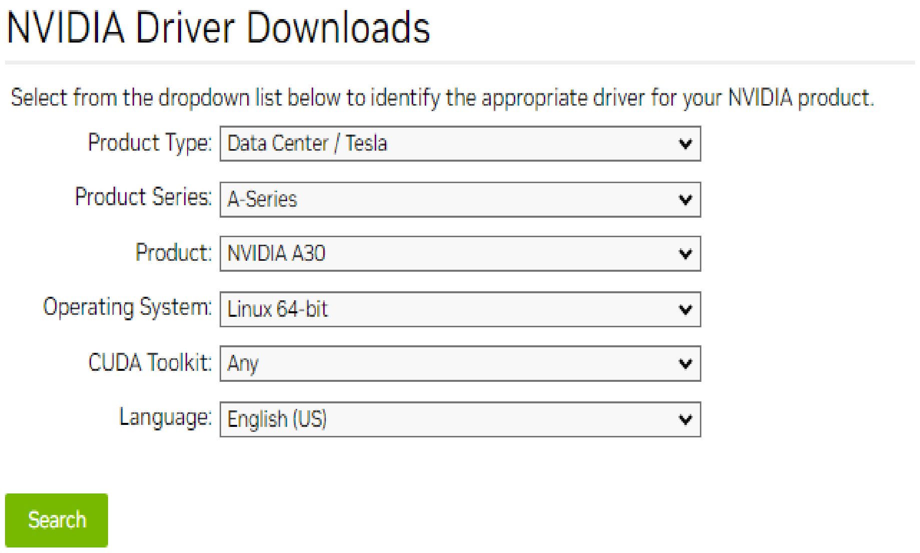
  After the ECS is restarted, the ECS can run properly.

- Method 2: Update the driver version.

  If the problem persists after the ECS is restarted, download the latest CUDA driver from the NVIDIA official website.

  a. Log in to the official NVIDIA driver download page at **https://www.nvidia.cn/Download/index.aspx?lang=en**.

  Figure 8-19 Driver download page

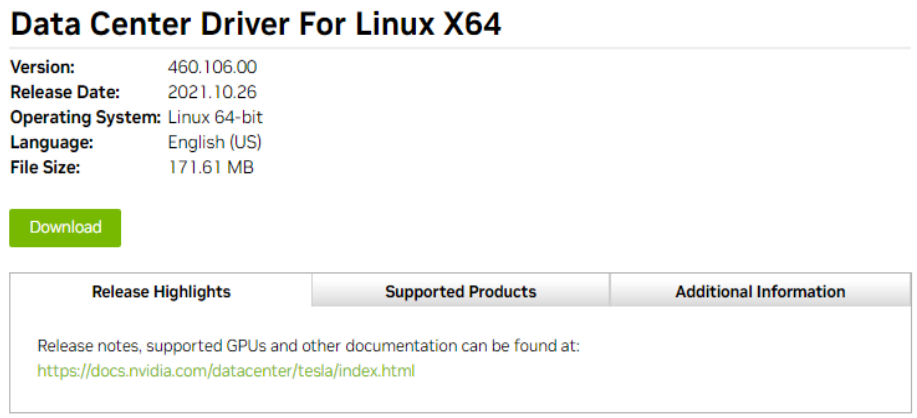
  NVIDIA Driver Downloads

  Select from the dropdown list below to identify the appropriate driver for your NVIDIA product.

  Product Type: Data Center / Tesla
  Product Series: A-Series
  Product: NVIDIA A30
  Operating System: Linux 64-bit
  CUDA Toolkit: Any
  Language: English (US)

  b. Enter the product information and click **Search**.

Figure 8-20 Latest driver version download page



Data Center Driver For Linux X64

Version: 460.106.00
Release Date: 2021.10.26
Operating System: Linux 64-bit
Language: English (US)
File Size: 171.61 MB

Release notes, supported GPUs and other documentation can be found at:
https://docs.nvidia.com/datacenter/tesla/index.html

On the **Release Highlights** tab, you can learn about the version updates and resolved issues of this version and determine whether to upgrade accordingly.

8.15 How Can I Boot a Linux ECS into Single-User Mode?

Scenarios

Single-user mode is a special system running mode of the Linux OS. In this mode, not all services may be loaded during startup, and a minimal runtime environment is provided. It is usually used for system maintenance and repair, and password resetting.

⚠ CAUTION

In single-user mode, you have high permissions. Incorrect operations may cause data loss or system damage. Exercise caution when performing operations in single-user mode.

This section describes how to boot a Linux ECS into single-user mode.

Procedure

1. Remotely log in to the ECS.

   For details, see **Logging In to a Linux ECS Using VNC**.

2. In the upper left corner of the login page, click **Ctrl+Alt+Del** to restart the ECS.

   This method does not apply to the following scenarios:

   - The ECS is experiencing lag.
   - The ECS is running EulerOS or Huawei Cloud EulerOS.

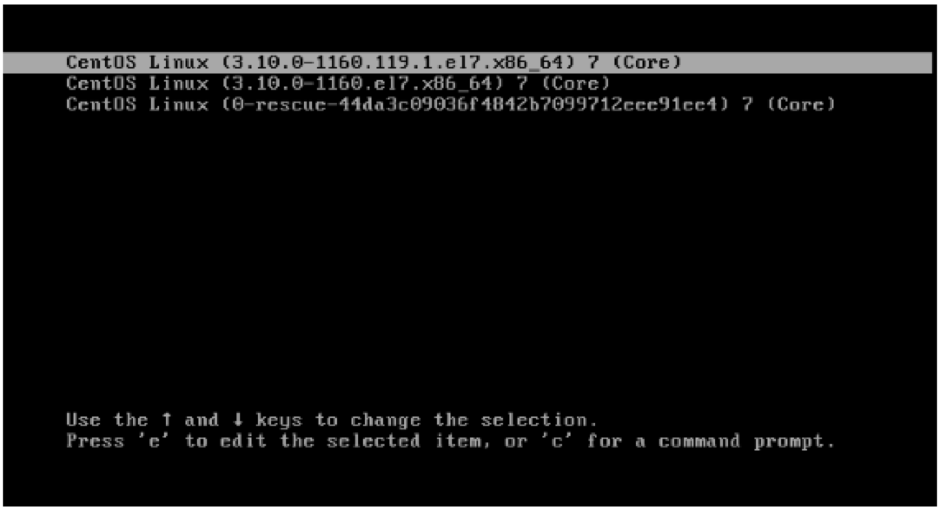
3. Enter single-user mode from kernel edit mode.

Select the instructions for entering single-user mode based on the OS type.

CentOS 7/8, CentOS Stream 8/9, AlmaLinux 8/9, and Rocky Linux 8/9

1. After the ECS is restarted, the kernel page is displayed. Press **e** to enter kernel edit mode.

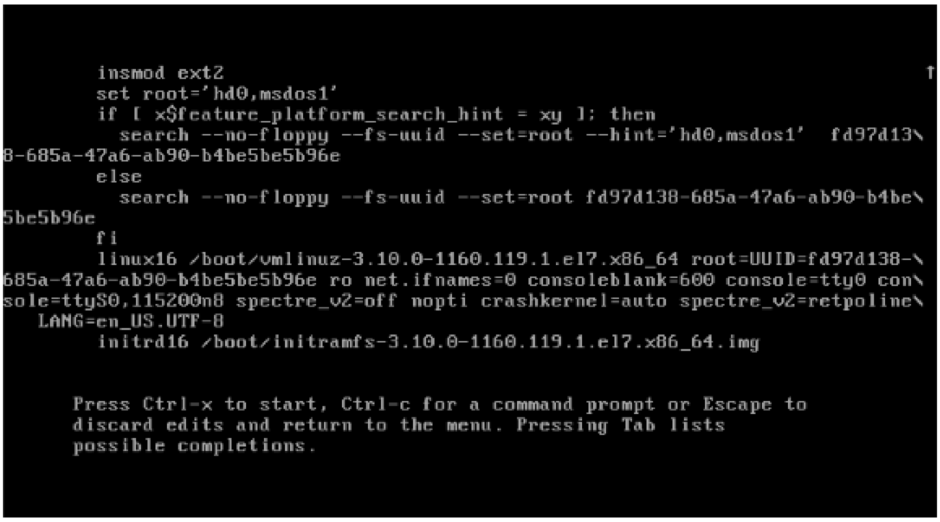
Figure 8-21 Kernel page



```
      CentOS Linux (3.10.0-1160.119.1.el7.x86_64) 7 (Core)
      CentOS Linux (3.10.0-1160.el7.x86_64) 7 (Core)
      CentOS Linux (0-rescue-44da3c09036f4842b7099712ece91ec4) 7 (Core)









      Use the ↑ and ↓ keys to change the selection.
      Press 'e' to edit the selected item, or 'c' for a command prompt.
```

2. After entering kernel edit mode, use the arrow keys on the keyboard to move the cursor to the line starting with **linux**.

Figure 8-22 Kernel editing mode

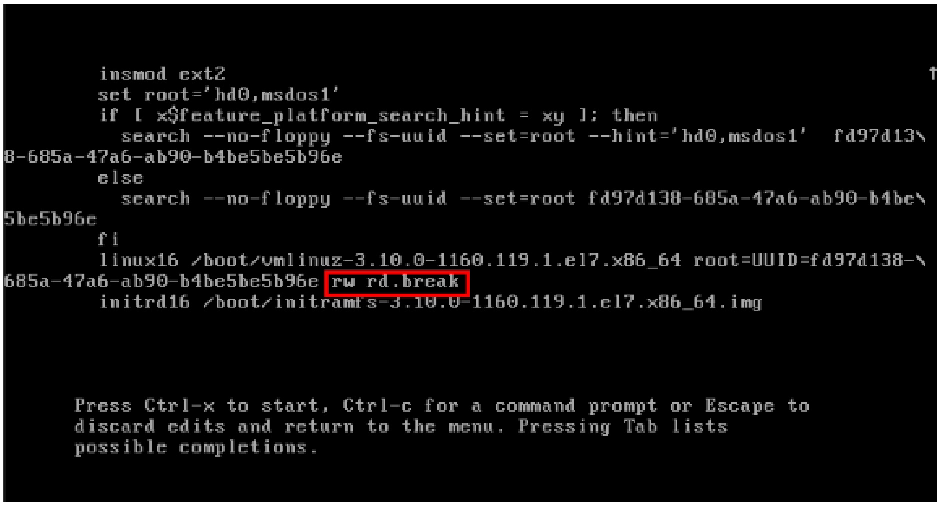


```
        insmod ext2                                                      ↑
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  fd97d13\
8-685a-47a6-ab90-b4be5be5b96e
        else
          search --no-floppy --fs-uuid --set=root fd97d138-685a-47a6-ab90-b4be\
5be5b96e
        fi
        linux16 /boot/vmlinuz-3.10.0-1160.119.1.el7.x86_64 root=UUID=fd97d138-\
685a-47a6-ab90-b4be5be5b96e ro net.ifnames=0 consoleblank=600 console=tty0 con\
sole=ttyS0,115200n8 spectre_v2=off nopti crashkernel=auto spectre_v2=retpoline\
   LANG=en_US.UTF-8
        initrd16 /boot/initramfs-3.10.0-1160.119.1.el7.x86_64.img


      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

3. Set the mode.
   - (Default) Single-user mode: In the line starting with **linux**, replace the content from **ro** to the end with **rw rd.break**.
   - Pre-mount mode: Replace the content from **ro** to the end with **rw rd.break=pre-mount**.

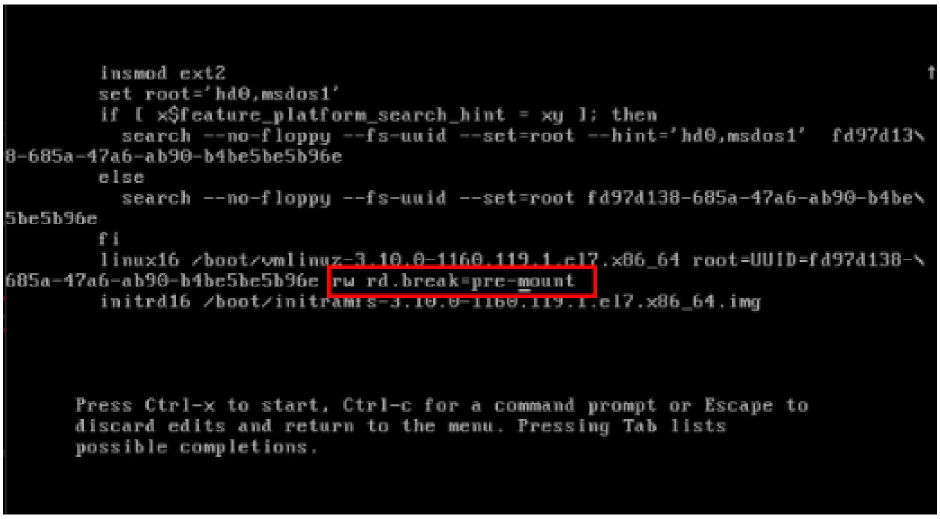
     The pre-mount mode is used to restore the file system of a system disk. Select the mode as needed.

Figure 8-23 Single-user mode



```
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  fd97d13\
8-685a-47a6-ab90-b4be5be5b96e
        else
          search --no-floppy --fs-uuid --set=root fd97d138-685a-47a6-ab90-b4be\
5be5b96e
        fi
        linux16 /boot/vmlinuz-3.10.0-1160.119.1.el7.x86_64 root=UUID=fd97d138-\
685a-47a6-ab90-b4be5be5b96e rw rd.break
        initrd16 /boot/initramfs-3.10.0-1160.119.1.el7.x86_64.img



      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

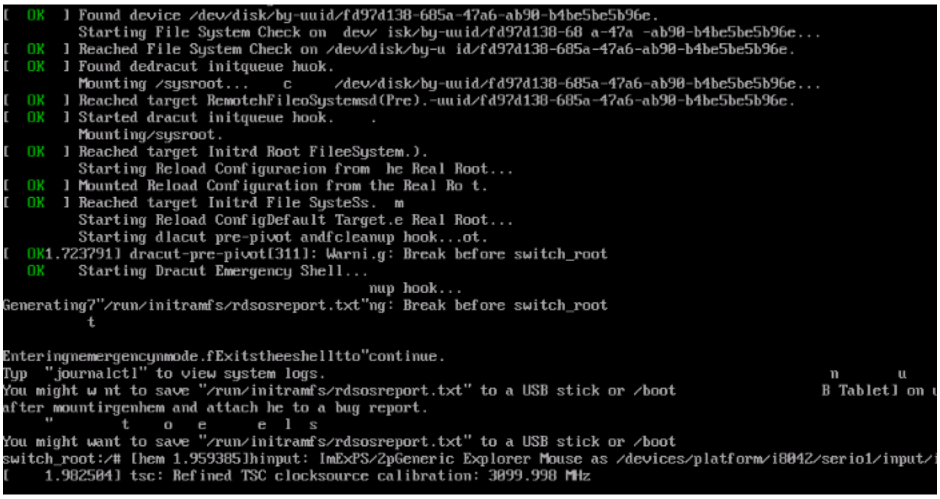
Figure 8-24 Pre-mount mode



```
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  fd97d13\
8-685a-47a6-ab90-b4be5be5b96e
        else
          search --no-floppy --fs-uuid --set=root fd97d138-685a-47a6-ab90-b4be\
5be5b96e
        fi
        linux16 /boot/vmlinuz-3.10.0-1160.119.1.el7.x86_64 root=UUID=fd97d138-\
685a-47a6-ab90-b4be5be5b96e rw rd.break=pre-mount
        initrd16 /boot/initramfs-3.10.0-1160.119.1.el7.x86_64.img



      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

4. Press **Ctrl** and **X** to start the system. The system enters single-user mode.

Figure 8-25 Starting the system

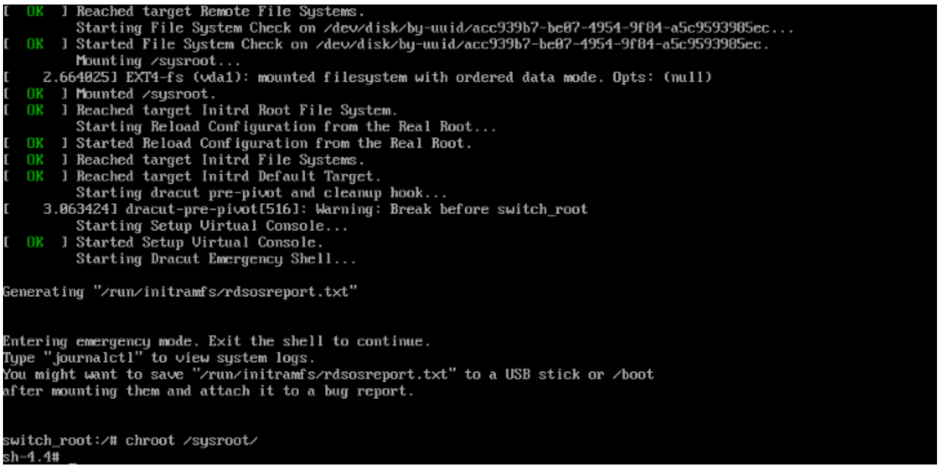


```
[  OK  ] Found device /dev/disk/by-uuid/fd97d138-685a-47a6-ab90-b4be5be5b96e.
         Starting File System Check on  dev/ isk/by-uuid/fd97d138-68 a-47a -ab90-b4be5be5b96e...
[  OK  ] Reached File System Check on /dev/disk/by-u id/fd97d138-685a-47a6-ab90-b4be5be5b96e.
[  OK  ] Found dedracut initqueue huok.
         Mounting /sysroot...    c     /dev/disk/by-uuid/fd97d138-685a-47a6-ab90-b4be5be5b96e...
[  OK  ] Reached target RemotehFileoSystemsd(Pre).-uuid/fd97d138-685a-47a6-ab90-b4be5be5b96e.
[  OK  ] Started dracut initqueue hook.    .
         Mounting/sysroot.
[  OK  ] Reached target Initrd Root FileeSystem.).
         Starting Reload Configuracion from  he Real Root...
[  OK  ] Mounted Reload Configuration from the Real Ro t.
[  OK  ] Reached target Initrd File SysteSs.  m
         Starting Reload ConfigDefault Target.e Real Root...
         Starting dlacut pre-pivot andfcleanup hook...ot.
[  OK1.723791] dracut-pre-pivot[311]: Warni.g: Break before switch_root
   OK    Starting Dracut Emergency Shell...
                                      nup hook...
Generating7"/run/initramfs/rdsosreport.txt"ng: Break before switch_root
        t

Enteringnemergencynmode.fExitstheeshellto"continue.
Typ  "journalctl" to view system logs.                                        n      u
You might w nt to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot             B Tablet] on 
after mountirgenhem and attach he to a bug report.
    "       t   o   e     e  l  s
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
switch_root:/# [hem 1.959385]hinput: ImExPS/2pGeneric Explorer Mouse as /devices/platform/i8042/serio1/input/
[    1.982504] tsc: Refined TSC clocksource calibration: 3099.998 MHz
```

5. Run the following command to switch to the real **root** directory:

   chroot /sysroot

Figure 8-26 Switching to the real **root** directory

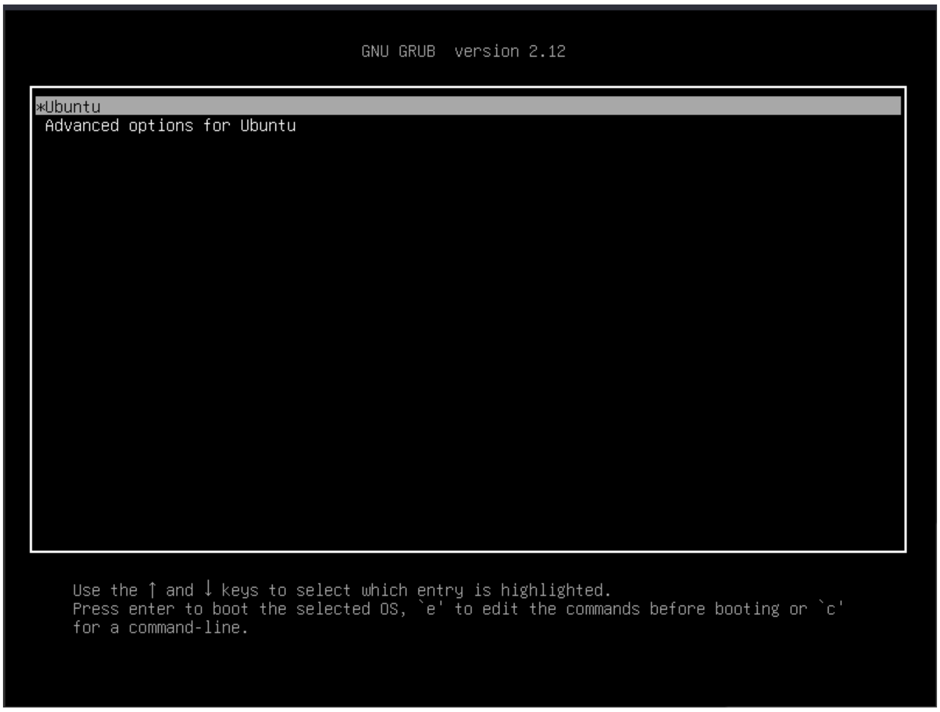


```
[  OK  ] Reached target Remote File Systems.
         Starting File System Check on /dev/disk/by-uuid/acc939b7-be07-4954-9f84-a5c9593985ec...
[  OK  ] Started File System Check on /dev/disk/by-uuid/acc939b7-be07-4954-9f84-a5c9593985ec.
         Mounting /sysroot...
[    2.664025] EXT4-fs (vda1): mounted filesystem with ordered data mode. Opts: (null)
[  OK  ] Mounted /sysroot.
[  OK  ] Reached target Initrd Root File System.
         Starting Reload Configuration from the Real Root...
[  OK  ] Started Reload Configuration from the Real Root.
[  OK  ] Reached target Initrd File Systems.
[  OK  ] Reached target Initrd Default Target.
         Starting dracut pre-pivot and cleanup hook...
[    3.063424] dracut-pre-pivot[516]: Warning: Break before switch_root
         Starting Setup Virtual Console...
[  OK  ] Started Setup Virtual Console.
         Starting Dracut Emergency Shell...

Generating "/run/initramfs/rdsosreport.txt"


Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.


switch_root:/# chroot /sysroot/
sh-4.4# _
```

Ubuntu 20-24, Debian10-12, and openEuler

1. After the ECS is restarted, the kernel page is displayed. Press **e** to enter kernel edit mode.

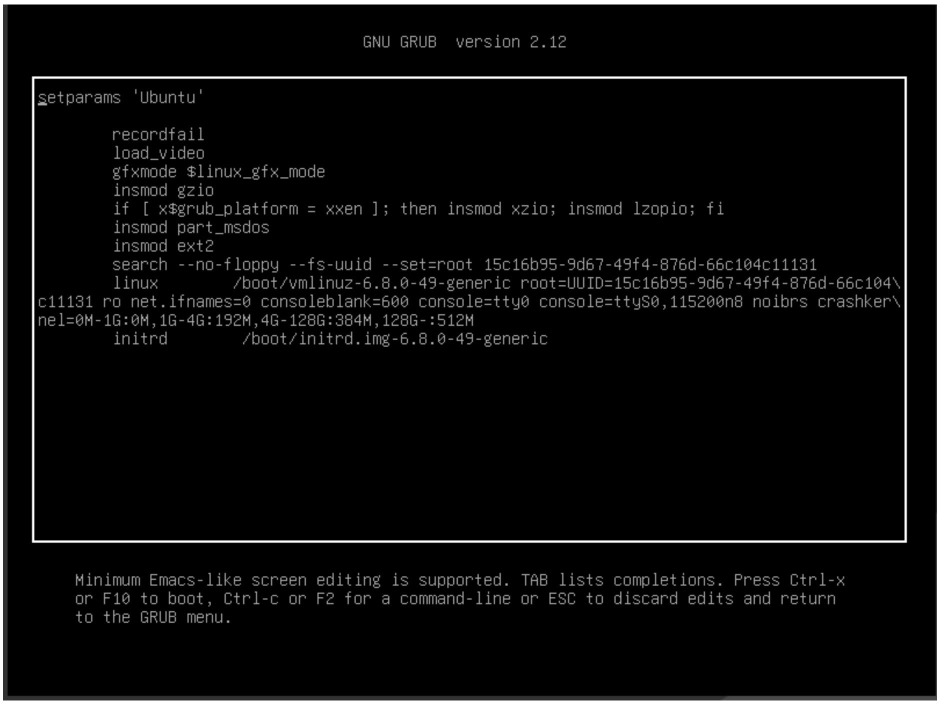
Figure 8-27 Kernel page



```
                         GNU GRUB  version 2.12

 *Ubuntu
  Advanced options for Ubuntu

      Use the ↑ and ↓ keys to select which entry is highlighted.
      Press enter to boot the selected OS, `e' to edit the commands before booting or `c'
      for a command-line.
```

2. After entering kernel edit mode, use the arrow keys on the keyboard to move the cursor to the line starting with **linux**.

Figure 8-28 Kernel editing mode

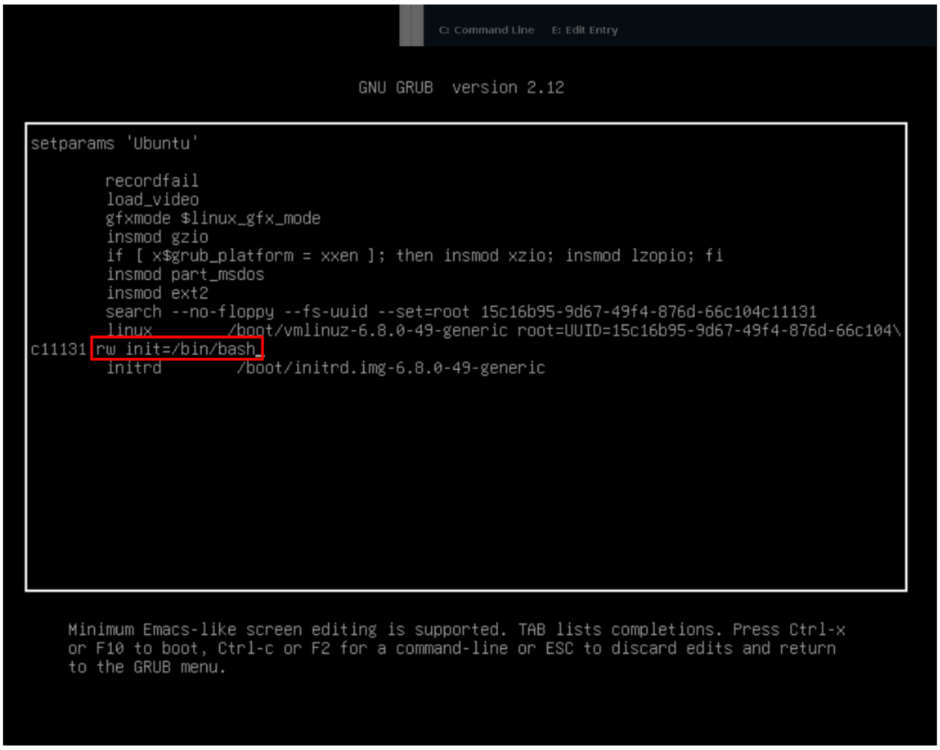


```
                          GNU GRUB  version 2.12

setparams 'Ubuntu'

        recordfail
        load_video
        gfxmode $linux_gfx_mode
        insmod gzio
        if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
        insmod part_msdos
        insmod ext2
        search --no-floppy --fs-uuid --set=root 15c16b95-9d67-49f4-876d-66c104c11131
        linux        /boot/vmlinuz-6.8.0-49-generic root=UUID=15c16b95-9d67-49f4-876d-66c104\
c11131 ro net.ifnames=0 consoleblank=600 console=tty0 console=ttyS0,115200n8 noibrs crashker\
nel=0M-1G:0M,1G-4G:192M,4G-128G:384M,128G-:512M
        initrd        /boot/initrd.img-6.8.0-49-generic

    Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x
    or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return
    to the GRUB menu.
```

3. Set the mode.
   - (Default) Single-user mode: In the line starting with **linux**, replace the content from **ro** to the end with **rw init=/bin/bash**.
   - Pre-mount mode: Replace the content from **tty0** to the end with **break**.

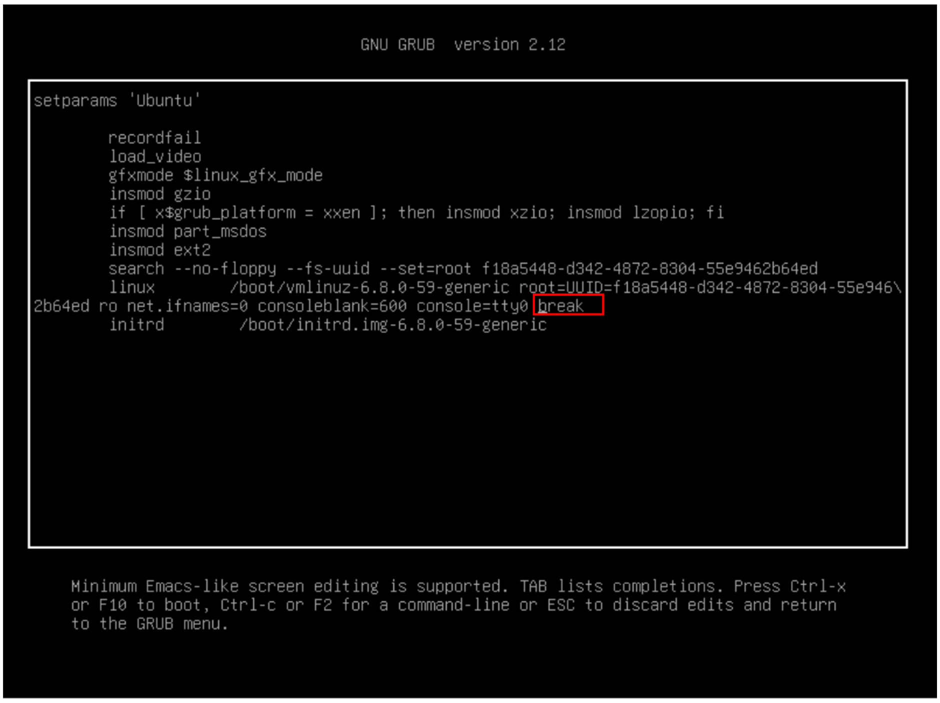
     The pre-mount mode is used to restore the file system of a system disk. Select the mode as needed.

Figure 8-29 Single-user mode



```
                         GNU GRUB  version 2.12

setparams 'Ubuntu'

        recordfail
        load_video
        gfxmode $linux_gfx_mode
        insmod gzio
        if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
        insmod part_msdos
        insmod ext2
        search --no-floppy --fs-uuid --set=root 15c16b95-9d67-49f4-876d-66c104c11131
        linux        /boot/vmlinuz-6.8.0-49-generic root=UUID=15c16b95-9d67-49f4-876d-66c104\
c11131 rw init=/bin/bash_
        initrd        /boot/initrd.img-6.8.0-49-generic

      Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x
      or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return
      to the GRUB menu.
```

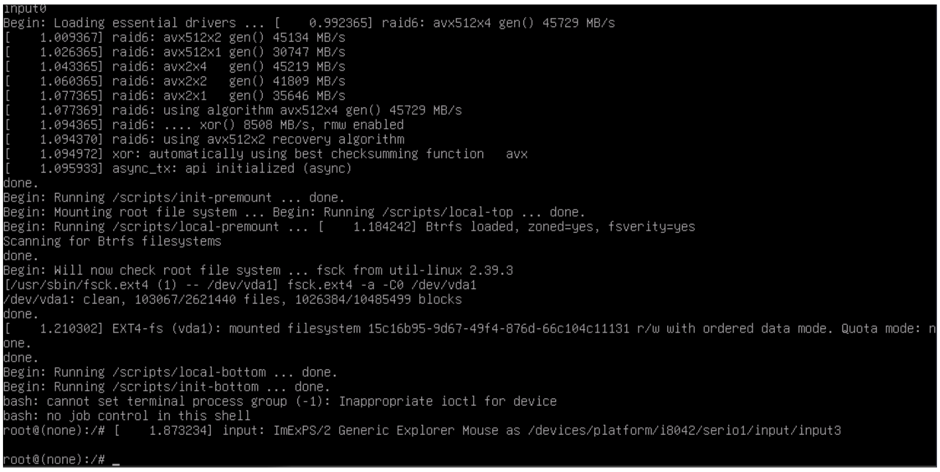
Figure 8-30 Pre-mount mode



```
                         GNU GRUB  version 2.12

setparams 'Ubuntu'

        recordfail
        load_video
        gfxmode $linux_gfx_mode
        insmod gzio
        if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
        insmod part_msdos
        insmod ext2
        search --no-floppy --fs-uuid --set=root f18a5448-d342-4872-8304-55e9462b64ed
        linux        /boot/vmlinuz-6.8.0-59-generic root=UUID=f18a5448-d342-4872-8304-55e946\
2b64ed ro net.ifnames=0 consoleblank=600 console=tty0 break
        initrd        /boot/initrd.img-6.8.0-59-generic

      Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x
      or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return
      to the GRUB menu.
```

4. Press **Ctrl** and **X** to start the system. The system enters single-user mode.

Figure 8-31 Starting the system

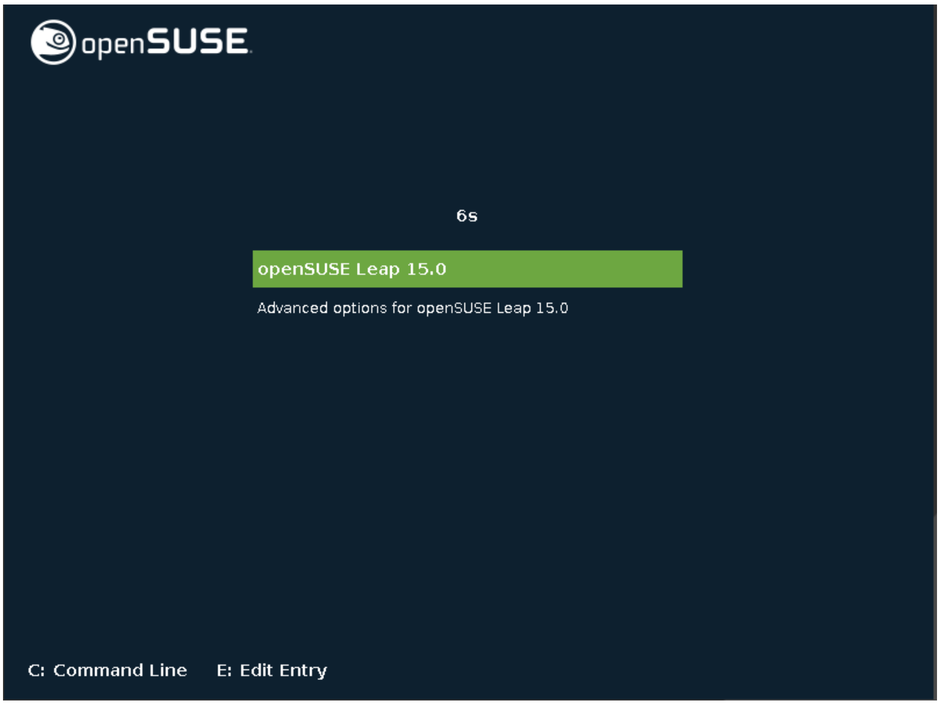


```
input0
Begin: Loading essential drivers ... [    0.992365] raid6: avx512x4 gen() 45729 MB/s
[    1.009367] raid6: avx512x2 gen() 45134 MB/s
[    1.026365] raid6: avx512x1 gen() 30747 MB/s
[    1.043365] raid6: avx2x4   gen() 45219 MB/s
[    1.060365] raid6: avx2x2   gen() 41809 MB/s
[    1.077365] raid6: avx2x1   gen() 35646 MB/s
[    1.077369] raid6: using algorithm avx512x4 gen() 45729 MB/s
[    1.094365] raid6: .... xor() 8508 MB/s, rmw enabled
[    1.094370] raid6: using avx512x2 recovery algorithm
[    1.094972] xor: automatically using best checksumming function   avx
[    1.095933] async_tx: api initialized (async)
done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... [    1.184242] Btrfs loaded, zoned=yes, fsverity=yes
Scanning for Btrfs filesystems
done.
Begin: Will now check root file system ... fsck from util-linux 2.39.3
[/usr/sbin/fsck.ext4 (1) -- /dev/vda1] fsck.ext4 -a -C0 /dev/vda1
/dev/vda1: clean, 103067/2621440 files, 1026384/10485499 blocks
done.
[    1.210302] EXT4-fs (vda1): mounted filesystem 15c16b95-9d67-49f4-876d-66c104c11131 r/w with ordered data mode. Quota mode: n
one.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# [    1.873234] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/input3

root@(none):/# _
```

openSUSE

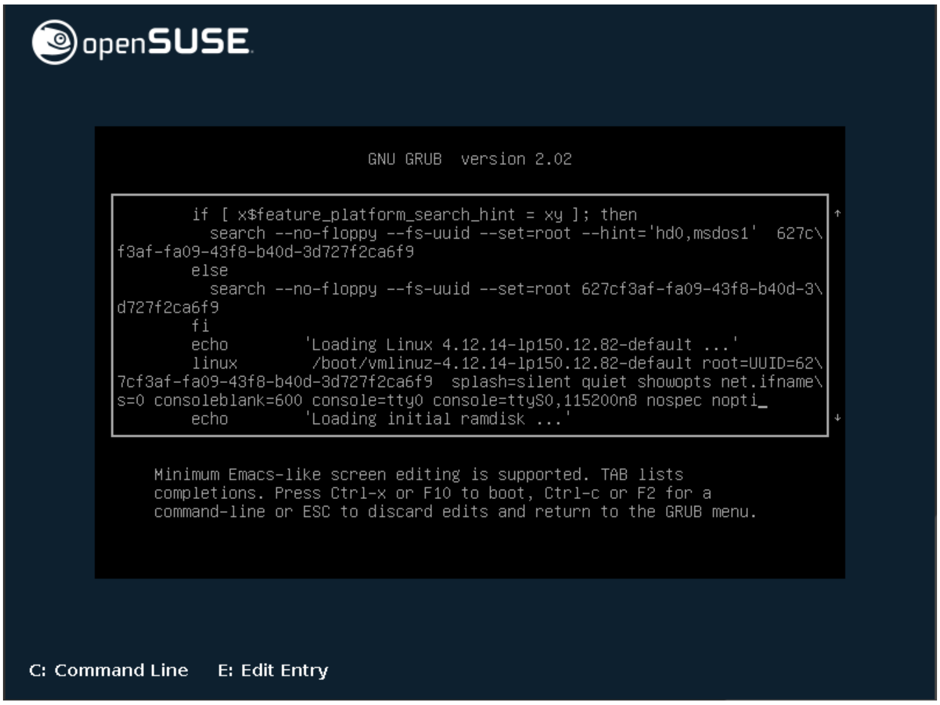
1. After the ECS is restarted, the kernel page is displayed. Press **e** to enter kernel edit mode.

Figure 8-32 Kernel page



2. After entering kernel edit mode, use the arrow keys to move the cursor to the line starting with **linux**.

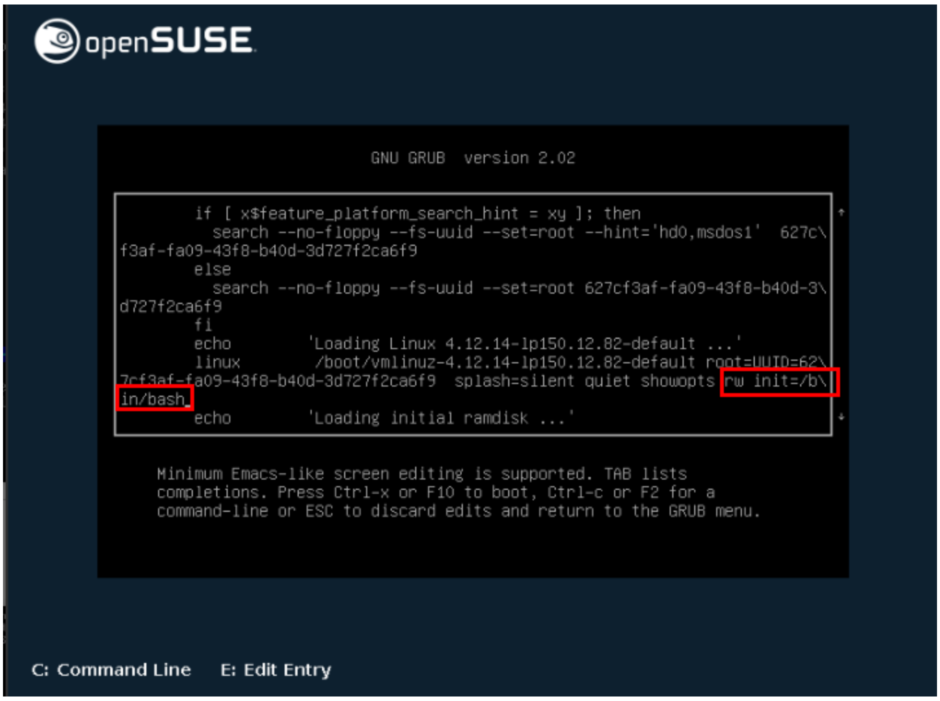
Figure 8-33 Kernel editing mode



```
                             GNU GRUB  version 2.02

        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  627c\
f3af-fa09-43f8-b40d-3d727f2ca6f9
        else
          search --no-floppy --fs-uuid --set=root 627cf3af-fa09-43f8-b40d-3\
d727f2ca6f9
        fi
        echo        'Loading Linux 4.12.14-lp150.12.82-default ...'
        linux        /boot/vmlinuz-4.12.14-lp150.12.82-default root=UUID=62\
7cf3af-fa09-43f8-b40d-3d727f2ca6f9  splash=silent quiet showopts net.ifname\
s=0 consoleblank=600 console=tty0 console=ttyS0,115200n8 nospec nopti_
        echo        'Loading initial ramdisk ...'

    Minimum Emacs-like screen editing is supported. TAB lists
    completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
    command-line or ESC to discard edits and return to the GRUB menu.
```

3. In the line starting with **linux**, replace the content from **net** to the end with **rw init=/bin/bash**.

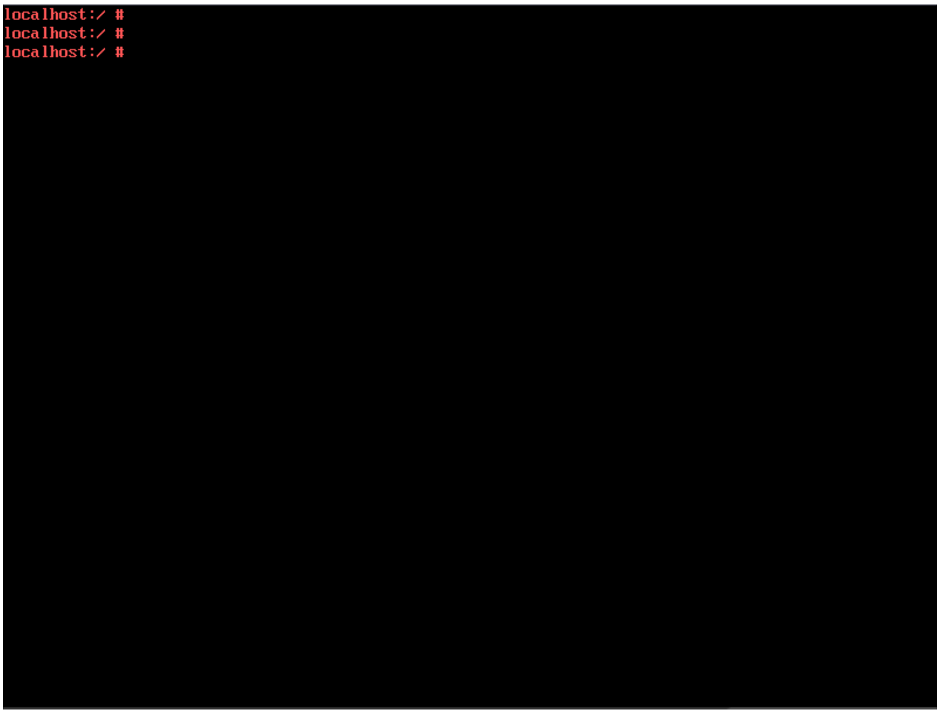
Figure 8-34 Single-user mode



```
                             GNU GRUB  version 2.02

        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  627c\
f3af-fa09-43f8-b40d-3d727f2ca6f9
        else
          search --no-floppy --fs-uuid --set=root 627cf3af-fa09-43f8-b40d-3\
d727f2ca6f9
        fi
        echo        'Loading Linux 4.12.14-lp150.12.82-default ...'
        linux        /boot/vmlinuz-4.12.14-lp150.12.82-default root=UUID=62\
7cf3af-fa09-43f8-b40d-3d727f2ca6f9  splash=silent quiet showopts rw init=/b\
in/bash_
        echo        'Loading initial ramdisk ...'

    Minimum Emacs-like screen editing is supported. TAB lists
    completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
    command-line or ESC to discard edits and return to the GRUB menu.
```

4. Press **Ctrl** and **X** to start the system. The system enters single-user mode.

Figure 8-35 Starting the system



```
localhost:/ #
localhost:/ #
localhost:/ #
```

8.16 How Can I Boot a Linux ECS into Debug Shell Mode?

Scenarios

Debug Shell is an emergency command line interface (CLI). When the Linux systemd cannot start properly or has a serious fault, you can use Debug Shell to rectify faults as user **root** without entering the password.

Debug Shell applies to the following scenarios:

- Reset passwords: If you forget the password of user **root**, you can reset the password in Debug Shell mode.
- Check error logs and fix configurations: If the OS is suspended after systemd starts, you can enter Debug Shell mode to check error logs and fix systemd configurations such as fstab and network configurations.

This section describes how to boot a Linux ECS into Debug Shell mode.

Procedure

1. Remotely log in to the ECS.

   For details, see **Logging In to a Linux ECS Using VNC**.

2. In the upper left corner of the login page, click **Ctrl+Alt+Del** to restart the ECS.

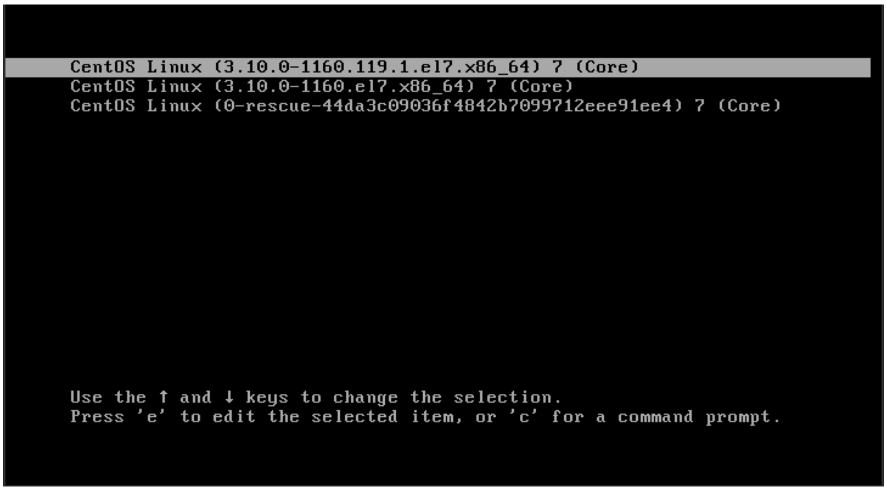
   This method does not apply to the following scenarios:

   - The ECS is experiencing lag.

  - The ECS is running EulerOS or Huawei Cloud EulerOS.

3. Enter Debug Shell mode from kernel edit mode.
   a. After the ECS is restarted, the kernel page is displayed. Press **e** to enter kernel edit mode.

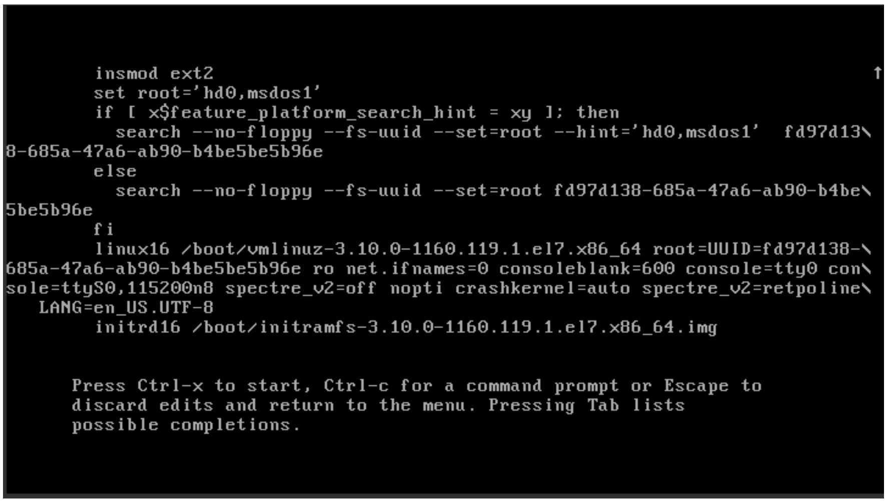
Figure 8-36 Kernel page



```
    CentOS Linux (3.10.0-1160.119.1.el7.x86_64) 7 (Core)
    CentOS Linux (3.10.0-1160.el7.x86_64) 7 (Core)
    CentOS Linux (0-rescue-44da3c09036f4842b7099712eee91ee4) 7 (Core)









    Use the ↑ and ↓ keys to change the selection.
    Press 'e' to edit the selected item, or 'c' for a command prompt.
```

   b. After entering kernel edit mode, use the arrow keys to move the cursor to the line starting with **linux**.

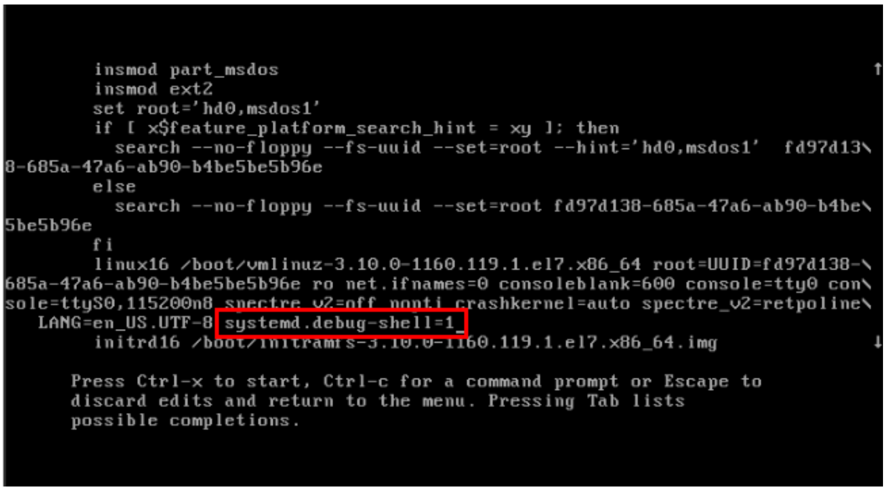
Figure 8-37 Kernel editing mode



```
        insmod ext2                                                   ↑
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  fd97d13\
8-685a-47a6-ab90-b4be5be5b96e
        else
          search --no-floppy --fs-uuid --set=root fd97d138-685a-47a6-ab90-b4be\
5be5b96e
        fi
        linux16 /boot/vmlinuz-3.10.0-1160.119.1.el7.x86_64 root=UUID=fd97d138-\
685a-47a6-ab90-b4be5be5b96e ro net.ifnames=0 consoleblank=600 console=tty0 con\
sole=ttyS0,115200n8 spectre_v2=off nopti crashkernel=auto spectre_v2=retpoline\
   LANG=en_US.UTF-8
        initrd16 /boot/initramfs-3.10.0-1160.119.1.el7.x86_64.img


      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

   c. Add **systemd.debug-shell=1** to the end of the line starting with **linux**.

Figure 8-38 Modifying the startup permissions

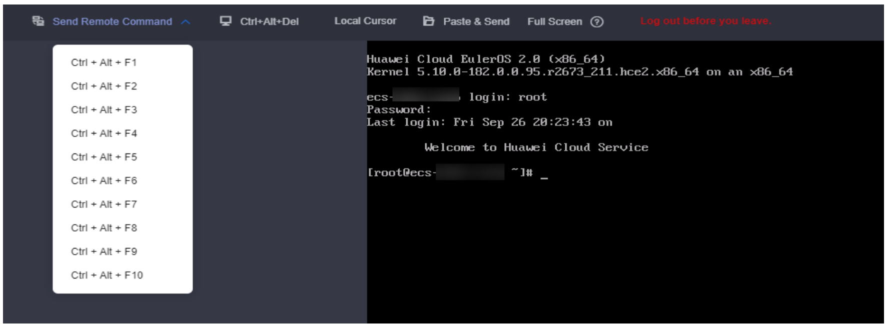


```
        insmod part_msdos                                                        ↑
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  fd97d13\
8-685a-47a6-ab90-b4be5be5b96e
        else
          search --no-floppy --fs-uuid --set=root fd97d138-685a-47a6-ab90-b4be\
5be5b96e
        fi
        linux16 /boot/vmlinuz-3.10.0-1160.119.1.el7.x86_64 root=UUID=fd97d138-\
685a-47a6-ab90-b4be5be5b96e ro net.ifnames=0 consoleblank=600 console=tty0 con\
sole=ttyS0,115200n8 spectre_v2=off nopti crashkernel=auto spectre_v2=retpoline\
   LANG=en_US.UTF-8 systemd.debug-shell=1_
        initrd16 /boot/initramfs-3.10.0-1160.119.1.el7.x86_64.img                ↓

      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

d. Press **Ctrl** and **X** to start the system.

e. After starting the system, click **Ctrl + Alt + F9** from the **Send Remote Command** drop-down list in the upper left corner to enter Debug Shell mode.

Figure 8-39 Entering Debug Shell mode



```
Huawei Cloud EulerOS 2.0 (x86_64)
Kernel 5.10.0-182.0.0.95.r2673_211.hce2.x86_64 on an x86_64

ecs-[redacted] login: root
Password:
Last login: Fri Sep 26 20:23:43 on

        Welcome to Huawei Cloud Service

[root@ecs-[redacted] ~]# _
```

9 Disk Partition, Attachment, and Expansion

9.1 Why Can't I Find My Newly Purchased Data Disk After I Log In to My Windows ECS?

Symptom

After logging in to my Windows ECS, I cannot find the attached data disk.

⚠ **CAUTION**

Formatting a disk will cause data loss. Before formatting a disk, create a backup for it.

Possible Causes

- A newly added data disk has not been partitioned or initialized.
- The disk becomes offline after the ECS OS is changed or the ECS specifications are modified.

Newly Added Data Disk Has Not Been Partitioned or Initialized

A new data disk does not have partitions and file systems by default. That is why it is unavailable in **My Computer**. To resolve this issue, manually initialize the disk.

For details, see **Initialization Overview**.

Disk Becomes Offline After the ECS OS Is Changed or the ECS Specifications Are Modified

After the ECS OS is changed, data disks may become unavailable due to file system inconsistency. After the specifications of a Windows ECS are modified, data disks may be offline.

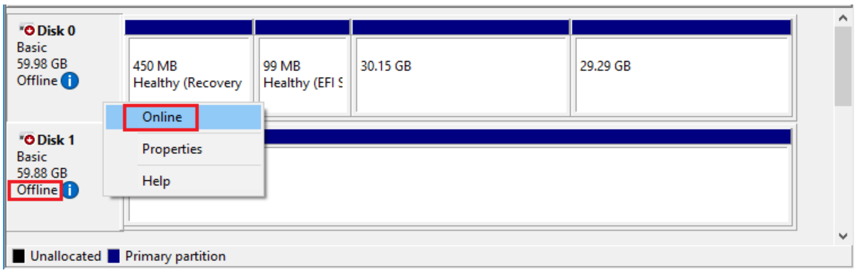
1. Log in to the ECS, open the **cmd** window, and enter **diskmgmt.msc** to switch to the **Disk Management** page.

   Check whether the affected disk is offline.

2. Set the affected disk to be online.

   In the disk list, right-click the affected disk and choose **Online** from the shortcut menu to make it online.

   Figure 9-1 Setting disk online

3. In **My Computer**, check whether the data disk is displayed properly.

   If the fault persists, initialize and partition the disk again. Before initializing the disk, create a backup for it.

9.2 How Can I Adjust System Disk Partitions?

Scenarios

If the capacity of system disk partitions is inconsistent with the actual system disk capacity after an ECS is created, you can manually adjust the partitions to expand the system disk.

There are two ways to expand a system disk:

- Consider the empty partition as a new partition and attach this partition to a directory in the root partition after formatting it. For details, see this section.
- Add the empty partition to the root partition to be expanded. For detailed operations, see the following:
  - **How Can I Add the Empty Partition of an Expanded System Disk to the End Root Partition Online?**
  - **How Can I Add the Empty Partition of an Expanded System Disk to the Non-end Root Partition Online?**

Procedure

This section uses an ECS running CentOS 7.3 64-bit as an example. A 60 GB system disk was created with the ECS. However, the capacity of the system disk partition is displayed as only 40 GB.

To use the 20 GB capacity, performing the following operations:

Step 1 View disk partitions.

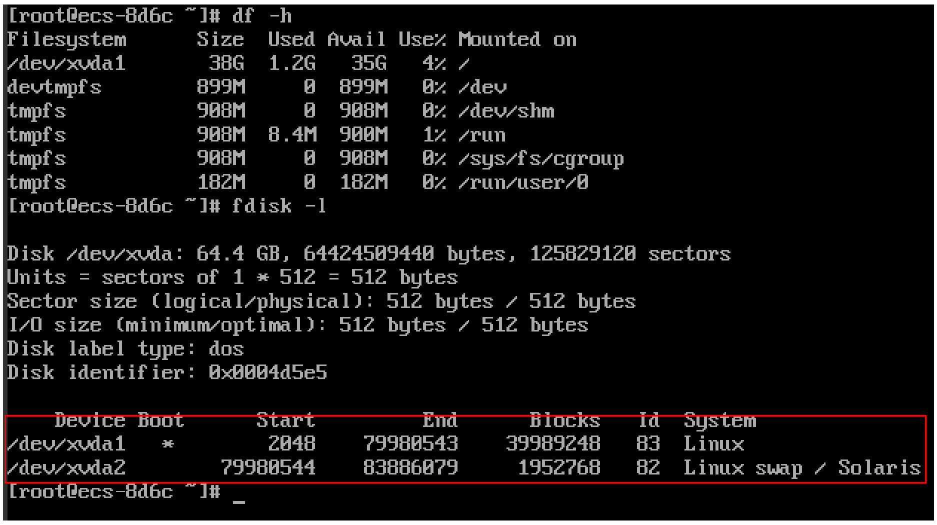
1. Log in to the ECS as user **root**.

2. Run the following command to view details about the ECS disk:

   fdisk -l

   In the following command output, **/dev/xvda** or **/dev/vda** indicates the system disk.

   Figure 9-2 Viewing details about the disk

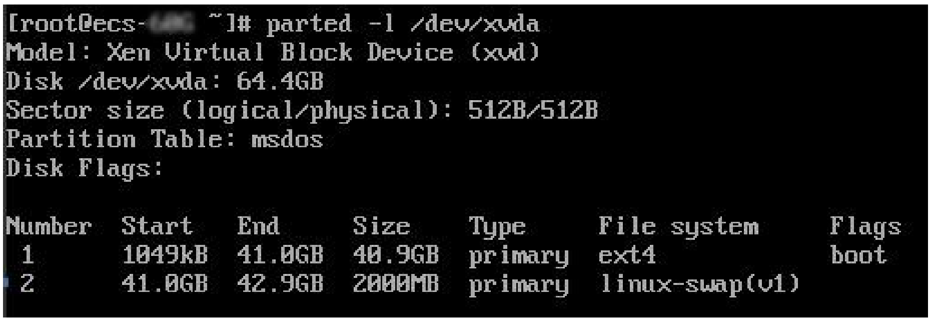


```
[root@ecs-8d6c ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       38G  1.2G   35G   4% /
devtmpfs        899M     0  899M   0% /dev
tmpfs           908M     0  908M   0% /dev/shm
tmpfs           908M  8.4M  900M   1% /run
tmpfs           908M     0  908M   0% /sys/fs/cgroup
tmpfs           182M     0  182M   0% /run/user/0
[root@ecs-8d6c ~]# fdisk -l

Disk /dev/xvda: 64.4 GB, 64424509440 bytes, 125829120 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0004d5e5

    Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *        2048    79980543    39989248   83  Linux
/dev/xvda2        79980544    83886079     1952768   82  Linux swap / Solaris
[root@ecs-8d6c ~]# _
```

3. Run the following command to view disk partitions:

   parted -l /dev/xvda

   Figure 9-3 Viewing disk partitions



```
[root@ecs-[redacted] ~]# parted -l /dev/xvda
Model: Xen Virtual Block Device (xvd)
Disk /dev/xvda: 64.4GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system     Flags
 1      1049kB  41.0GB  40.9GB  primary  ext4            boot
 2      41.0GB  42.9GB  2000MB  primary  linux-swap(v1)
```

Step 2 Create a partition for the expanded system disk capacity.

1. Run the following command to switch to the fdisk mode (taking **/dev/xvda** as an example):

   fdisk /dev/xvda

   Information similar to the following is displayed:

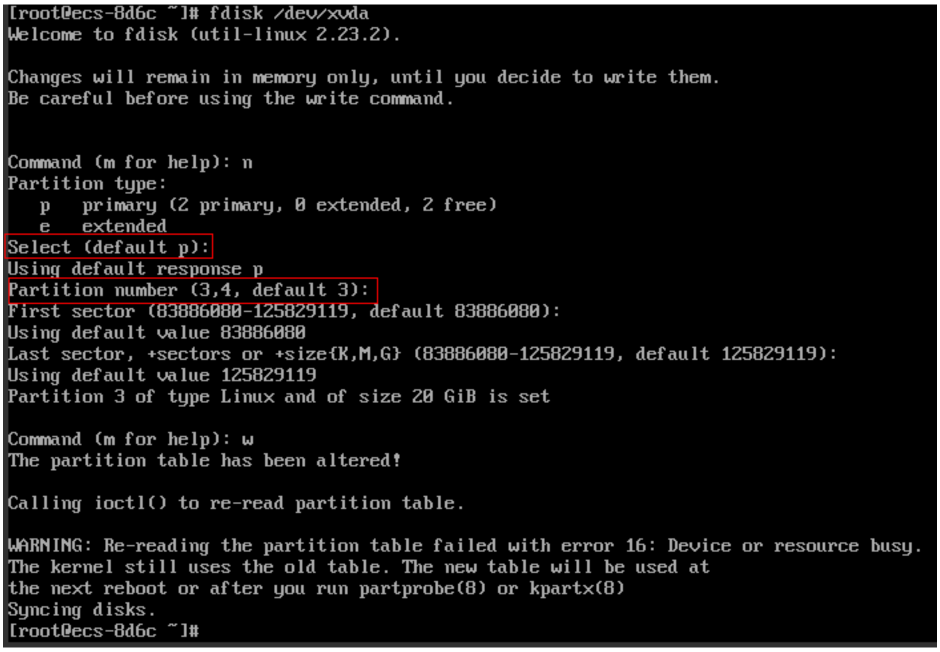
```
[root@ecs-8d6c ]# fdisk /dev/xvda
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help):
```

2. Enter **n** and press **Enter** to create a new partition.

   Because the system disk has two existing partitions, the system automatically creates the third one.

Information similar to the following is displayed.

Figure 9-4 Creating a new partition

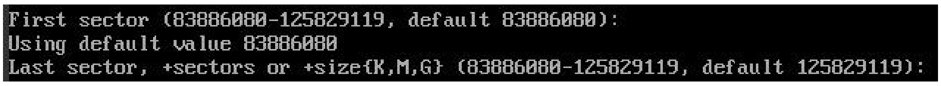


```
[root@ecs-8d6c ~]# fdisk /dev/xvda
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help): n
Partition type:
   p   primary (2 primary, 0 extended, 2 free)
   e   extended
Select (default p):
Using default response p
Partition number (3,4, default 3):
First sector (83886080-125829119, default 83886080):
Using default value 83886080
Last sector, +sectors or +size{K,M,G} (83886080-125829119, default 125829119):
Using default value 125829119
Partition 3 of type Linux and of size 20 GiB is set

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
[root@ecs-8d6c ~]#
```

3. Enter the new partition's start cylinder number and press **Enter**.

   The start cylinder number must be greater than the end cylinder numbers of existing partitions. In this example, use the default value for the new partition's start cylinder number and press **Enter**. Information similar to the following is displayed.

   Figure 9-5 Specifying the new partition's start cylinder number

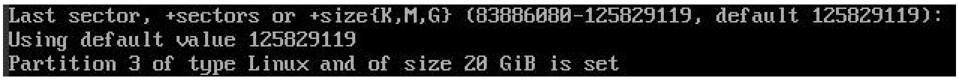
   

   ```
   First sector (83886080-125829119, default 83886080):
   Using default value 83886080
   Last sector, +sectors or +size{K,M,G} (83886080-125829119, default 125829119):
   ```

4. Enter the new partition's end cylinder number and press **Enter**.

   In this example, use the default value for the new partition's end cylinder number and press **Enter**. Information similar to the following is displayed.

   Figure 9-6 Specifying the new partition's end cylinder number

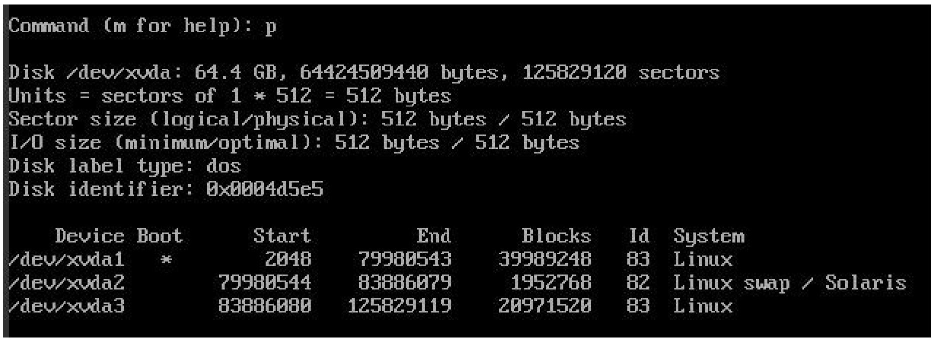
   

   ```
   Last sector, +sectors or +size{K,M,G} (83886080-125829119, default 125829119):
   Using default value 125829119
   Partition 3 of type Linux and of size 20 GiB is set
   ```

5. Enter **p** and press **Enter** to view the created partition.

   Information similar to the following is displayed.

Figure 9-7 Viewing the created partition



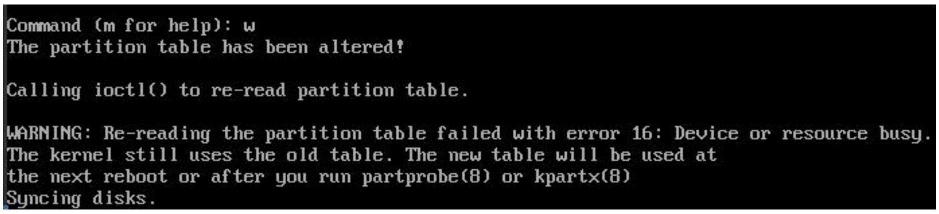
```
Command (m for help): p

Disk /dev/xvda: 64.4 GB, 64424509440 bytes, 125829120 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0004d5e5

    Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *        2048    79980543    39989248   83  Linux
/dev/xvda2        79980544    83886079     1952768   82  Linux swap / Solaris
/dev/xvda3        83886080   125829119    20971520   83  Linux
```

6. Enter **w** and press **Enter**. The system saves and exits the partition.

   The system automatically writes the partition result into the partition list. Then, the partition is created.

   Information similar to the following is displayed.

Figure 9-8 Completing the partition creation

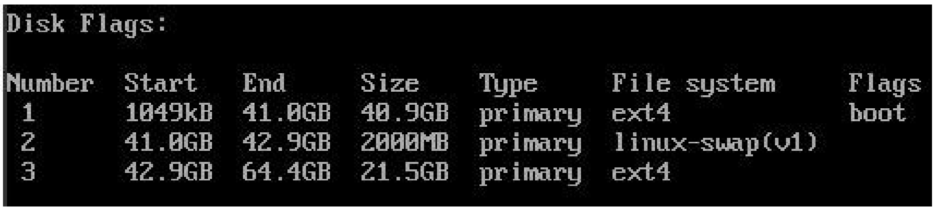


```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

7. Run the following command to view disk partitions:

   parted -l /dev/xvda

Figure 9-9 Viewing disk partitions



```
Disk Flags:

Number  Start   End     Size    Type     File system     Flags
 1      1049kB  41.0GB  40.9GB  primary  ext4            boot
 2      41.0GB  42.9GB  2000MB  primary  linux-swap(v1)
 3      42.9GB  64.4GB  21.5GB  primary  ext4
```

Step 3 Run the following command to synchronize the modifications in the partition list with the OS:

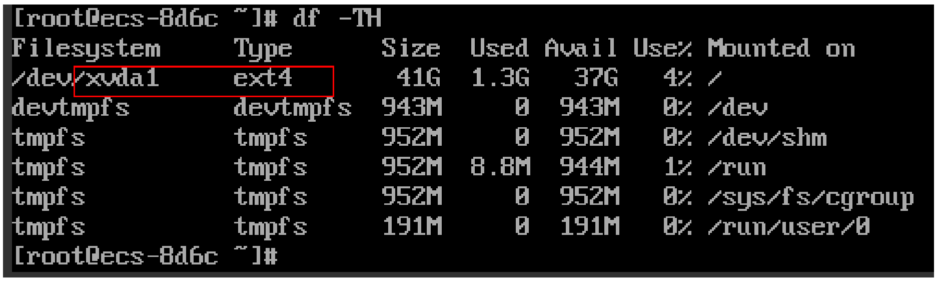
partprobe

Step 4 Configure the type of the new partition file system.

1. Run the following command to view the type of the file system:

   df -TH

Figure 9-10 Viewing the file system type



```
[root@ecs-8d6c ~]# df -TH
Filesystem     Type      Size  Used Avail Use% Mounted on
/dev/xvda1     ext4       41G  1.3G   37G   4% /
devtmpfs       devtmpfs  943M     0  943M   0% /dev
tmpfs          tmpfs     952M     0  952M   0% /dev/shm
tmpfs          tmpfs     952M  8.8M  944M   1% /run
tmpfs          tmpfs     952M     0  952M   0% /sys/fs/cgroup
tmpfs          tmpfs     191M     0  191M   0% /run/user/0
[root@ecs-8d6c ~]#
```

2. Run the following command to format the partition (taking the **ext4** type as an example):

   mkfs -t ext4 /dev/xvda3

   NOTE

   Formatting the partition requires a period of time. During this time, observe the system running status and do not exit the system.

   Information similar to the following is displayed:

```
[root@ecs-86dc ]# mkfs -t ext4 /dev/xvda3
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
1790544 inodes, 7156992 blocks
357849 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2155872256
219 block groups
32768 blocks per group, 32768 fragments per group
8176 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Step 5 Mount the new partition to the target directory.

If you mount the new partition to a directory that is not empty, the subdirectories and files in the directory will be hidden. It is a good practice to mount the new partition to an empty directory or a newly created directory. If you want to mount the new partition to a directory that is not empty, temporarily move the subdirectories and files in the directory to another directory. After the partition is mounted, move the subdirectories and files back.

Take the newly created directory **/root/new** as an example.

1. Run the following command to create the **/root/new** directory:

   mkdir /root/new

2. Run the following command to mount the new partition to the **/root/new** directory:

   mount /dev/xvda3 /root/new

   Information similar to the following is displayed:

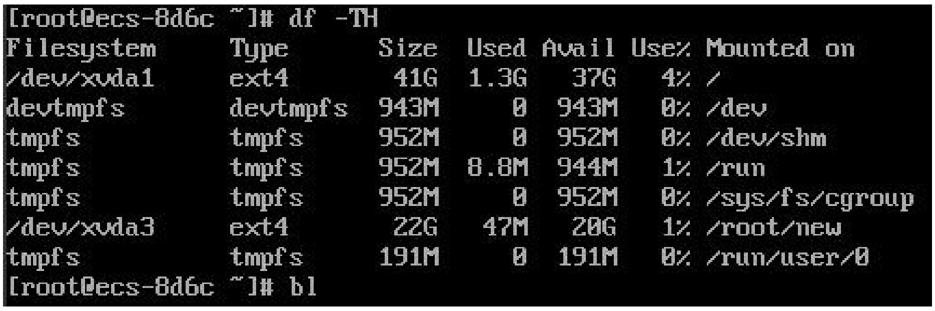
```
[root@ecs-86dc ]# mount /dev/xvda3 /root/new
[root@ecs-86dc ]#
```

3. Run the following command to view the mounted file systems:

   df -TH

   Information similar to the following is displayed:

   Figure 9-11 Viewing the mounted file systems



```
[root@ecs-8d6c ~]# df -TH
Filesystem     Type      Size  Used Avail Use% Mounted on
/dev/xvda1     ext4       41G  1.3G   37G   4% /
devtmpfs       devtmpfs  943M     0  943M   0% /dev
tmpfs          tmpfs     952M     0  952M   0% /dev/shm
tmpfs          tmpfs     952M  8.8M  944M   1% /run
tmpfs          tmpfs     952M     0  952M   0% /sys/fs/cgroup
/dev/xvda3     ext4       22G   47M   20G   1% /root/new
tmpfs          tmpfs     191M     0  191M   0% /run/user/0
[root@ecs-8d6c ~]# bl
```

Step 6 Determine whether to set automatic mounting upon system startup for the new disk.

If you do not set automatic mounting upon system startup, you must mount the new partition to the specified directory again after the ECS is restarted.

- If automatic mounting is required, go to step **Step 7**.
- If automatic mounting is not required, no further action is required.

Step 7 Set automatic mounting upon system startup for the new disk.

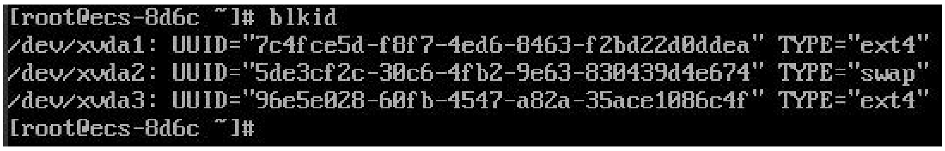
NOTE

Do not set automatic mounting upon system startup for unformatted disks because this will cause ECS startup failures.

1. Run the following command to obtain the file system type and UUID:

   blkid

   Figure 9-12 Viewing the file system type



```
[root@ecs-8d6c ~]# blkid
/dev/xvda1: UUID="7c4fce5d-f8f7-4ed6-8463-f2bd22d0ddea" TYPE="ext4"
/dev/xvda2: UUID="5de3cf2c-30c6-4fb2-9e63-830439d4e674" TYPE="swap"
/dev/xvda3: UUID="96e5e028-60fb-4547-a82a-35ace1086c4f" TYPE="ext4"
[root@ecs-8d6c ~]#
```

   According to the preceding figure, the UUID of the new partition is 96e5e028-b0fb-4547-a82a-35ace1086c4f.

2. Run the following command to open the **fstab** file using the vi editor:

   vi /etc/fstab

3. Press **i** to enter editing mode.
4. Move the cursor to the end of the file and press **Enter**. Then, add the following information:

   UUID=96e5e028-b0fb-4547-a82a-35ace1086c4f /root/new ext4 defaults 0 0

5. Press **Esc**, run the following command, and press **Enter**. The system saves the configurations and exits the vi editor.

   ```
   :wq
   ```

NOTE

If you want to detach a new disk for which automatic mounting upon system startup has been set, you must delete the automatic mounting configuration before you detach the disk. Otherwise, the ECS cannot be started after you detach the disk. To delete the automatic mounting configuration, perform the following operations:

1. Run the following command to open the **fstab** file using the vi editor:

   ```
   vi /etc/fstab
   ```

2. Press **i** to enter editing mode.
3. Delete the following statement:

   ```
   UUID=96e5e028-b0fb-4547-a82a-35ace1086c4f /root/new ext4 defaults 0 0
   ```

4. Press **Esc**, run the following command, and press **Enter**. The system saves the configurations and exits the vi editor.

   ```
   :wq
   ```

----End

9.3 How Do I Obtain My Disk Device Name in the ECS OS Using the Device Identifier Provided on the Console?

Scenarios

You find that the device name displayed in the ECS OS is different from that displayed on the management console and you cannot determine which disk name is correct. This section describes how to obtain the disk name used in an ECS OS according to the device identifier on the console.

For details about how to attach disks, see **Attaching a Disk to an ECS**.

Obtaining the Disk ID of an ECS on the Console

1. Log in to the **management console**.
2. Choose **Compute** > **Elastic Cloud Server**.
3. Click the target ECS name in the ECS list.

   The ECS details page is displayed.

4. Click the **Disks** tab and then click ⌄ to expand the disk information.
5. Check the device type and ID of the disk.

   NOTE

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

   - KVM ECS

  - If **Device Type** is **VBD**, use a serial number or BDF to obtain the disk device name. (Kunpeng ECSs only support serial numbers to obtain disk device names.)

    If you use a serial number (recommended) to obtain the disk device name, see **Using a Serial Number to Obtain the Disk Device Name (Windows)** and **Using a Serial Number to Obtain a Disk Device Name (Linux)**.

    If you use a BDF to obtain the disk device name, see **Using a BDF to Obtain a Disk Device Name (Linux)**. (BDF cannot be used to obtain the disk device name of Windows ECSs.)

  - If **Device Type** is **SCSI**, use a WWN to obtain the disk device name. For details, see **Using a WWN to Obtain the Disk Name (Windows)** and **Using a WWN to Obtain a Disk Device Name (Linux)**.

- QingTian ECS

  For QingTian ECSs such as C7 or M7 series, the **Device Type** is **VBD** or **SCSI**, and the device ID is **WWN**. You can use the WWN to obtain the disk device name of the ECS. For details, see **Using a WWN to Obtain the Disk Name (Windows)** and **Using a WWN to Obtain a Disk Device Name (Linux)**.

- Xen ECS

  - For details, see **Obtaining the Disk Device Name of a Xen Instance**.

Using a Serial Number to Obtain the Disk Device Name (Windows)

If a serial number is displayed on the console, use either of the following methods to obtain the disk name.

cmd

1. Start **cmd** in a Windows OS as an administrator and run either of the following commands:

   wmic diskdrive get serialnumber

   wmic path win32_physicalmedia get SerialNumber

   wmic path Win32_DiskDrive get SerialNumber

   NOTE

   A serial number is the first 20 digits of a disk UUID.

   For example, if the serial number of a VBD disk on the console is 97c876c0-54b3-460a-b, run either of the following commands to obtain the serial number of the disk on the ECS OS:

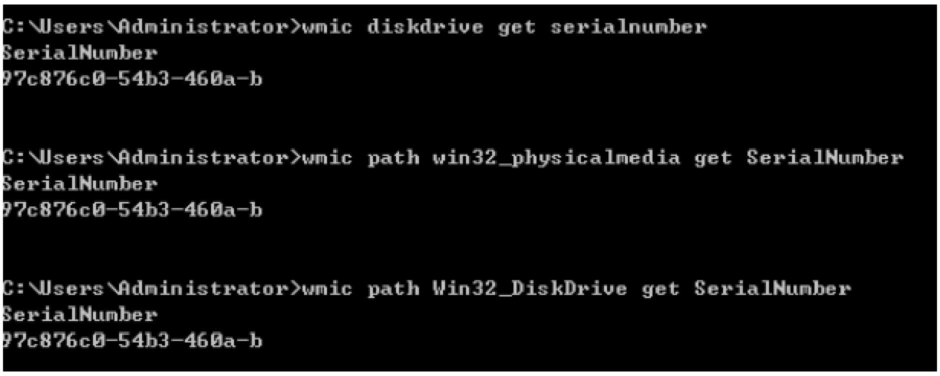
   wmic diskdrive get serialnumber

   wmic path win32_physicalmedia get SerialNumber

   wmic path Win32_DiskDrive get SerialNumber

   The following information is displayed.

Figure 9-13 Obtaining the disk serial number

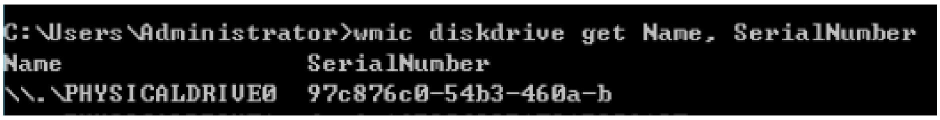


```
C:\Users\Administrator>wmic diskdrive get serialnumber
SerialNumber
97c876c0-54b3-460a-b


C:\Users\Administrator>wmic path win32_physicalmedia get SerialNumber
SerialNumber
97c876c0-54b3-460a-b


C:\Users\Administrator>wmic path Win32_DiskDrive get SerialNumber
SerialNumber
97c876c0-54b3-460a-b
```

2. Run the following command to check the disk corresponding to the serial number:

   wmic diskdrive get Name, SerialNumber

Figure 9-14 Checking the disk corresponding to the serial number



```
C:\Users\Administrator>wmic diskdrive get Name, SerialNumber
Name                    SerialNumber
\\.\PHYSICALDRIVE0      97c876c0-54b3-460a-b
```

PowerShell

1. Start PowerShell as an administrator in a Windows OS.
2. Run the following command to check the disk on which the logical disk is created:
   - Windows Server 2012 or later
     i. Run the following command to check the disk on which the logical disk is created:

        Get-CimInstance -ClassName Win32_LogicalDiskToPartition | select Antecedent, Dependent |fl

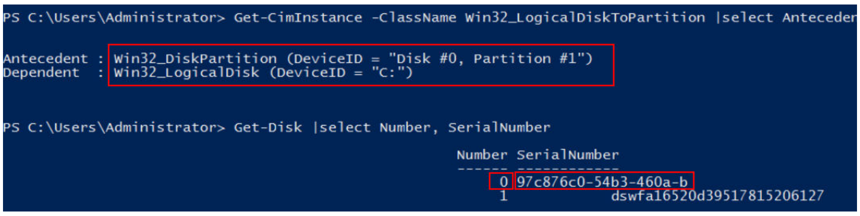
        As shown in **Figure 9-15**, the disk is **Disk 0**.

     ii. Run the following command to view the mapping between the serial number and the disk:

        Get-Disk |select Number, SerialNumber

        As shown in **Figure 9-15**, the disk is **Disk 0**.

Figure 9-15 Viewing the disk on which the logical disk is created



```
PS C:\Users\Administrator> Get-CimInstance -ClassName Win32_LogicalDiskToPartition |select Anteceder

Antecedent : Win32_DiskPartition (DeviceID = "Disk #0, Partition #1")
Dependent  : Win32_LogicalDisk (DeviceID = "C:")


PS C:\Users\Administrator> Get-Disk |select Number, SerialNumber

                                                    Number SerialNumber
                                                    ------ ------------
                                                         0 97c876c0-54b3-460a-b
                                                         1           dswfa16520d39517815206127
```

   - Versions earlier than Windows 2012
     i. Run the following command to check the disk on which the logical disk is created:

   Get-WmiObject -Class Win32_PhysicalMedia |select Tag, Serialnumber

ii. Run the following command to view the mapping between the serial number and the disk:

   Get-WmiObject -Class Win32_LogicalDiskToPartition |select Antecedent, Dependent |fl

Using a Serial Number to Obtain a Disk Device Name (Linux)

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

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

ll /dev/disk/by-id/*

NOTE

A serial number is the first 20 digits of a disk UUID.

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/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
```

/dev/vdb is the disk device name.

Using a BDF to Obtain a Disk Device Name (Linux)

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
   ```

   /dev/vdb is the disk device name.

Using a WWN to Obtain the Disk Name (Windows)

1. Obtain the device identifier on the console by referring to **Obtaining the Disk ID of an ECS on the Console**.
2. Manually convert the WWN.

For example, the obtained WWN (device identifier) is 688860300003**3252f**fa16520d39517815.

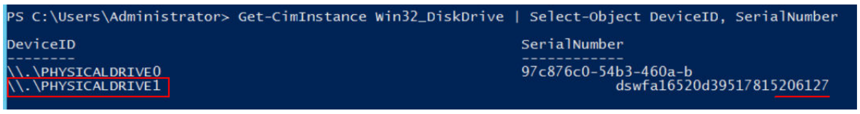
a. Obtain the 21st to 17th digits that are counted backwards (**3252f**).

b. Convert a hexadecimal (**3252f**) to a decimal (**206127**).

3. Start PowerShell as an administrator in a Windows OS.
4. Run the following command:

   Get-CimInstance Win32_DiskDrive | Select-Object DeviceID, SerialNumber
5. In the command output, the disk whose serial number ends with **206127** is the disk corresponding to the WWN.

Figure 9-16 Disk with the serial number ending with **206127**



```
PS C:\Users\Administrator> Get-CimInstance Win32_DiskDrive | Select-Object DeviceID, SerialNumber

DeviceID                                                SerialNumber
--------                                                ------------
\\.\PHYSICALDRIVE0                                      97c876c0-54b3-460a-b
\\.\PHYSICALDRIVE1                                                dswfa16520d39517815206127
```

Using a WWN to Obtain a Disk Device Name (Linux)

1. Log in to the ECS 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 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
lrwxrwxrwx 1 root root  9 May 21 20:22 scsi-36888603000008b32fa16688d09368506 -> ../../sda
```

Obtaining the Disk Device Name of a Xen Instance

Step 1 Obtain the disk information displayed on the console.

1. Log in to the **management console**.
2. Choose **Compute** > **Elastic Cloud Server**.
3. Click the target ECS name in the ECS list.

   The ECS details page is displayed.
4. Click the **Disks** tab and then click ⌄ to expand the disk information.
5. Check the device name, type, and ID of the disk.
   - If the device type is **VBD**, go to step **Step 2**.
   - If the device type is **SCSI**, go to step **Step 3**.

NOTE

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

Step 2 Check the device name attached to the VBD disk in the ECS.

For a VBD disk, the device name displayed on the management console corresponds to the disk device name in the ECS OS. For details, see **Table 9-1**.

Table 9-1 Mapping between disk device names displayed on the management console and those obtained on the ECS

Device Name (on Management Console)	Device Name (in ECS)
/dev/sd***	/dev/xvd***
/dev/vd***	/dev/xvd***
/dev/xvd***	/dev/xvd***

An example is provided as follows:

If the device name displayed on the management console is **/dev/sdb**, the device name of the device attached to the ECS is **/dev/xvdb**.

Step 3 Check the device name of the SCSI disk attached to the ECS.

1. Obtain the disk device ID.

   The device ID of the SCSI disk is the disk WWN on the ECS.
2. Log in to the ECS as user **root**.
3. Run the following command to view the disk device name:

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

   ```
   [root@host-192-168-133-148 block]# ll /dev/disk/by-id/ |grep 6888603000008b32fa16688d09368506 |
   grep scsi-3
   lrwxrwxrwx 1 root root  9 May 21 20:22 scsi-36888603000008b32fa16688d09368506 -> ../../sda
   ```

----End

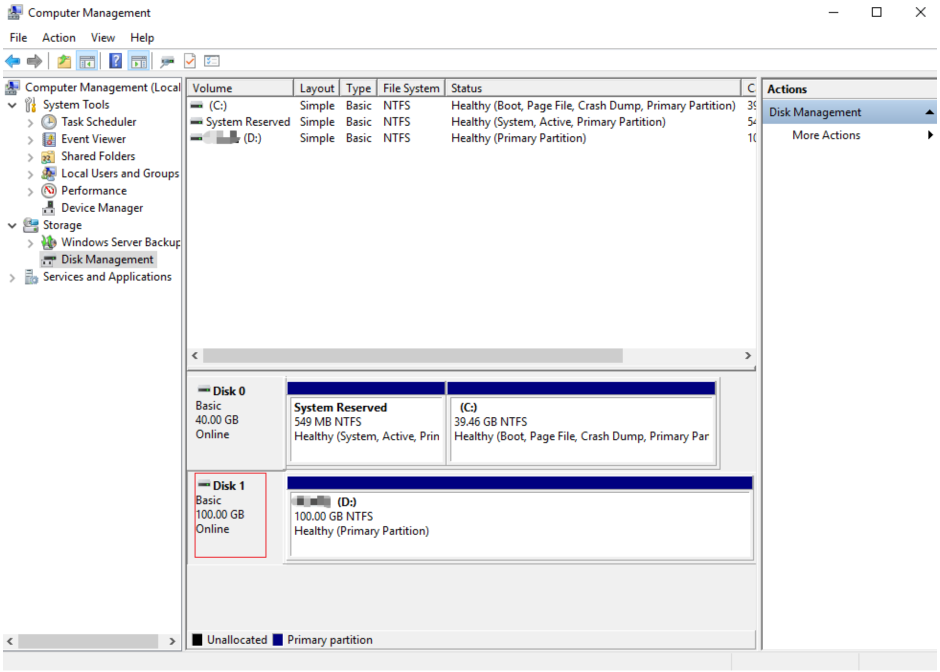
9.4 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Windows ECS?

This section uses an ECS running Windows Server 2019 64-bit as an example to describe how to obtain the mapping between disk partitions and disk devices.

For KVM or QingTian instances, see **How Do I Obtain My Disk Device Name in the ECS OS Using the Device Identifier Provided on the Console?**

1. Log in to the Windows ECS.
2. Click **Start** in the lower left corner of the desktop.
3. Choose **Control Panel** > **Administrative Tools** > **Computer Management**.
4. In the navigation pane on the left, choose **Storage** > **Disk Management**.

Figure 9-17 Disk Management

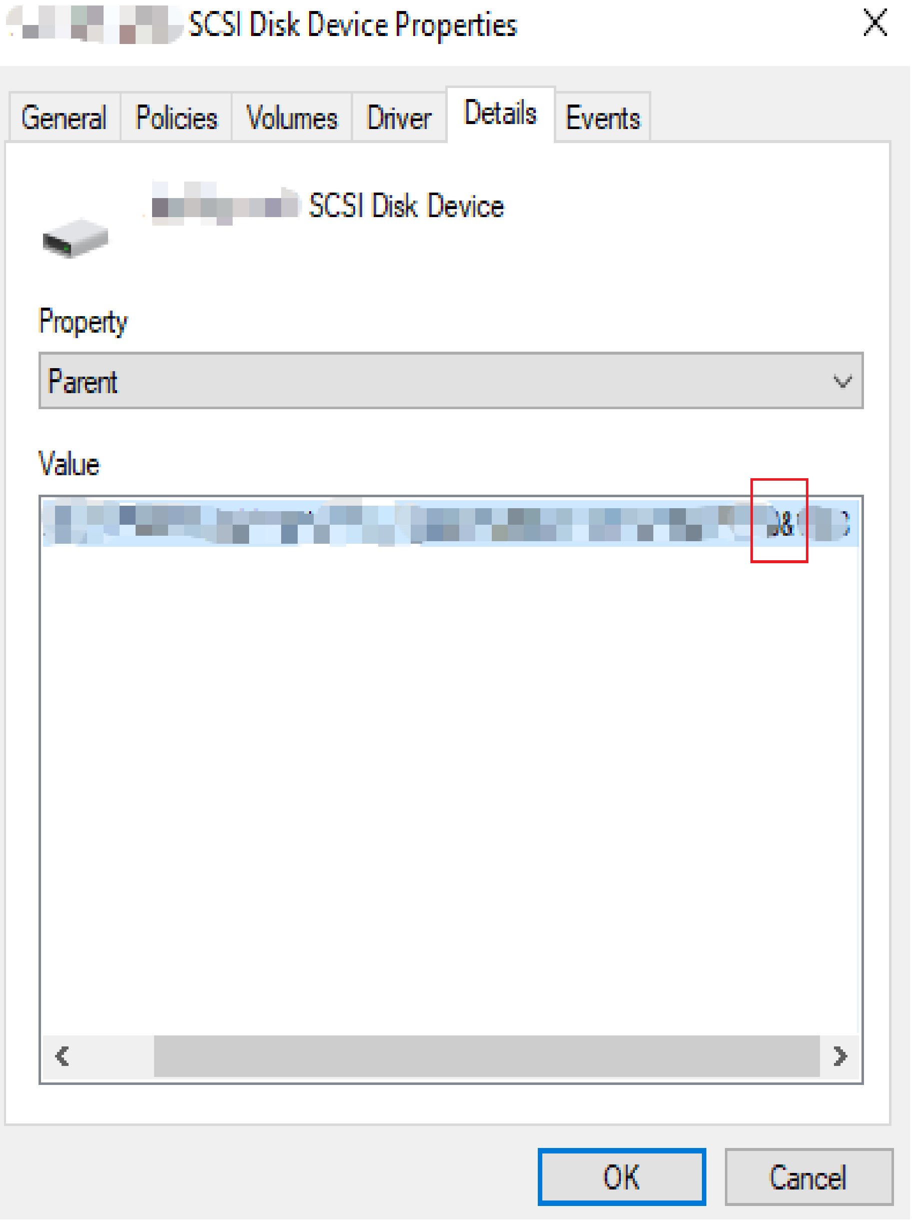


Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)
(D:)	Simple	Basic	NTFS	Healthy (Primary Partition)

5. Taking disk 1 marked in **Figure 9-17** as an example, view the disk device for disk 1.
   a. Right-click the gray area where disk 1 is located, as shown in the red box in **Figure 9-17**.
   b. Click **Properties**.

      The **SCSI Disk Device Properties** dialog box is displayed.
   c. Click the **Details** tab and set **Property** to **Parent**.

Figure 9-18 Disk device details



d. Record the digits following **&** in the parameter value, for example, **51776**, which is the primary/secondary device number corresponding to the disk partition.

e. Obtain the disk device according to the information listed in **Table 9-2**.

The disk device corresponding to **51776** is **xvde**. The disk device used by disk 1 is xvde.

Table 9-2 Mapping between disk partitions and disk devices

Primary/Secondary Device Number for a Disk Partition	Disk Device
51712	xvda

Primary/Secondary Device Number for a Disk Partition	Disk Device
51728	xvdb
51744	xvdc
51760	xvdd
51776	xvde
51792	xvdf
51808	xvdg
51824	xvdh
51840	xvdi
51856	xvdj
51872	xvdk
51888	xvdl
51904	xvdm
51920	xvdn
51936	xvdo
51952	xvdp
268439552	xvdq
268439808	xvdr
268440064	xvds
268440320	xvdt
268440576	xvdu
268440832	xvdv
268441088	xvdw
268441344	xvdx

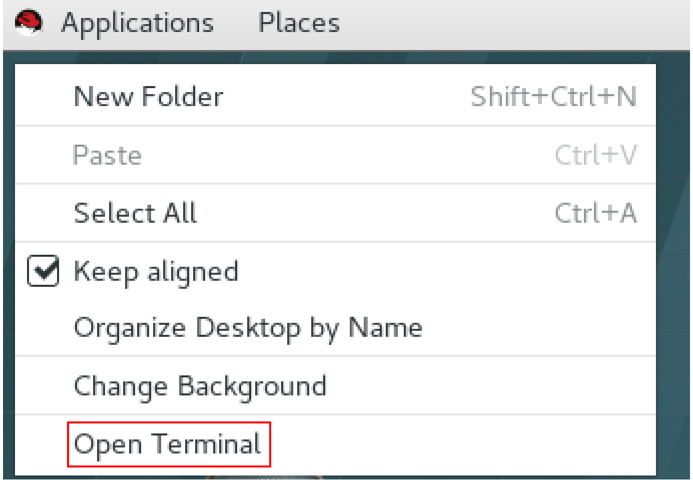
9.5 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Linux ECS?

For a Xen ECS running Linux, its disk partitions correspond to disk devices. This section uses a Linux ECS running Red Hat Enterprise Linux 7 as an example to describe how to obtain the mapping between disk partitions and disk devices.

For KVM or QingTian instances, see **How Do I Obtain My Disk Device Name in the ECS OS Using the Device Identifier Provided on the Console?**

1. Log in to the Linux ECS running Red Hat Enterprise Linux 7 as user **root**.
2. Right-click in the blank area of the desktop and choose **Open Terminal** from the shortcut menu.

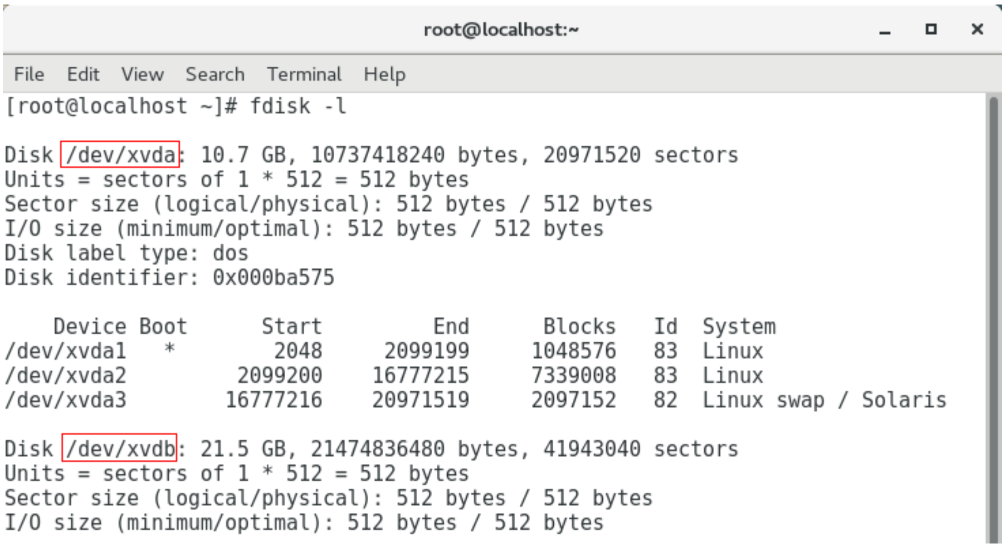
Figure 9-19 open terminal



3. Run the following command to view disk partitions and disk devices:

   fdisk -l

Figure 9-20 Viewing disk partitions and disk devices



```
[root@localhost ~]# fdisk -l

Disk /dev/xvda: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000ba575

    Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *        2048     2099199     1048576   83  Linux
/dev/xvda2         2099200    16777215     7339008   83  Linux
/dev/xvda3        16777216    20971519     2097152   82  Linux swap / Solaris

Disk /dev/xvdb: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Table 9-3 lists the mapping between disk partitions and disk devices.

Table 9-3 Mapping between disk partitions and disk devices

Disk Partition	Disk Device
xvda	xvda

Disk Partition	Disk Device
xvdb	xvdb
xvdc	xvdc
xvdd	xvdd
xvde	xvde
xvdf	xvdf
xvdg	xvdg
xvdh	xvdh
xvdi	xvdi
xvdj	xvdj
xvdk	xvdk
xvdl	xvdl
xvdm	xvdm
xvdn	xvdn
xvdo	xvdo
xvdp	xvdp
xvdq	xvdq
xvdr	xvdr
xvds	xvds
xvdt	xvdt
xvdu	xvdu
xvdv	xvdv
xvdw	xvdw
xvdx	xvdx

9.6 How Can I Enable Virtual Memory on a Windows ECS?

Enabling ECS virtual memory will deteriorate I/O performance. If the ECS memory is insufficient, increase the memory by performing the operations in **Modifying Individual ECS Specifications**. If you really need to enable virtual memory, see the operations described below.

NOTE

If the memory usage is excessively high and the I/O performance is not as good as expected, you are not advised to enable virtual memory. The reason is as follows: The excessively high memory usage limits the system performance improvement. Furthermore, frequent memory switching requires massive additional I/O operations, which will further deteriorate the I/O performance and the overall system performance.

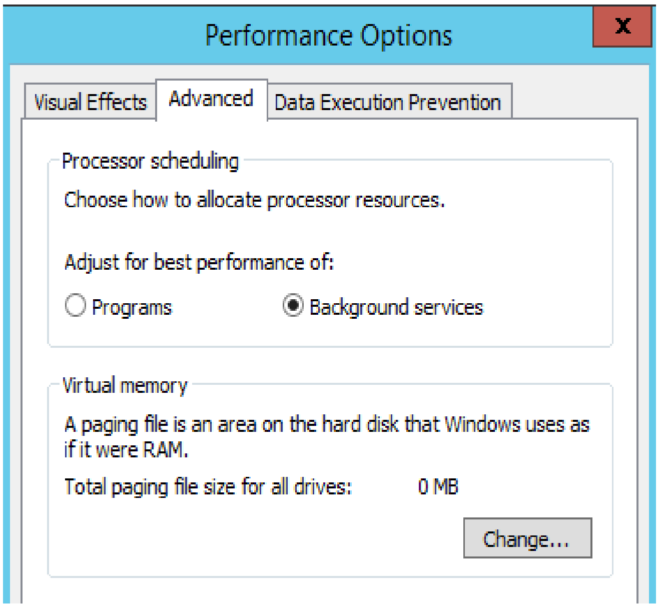
The operations described in this section apply to ECSs running Windows Server 2008 or later.

1. Right-click **Computer** and choose **Properties** from the shortcut menu.
2. In the left navigation pane, choose **Advanced system settings**.

   The **System Properties** dialog box is displayed.
3. Click the **Advanced** tab and then **Settings** in the **Performance** pane.

   The **Performance Options** dialog box is displayed.

Figure 9-21 Performance Options



Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

○ Programs ● Background services

Virtual memory

A paging file is an area on the hard disk that Windows uses as if it were RAM.

Total paging file size for all drives: 0 MB

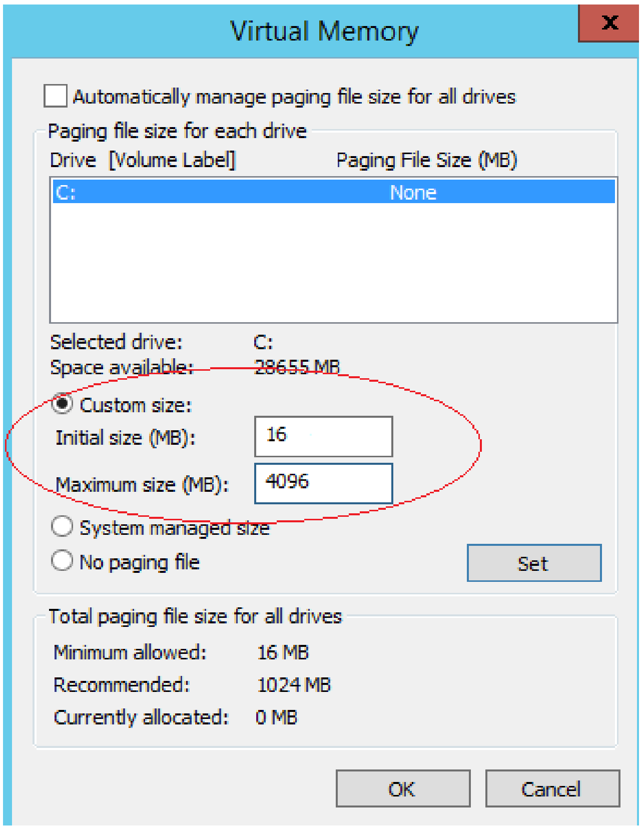
4. Click the **Advanced** tab and then **Background Services** in the **Processor scheduling** pane.
5. Click **Change** in the **Virtual memory** pane.

   The **Virtual Memory** dialog box is displayed.
6. Configure virtual memory based on service requirements.
   - **Automatically manage paging file size for all drives**: Deselect the checkbox.
   - **Drive**: Select the drive where the virtual memory file is stored.

     You are advised not to select the system disk to store the virtual memory.
   - **Custom size**: Select **Custom size** and set **Initial size** and **Maximum size**.

     Considering **Memory.dmp** caused by blue screen of death (BSOD), you are advised to set **Initial size** to **16** and **Maximum size** to **4096**.

Figure 9-22 Virtual Memory



Virtual Memory

☐ Automatically manage paging file size for all drives

Paging file size for each drive

Drive [Volume Label]	Paging File Size (MB)
C:	None

Selected drive: C:
Space available: 28655 MB

● Custom size:
Initial size (MB): 16
Maximum size (MB): 4096

○ System managed size
○ No paging file

Total paging file size for all drives
Minimum allowed: 16 MB
Recommended: 1024 MB
Currently allocated: 0 MB

7. Click **Set** and then **OK** to complete the configuration.
8. Restart the ECS for the configuration to take effect.

9.7 How Can I Add the Empty Partition of an Expanded System Disk to the End Root Partition Online?

Scenarios

If the capacity of system disk partitions is inconsistent with the actual system disk capacity after an ECS is created, you can add the empty partition to the root partition of the system disk.

This section describes how to add the empty partition to the end root partition online.

Procedure

In the following operations, the ECS that runs CentOS 6.5 64bit and has a 50 GB system disk is used as an example. The system disk has two partitions, **/dev/xvda1: swap** and **/dev/xvda2: root**, and the root partition is the end partition.

1. Run the following command to view disk partitions:

   parted -l /dev/xvda

```
[root@sluo-ecs-5e7d ~]# parted -l /dev/xvda
Disk /dev/xvda: 53.7GB
```

```
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start   End     Size    Type     File system     Flags
 1      1049kB  4296MB  4295MB  primary  linux-swap(v1)
 2      4296MB  42.9GB  38.7GB  primary  ext4            boot
```

2. Run the following command to obtain the file system type and UUID:

   blkid

```
/dev/xvda1: UUID="25ec3bdb-ba24-4561-bcdc-802edf42b85f" TYPE="swap"
/dev/xvda2: UUID="1a1ce4de-e56a-4e1f-864d-31b7d9dfb547" TYPE="ext4"
```

3. Run the following command to install the growpart tool:

   This tool may be integrated in the **cloud-utils-growpart/cloud-utils/cloud-initramfs-tools/cloud-init** package. Run the **yum install cloud-*** command to ensure it is available.

   yum install cloud-utils-growpart

4. Run the following command to expand the root partition (the second partition) using growpart:

   growpart /dev/xvda 2

```
[root@sluo-ecs-5e7d ~]# growpart /dev/xvda 2
CHANGED: partition=2 start=8390656 old: size=75495424 end=83886080 new: 
size=96465599,end=104856255
```

5. Run the following command to verify that online capacity expansion is successful:

   parted -l /dev/xvda

```
[root@sluo-ecs-5e7d ~]# parted -l /dev/xvda
Disk /dev/xvda: 53.7GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start   End     Size    Type     File system     Flags
 1      1049kB  4296MB  4295MB  primary  linux-swap(v1)
 2      4296MB  53.7GB  49.4GB  primary  ext4            boot
```

6. Run the following command to expand the capacity of the file system:

   resize2fs -f *$Partition name*

   Suppose the partition name is **/dev/xvda2**, run the following command:

```
[root@sluo-ecs-a611 ~]# resize2fs -f /dev/xvda2
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/xvda2 is mounted on /; on-line resizing required
old_desc_blocks = 3, new_desc_blocks = 3
....
[root@sluo-ecs-a611 ~] # df -hT    //Check file system capacity expansion
```

9.8 How Can I Add the Empty Partition of an Expanded System Disk to the Non-end Root Partition Online?

Scenarios

If the capacity of system disk partitions is inconsistent with the actual system disk capacity after an ECS is created, you can add the empty partition to the root partition of the system disk.

This section describes how to add the empty partition to the non-end root partition online.

Procedure

In the following operations, the ECS that runs CentOS 6.5 64bit and has a 100 GB system disk is used as an example. The system disk has two partitions, **/dev/xvda1: root** and **/dev/xvda2: swap**, and the root partition is not the end partition.

1. Run the following command to view disk partitions:

   parted -l /dev/xvda

   ```
   [root@sluo-ecs-a611 ~]# parted -l /dev/xvda
   Disk /dev/xvda: 107GB
   Sector size (logical/physical): 512B/512B
   Partition Table: msdos
   Disk Flags:

   Number  Start   End     Size    Type     File system     Flags
    1      1049kB  41.0GB  40.9GB  primary  ext4            boot
    2      41.0GB  42.9GB  2000MB  primary  linux-swap(v1)
   ```

   The first is the root partition, and the second is the swap partition.

2. View and edit the fstab partition table to delete the swap partition attachment information.

   a. Run the following command to view the fstab partition table:

      tail -n 3 /etc/fstab

      ```
      [root@sluo-ecs-a611 ~]# tail -n 3 /etc/fstab
      #
      UUID=7c4fce5d-f8f7-4ed6-8463-f2bd22d0ddea /                       ext4    defaults        1 1
      UUID=5de3cf2c-30c6-4fb2-9e63-830439d4e674 swap                    swap    defaults        0 0
      ```

   b. Run the following command to edit the fstab partition table and delete the swap partition attachment information.

      vi /etc/fstab

      tail -n 3 /etc/fstab

      ```
      [root@sluo-ecs-a611 ~]# vi /etc/fstab
      [root@sluo-ecs-a611 ~]# tail -n 3 /etc/fstab
      #
      UUID=7c4fce5d-f8f7-4ed6-8463-f2bd22d0ddea /                       ext4    defaults        1 1
      ```

3. Run the following command to disable the swap partition:

   swapoff -a

4. Delete the swap partition.

   a. Run the following command to view the partition:

      parted /dev/xvda

      ```
      [root@sluo-ecs-a611 ~]# parted /dev/xvda
      GNU Parted 3.1
      Using /dev/xvda
      Welcome to GNU Parted! Type ´help´ to view a list of commands.
      (parted) help
        align-check TYPE N                        check partition N for TYPE(min|opt) alignment
        help [COMMAND]                           print general help, or help on COMMAND
        mklabel,mktable LABEL-TYPE               create a new disklabel (partition table)
        mkpart PART-TYPE [FS-TYPE] START END     make a partition
        name NUMBER NAME                         name partition NUMBER as NAME
        print [devices|free|list,all|NUMBER]     display the partition table, available devices, free space,
      all found partitions, or a
              particular partition
        quit                                     exit program
        rescue START END                         rescue a lost partition near START and END
        rm NUMBER                                delete partition NUMBER
        select DEVICE                            choose the device to edit
        disk_set FLAG STATE                      change the FLAG on selected device
        disk_toggle [FLAG]                       toggle the state of FLAG on selected device
      ```

```
  set NUMBER FLAG STATE                    change the FLAG on partition NUMBER
  toggle [NUMBER [FLAG]]                   toggle the state of FLAG on partition NUMBER
  unit UNIT                                set the default unit to UNIT
  version                                  display the version number and copyright information of GNU
Parted
(parted)
```

   b. Press **p**.

```
Disk /dev/xvda: 107GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system     Flags
 1      1049kB  41.0GB  40.9GB  primary  ext4            boot
 2      41.0GB  42.9GB  2000MB  primary  linux-swap(v1)

```

   c. Run the following command to delete the partition:

      rm 2

```
(parted) rm2
```

   d. Press **p**.

```
(parted) p
Disk /dev/xvda: 107GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system  Flags
 1      1049kB  41.0GB  40.9GB  primary  ext4         boot
```

   e. Run the following command to edit the fstab partition table:

      quit

```
(parted) quit
Information: You may need to update /etc/fstab.
```

5. Run the following command to view partition after the swap partition is deleted:

   parted -l /dev/xvda

```
[root@sluo-ecs-a611 ~]# parted -l /dev/xvda
Disk /dev/xvda: 107GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system  Flags
 1      1049kB  41.0GB  40.9GB  primary  ext4         boot
```

6. Run the following command to install the growpart tool:

   This tool may be integrated in the **cloud-utils-growpart/cloud-utils/cloud-initramfs-tools/cloud-init** package. Run the **yum install cloud-*** command to ensure it is available.

   yum install cloud-utils-growpart

7. Run the following command to expand the root partition (the first partition) using growpart:

   growpart /dev/xvda 1

```
[root@sluo-ecs-a611 ~]# growpart /dev/xvda 1
CHANGED: partition=1 start=2048 old: size=79978496 end=79980544 new:
size=209710462,end=209712510
```

8. Run the following command to verify that online capacity expansion is successful:

```
[root@sluo-ecs-a611 ~]# parted -l /dev/xvda
Disk /dev/xvda: 107GB
```

```
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End    Size   Type     File system  Flags
 1      1049kB  107GB  107GB  primary  ext4         boot
```

9. Run the following command to expand the capacity of the file system:

   resize2fs -f *$Partition name*

   Suppose the partition name is **/dev/xvda1**, run the following command:

```
[root@sluo-ecs-a611 ~]# resize2fs -f /dev/xvda1
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/xvda1 is mounted on /; on-line resizing required
old_desc_blocks = 3, new_desc_blocks = 3
....
[root@sluo-ecs-a611 ~] # df -hT     //Check file system capacity expansion
```

9.9 Can I Attach Multiple Disks to an ECS?

Yes. The ECSs created after the disk function upgrade can have up to 60 attached disks.

- When you create an ECS, you can attach 24 disks to it.
- After you create an ECS, you can attach up to 60 disks to it.

Table 9-4 Numbers of disks that can be attached to a newly created ECS

ECS Type	Maximum VBD Disks	Maximum SCSI Disks	Constraint
Xen	60	59	VBD disks + SCSI disks ≤ 60 (This constraint does not apply to local disks.) The number of local disks is determined based on the ECS flavor.
KVM (excluding D2 ECSs)	24	59	VBD disks + SCSI disks ≤ 60 (This constraint does not apply to local disks.) The number of local disks is determined based on the ECS flavor.
D2	24	30	VBD disks + SCSI disks ≤ 54 (This constraint does not apply to local disks.) The number of local disks is determined based on the ECS flavor.

📖 **NOTE**

- The system disk of an ECS is of VBD type. The maximum number of SCSI disks is 59.
- For a D-series KVM ECS, its local disks use two SCSI controllers, indicating that 30 SCSI drive letters are used. A maximum of 30 SCSI disks can be attached to such an ECS.

The maximum number of disks that you can attach to an ECS that was created before the disk function upgrade remains unchanged, as shown in **Table 9-5**.

Table 9-5 Numbers of disks that can be attached to an existing ECS

ECS Type	Maximum VBD Disks	Maximum SCSI Disks	Maximum Local Disks	Constraint
Xen	60	59	59	VBD disks + SCSI disks + Local disks ≤ 60
KVM	24	23	59	VBD disks + SCSI disks ≤ 24

To attach 60 disks, enable advanced disk. For details, see **Enabling Advanced Disk**.

How Can I Check Whether an ECS Is Created Before or After the Disk Function Upgrade?

1. Log in to the **management console**.
2. Under **Compute**, click **Elastic Cloud Server**.
3. Click the name of the target ECS. The page providing details about the ECS is displayed.
4. Click the **Disks** tab.
5. Check the number of disks that can be attached to the ECS to determine the total number of disks.
   - If the total number of disks that can be attached is 24 (including the system disk), the ECS is created before the disk function upgrade.
   - If the total number of disks that can be attached is 60 (including the system disk), the ECS is created after the disk function upgrade.

9.10 What Are the Requirements for Attaching an EVS Disk to an ECS?

- The EVS disk and the target ECS must be located in the same AZ.
- The target ECS must be in **Running** or **Stopped** state.
- The EVS disk must not be frozen.

- For yearly/monthly ECSs:

  If you detach the system disk that you purchased when creating an ECS and want to continue using it as a system disk, you can only attach it to the original ECS. If you want to use it as a data disk, you can attach it to any ECS.

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

9.11 Which ECSs Can Be Attached with SCSI EVS Disks?

A Xen ECS running one of the following OSs supports SCSI EVS disks:

- Windows
- SUSE Enterprise Linux Server 11 SP4 64bit
- SUSE Enterprise Linux Server 12 64bit
- SUSE Enterprise Linux Server 12 SP1 64bit
- SUSE Enterprise Linux Server 12 SP2 64bit

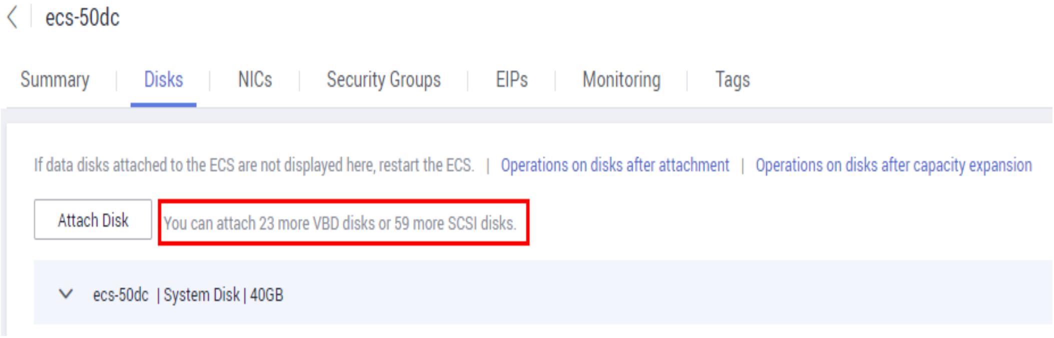
All KVM ECSs support SCSI EVS disks.

9.12 What Should I Do If Attaching a Disk to a Windows ECS Failed But There Are Still Available Device Names?

Symptom

On the Windows ECS details page, the system displays a message indicating that at most *n* more disks can be attached to the ECS. However, after you clicked **Attach Disk**, the attachment failed.

Figure 9-23 Disk attachment



ecs-50dc
Summary
Disks
NICs
Security Groups
EIPs
Monitoring
Tags
Operations on disks after attachment
Operations on disks after capacity expansion
Attach Disk

If data disks attached to the ECS are not displayed here, restart the ECS.

You can attach 23 more VBD disks or 59 more SCSI disks.

ecs-50dc | System Disk | 40GB

Possible Causes

If an EVS disk in arrears is not renewed, the system forcibly uninstalls it, which may cause a residual drive letter on the Windows ECS. As a result, the actual number of available device names on the ECS is less than the displayed number.

Solution

Restart the ECS and attach the disk again.

If the attaching still fails, contact customer service for technical support.

9.13 Why Does a Linux ECS with a SCSI Disk Attached Fails to Be Restarted?

Symptom

For a Linux ECS with a SCSI disk attached, if you have enabled automatic SCSI disk attachment upon ECS startup in **/etc/fstab** and the disk drive letter (for example, **/dev/sdb**) is used, the ECS fails to restart.

Possible Causes

SCSI disk allocation is determined based on the ID of the slot accommodating the disk as well as the available drive letter in the ECS. Each time you attach a disk to the ECS, an idle drive letter is automatically allocated in sequence. When the ECS starts, the disks are loaded in slot sequence. A slot ID corresponds to a drive letter.

After the SCSI disk is detached from the running ECS, the slot sequence for disks may change, leading to the disk drive letter being changed after the ECS is restarted. As a result, the slot IDs do not correspond to the drive letters, and the ECS fails to restart.

Solution

1. Log in to the ECS as user **root**.
2. Run the following command to obtain the SCSI ID according to the drive letter of the SCSI disk:

   ll /dev/disk/by-id/|grep *Disk drive letter*

   For example, if the drive letter of the SCSI disk is **/dev/sdb**, run the following command:

   ll /dev/disk/by-id/|grep sdb

   ```
   CNA64_22:/opt/galax/eucalyptus/ecs_scripts # ll /dev/disk/by-id/|grep sdb
   lrwxrwxrwx 1 root root  9 Dec  6 11:26 scsi-3688860300001436b005014f890338280 -> ../../sdb
   lrwxrwxrwx 1 root root  9 Dec  6 11:26 wwn-0x688860300001436b005014f890338280 -> ../../sdb
   ```

3. Change the drive letter (for example, **/dev/sdb**) of the SCSI disk to the corresponding SCSI ID in the **/etc/fstab** file.

   /dev/disk/by-id/*SCSI ID*

   For example, if the SCSI ID obtained in step 2 is scsi-3688860300001436b005014f890338280, use the following data to replace **/dev/sdb**:

   /dev/disk/by-id/scsi-3688860300001436b005014f890338280

9.14 How Can I Check Whether the ECSs Attached with the Same Shared SCSI Disk Are in the Same ECS Group?

Scenarios

Shared EVS disks of the SCSI type support SCSI locks. To improve data security, the shared EVS disks of the SCSI type must be attached to the ECSs in the same anti-affinity ECS group. This section describes how to check whether the ECSs attached with the same shared SCSI disk are in the same ECS group.

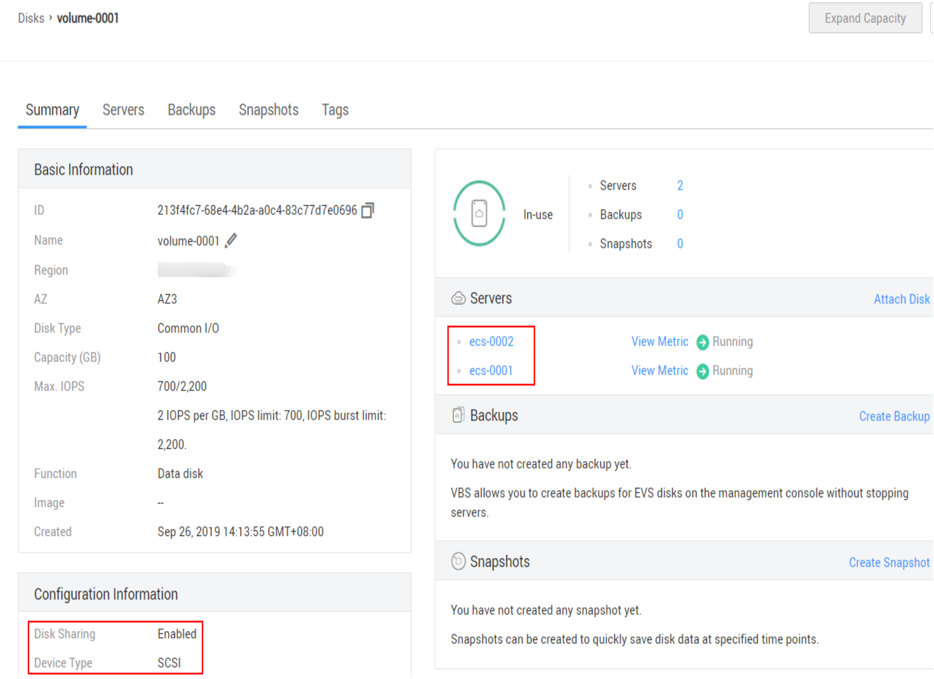
- For details about ECS groups, see **Managing ECS Groups**.
- For details about using shared EVS disks, see **Shared EVS Disks and Usage Instructions**.

Procedure

1. Log in to the **management console**.
2. Under **Storage**, click **Elastic Volume Service**.
3. Click the target shared SCSI disk to view its details.
4. In the **Servers** pane on the right side of the page, the ECSs to which the shared SCSI disk is attached are displayed.

   In this example, the ECSs to which the shared SCSI disk **volume-0001** is attached are **ecs-0001** and **ecs-0002**.

   Figure 9-24 Details about the disk

   ID 213f4fc7-68e4-4b2a-a0c4-83c77d7e0696
   Name volume-0001
   Region [redacted]
   AZ AZ3
   Disk Type Common I/O
   Capacity (GB) 100
   Max. IOPS 700/2,200
   2 IOPS per GB, IOPS limit: 700, IOPS burst limit: 2,200.
   Function Data disk
   Image --
   Created Sep 26, 2019 14:13:55 GMT+08:00

   Servers 2
   Backups 0
   Snapshots 0

   ecs-0002
   ecs-0001

   You have not created any backup yet.

   VBS allows you to create backups for EVS disks on the management console without stopping servers.

   You have not created any snapshot yet.

   Snapshots can be created to quickly save disk data at specified time points.

   Disk Sharing Enabled
   Device Type SCSI

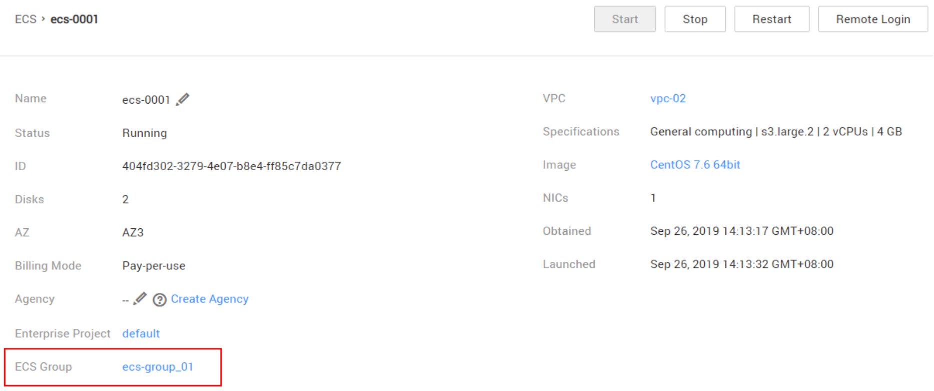
5. Click the names of these ECSs, respectively. On the page that provides details about an ECS, you can view the ECS group to which the current ECS belongs.

In this example, the ECS group to which ECS **ecs-0001** belongs is **ecs-group_01**.

NOTE

If the ECS group field is left blank, the ECS has not been added to any ECS group.

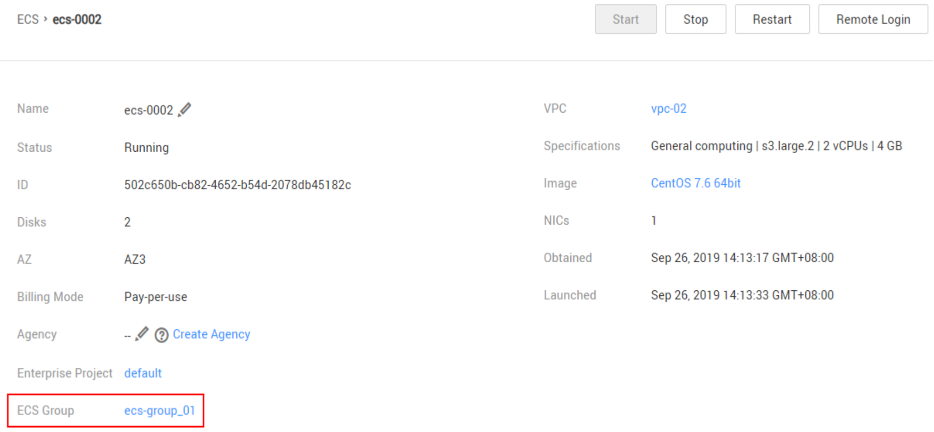
Figure 9-25 Details about an ECS (1)



Name: ecs-0001
Status: Running
ID: 404fd302-3279-4e07-b8e4-ff85c7da0377
Disks: 2
AZ: AZ3
Billing Mode: Pay-per-use
Agency: --
Enterprise Project: default
ECS Group: ecs-group_01
VPC: vpc-02
Specifications: General computing | s3.large.2 | 2 vCPUs | 4 GB
Image: CentOS 7.6 64bit
NICs: 1
Obtained: Sep 26, 2019 14:13:17 GMT+08:00
Launched: Sep 26, 2019 14:13:32 GMT+08:00

In this example, the ECS group to which ECS **ecs-0002** belongs is **ecs-group_01**.

Figure 9-26 Details about an ECS (2)



Name: ecs-0002
Status: Running
ID: 502c650b-cb82-4652-b54d-2078db45182c
Disks: 2
AZ: AZ3
Billing Mode: Pay-per-use
Agency: --
Enterprise Project: default
ECS Group: ecs-group_01
VPC: vpc-02
Specifications: General computing | s3.large.2 | 2 vCPUs | 4 GB
Image: CentOS 7.6 64bit
NICs: 1
Obtained: Sep 26, 2019 14:13:17 GMT+08:00
Launched: Sep 26, 2019 14:13:33 GMT+08:00

This indicates that the shared SCSI disk **volume-0001** is attached to ECSs **ecs-0001** and **ecs-0002**, and both ECSs are in ECS group **ecs-group_01**.

9.15 Can All Users Use the Encryption Feature?

The permissions of users in a user group to use the encryption feature are as follows:

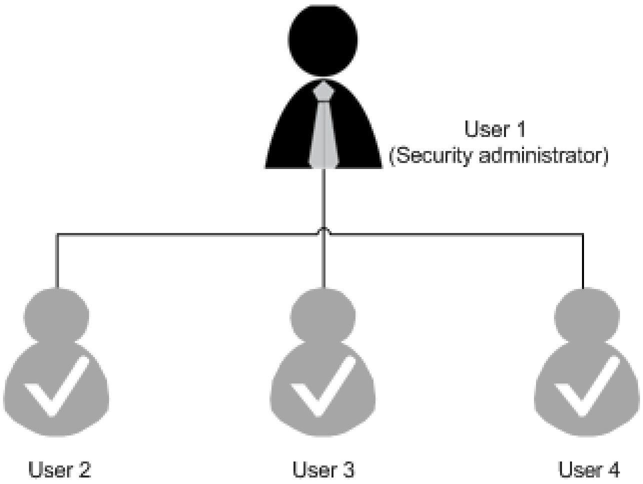
- The user who has security administrator permissions can grant KMS access permissions to EVS for using the encryption feature.
- When a common user who does not have security administrator permissions attempts to use the encryption feature, the condition varies depending on whether the user is the first one in the user group to use this feature.

  - If the common user is the first one in the user group to use the encryption feature, the common user must request a user who has security administrator permissions to grant the common user permissions. Then, the common user can use the encryption feature.
  - If the common user is not the first one in the user group to use the encryption feature, the user directly has the permissions to use the encryption feature.

The following section uses a user group as an example to describe how to grant KMS access permissions to EVS for using the encryption feature.

For example, a user group shown in **Figure 9-27** consists of four users, user 1 to user 4. User 1 has security administrator permissions. Users 2, 3, and 4 are common users who do not have security administrator permissions.

Figure 9-27 User group



Scenario 1: User 1 Uses the Encryption Feature

In this user group, if user 1 uses the encryption feature for the first time, the procedure is as follows:

1. User 1 creates Xrole to grant KMS access permissions to EVS.

   After user 1 grants permissions, the system automatically creates key **evs/default** for encrypting EVS disks.

   NOTE

   When user 1 uses the encryption feature for the first time, the user must grant the KMS access permissions to EVS. Then, all the users in the user group can use the encryption feature by default.

2. User 1 selects a key.

   One of the following keys can be used:

   - Default key **evs/default**
   - Custom key, which was created before using the EVS disk encryption feature
   - Newly created key (For instructions about how to create a key, see **Creating a Key Pair** in *Data Encryption Workshop User Guide*.)

After user 1 uses the encryption feature, all other users in the user group can use this feature, without requiring to contact user 1 for permissions granting.

Scenario 2: Common User Uses the Encryption Feature

In this user group, when user 3 uses the encryption feature for the first time:

1. The system displays a message indicating that the user has no permissions.
2. User 3 asks user 1 to create Xrole to grant KMS access permissions to EVS.

After user 1 grants the permissions, user 3 and all other users in the user group can use the encryption feature by default.

9.16 How Can I Add ECSs Using Local Disks to an ECS Group?

An ECS group logically isolates ECSs. ECSs in the same ECS group support anti-affinity and they are allocated on different hosts.

You can add an ECS to an ECS group in either of the following ways:

- During purchase: When purchasing an ECS, add the ECS to the ECS group by setting **ECS Group** in **Advanced Settings**.
- After purchase: After purchasing an ECS, click **Add ECS** to add the ECS to the ECS group.

Instances with local disks can be added to the ECS group at the time of purchase.

9.17 How Can I Delete or Unsubscribe from a Yearly/Monthly Disk?

Yearly/Monthly disks cannot be deleted. You can unsubscribe from them if needed. For details, see **Unsubscribing from or Deleting an EVS Disk**. To learn more about unsubscriptions, see **Unsubscription Overview**.

- Yearly/Monthly system disks cannot be unsubscribed from separately. They must be unsubscribed from together with their servers.
- Non-shared, yearly/monthly data disks purchased together with or later added to a yearly/monthly server have the same expiration time as the server. They can be unsubscribed from together with the server or separately when their statuses are **In-use**, **Available**, or **Error**.
- Yearly/Monthly data disks purchased on the EVS console have different expiration times as the server. They can be unsubscribed from separately.

9.18 Will My EVS Disk Be Unsubscribed from or Deleted When I Unsubscribe from or Delete Its Server?

- For pay-per-use disks:

  - If such disks are separately purchased and are attached, the system will prompt you whether to delete them when you delete the server. You can make the decision based on your requirements.
  - If such disks are purchased together with a server, the system disk as well as the data disks you have configured to release with server will be deleted. For the data disks not configured to release with server, the system will prompt you whether to delete them when you delete the server. You can make the decision based on your service requirements.
- For yearly/monthly disks:

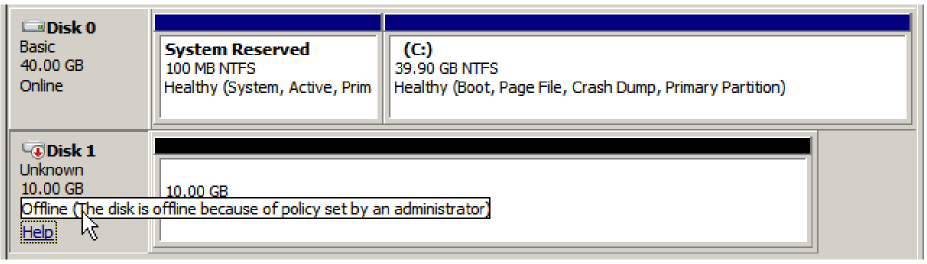
  If the disks are purchased together with a server, they will be unsubscribed from when you unsubscribe from the server.

9.19 Why Does a Disk Attached to a Windows ECS Go Offline?

Symptom

A disk attached to a Windows ECS goes offline, and the system displays the message "The disk is offline because of policy set by an administrator.", as shown in **Figure 9-28**.

Figure 9-28 Offline disk



Offline (The disk is offline because of policy set by an administrator)

Possible Causes

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

Table 9-6 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 offline by default, whereas disks on non-sharable buses are online.
OfflineInternal	Indicates that all newly detected disks are 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 ECS to **OnlineAll**.

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

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

   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 ECS with the SAN policy changed to create a private image so that the configuration takes effect permanently. After an ECS is created using this private image, the disks attached to the ECS are online by default. You only need to initialize them.

9.20 Why Does the Disk Drive Letter Change After the ECS Is Restarted?

Symptom

For a Linux ECS, the drive letter may change after an EVS disk is detached and then attached again, or after an EVS disk is detached and then the ECS is restarted.

Possible Causes

When a Linux ECS has multiple disks attached, it allocates drive letters in the attachment sequence and names the disks as **/dev/vda1**, **/dev/vdb1**, and **/dev/vdc1**, etc.

After a disk is detached and then attached again, or after a disk is detached and the ECS is restarted, the drive letter may change.

For example, an ECS has three disks attached: **/dev/vda1**, **/dev/vdb1**, and **/dev/vdc1**. The mounting parameters in **/etc/fstab** are as follows:

cat /etc/fstab

```
UUID=b9a07b7b-9322-4e05-ab9b-14b8050bdc8a  /  ext4  defaults  0  1
/dev/vdb1                  /data1   ext4  defaults  0  0
/dev/vdc1                  /data2   ext4  defaults  0  0
```

After **/dev/vdb1** is detached and the ECS is restarted, **/dev/vdc1** becomes **/dev/vdb1** and is mounted to **/data1**. In such a case, no disk is mounted to **/data2**.

The change of drive letters can affect the running of applications. To solve this problem, you are advised to use the universally unique identifiers (UUIDs) to replace **/dev/vdx** because a UUID uniquely identifies a disk partition in the Linux OS.

NOTE

This solution does not apply to shared EVS disks. Shared EVS disks may cause data inconsistency due to read/write conflicts and data caching.

For details, see **Attaching a Shared EVS Disk**.

Solution

1. Log in to the ECS.
2. Run the following command to obtain the partition UUID:

   blkid *Disk partition*

   In this example, run the following command to obtain the UUID of the **/dev/vdb1** partition:

   blkid /dev/vdb1

   Information similar to the following is displayed:

   ```
   [root@ecs-test-0001 ~]# blkid /dev/vdb1
   /dev/vdb1: UUID="b9a07b7b-9322-4e05-ab9b-14b8050cd8cc" TYPE="ext4"
   ```

   The UUID of the **/dev/vdb1** partition is displayed.
3. Run the following command to open the **fstab** file using the vi editor:

   vi /etc/fstab
4. Press **i** to enter the editing mode.
5. Move the cursor to the end of the file and press **Enter**. Then, add the following information:

   ```
   UUID=b9a07b7b-9322-4e05-ab9b-14b8050cd8cc    /data1    ext4    defaults        0 0
   ```

   The parameters are defined as follows:

   - **UUID=b9a07b7b-9322-4e05-ab9b-14b8050cd8cc**: UUID of a disk partition.
   - **/data1**: directory on which the partition is mounted. You can run **df -TH** to query the directory.
   - **ext4**: File system format of the partition. You can run **df -TH** to query the format.
   - **defaults**: partition mount option. Normally, this parameter is set to **defaults**.
   - **0** (the first one): whether to use Linux dump backup.
     - **0**: Linux dump backup is not used. Normally, dump backup is not used, and you can set this parameter to **0**.
     - **1**: Linux dump backup is used.
   - **0** (the second one): fsck option, that is, whether to use fsck to check disks during startup.

        - **0**: fsck is not used.
        - If the mount point is the root partition (**/**), this parameter must be set to **1**.

          When this parameter is set to **1** for the root partition, this parameter for other partitions must start with **2** so that the system checks the partitions in the ascending order of the values.

6. Repeat steps 2 to 5 to replace the UUID of **/dev/vdc1**.
7. Run the following command again to check the disk mounting parameters:

   cat /etc/fstab

   The following information is displayed:

```
UUID=b9a07b7b-9322-4e05-ab9b-14b8050bdc8a  /  ext4  defaults  0  1
UUID=b9a07b7b-9322-4e05-ab9b-14b8050cd8cc   /data1   ext4  defaults  0  0
UUID=b9a07b7b-9322-4e05-ab9b-14b8050ab6bb   /data2   ext4  defaults  0  0
```

9.21 How Can I Obtain Data Disk Information If Tools Are Uninstalled?

If you uninstall Tools from a Linux ECS in a non-PVOPS system, data disks cannot be identified. In such a case, you can create a new ECS and attach the data disks of the original ECS to the new ECS and view information about the data disks. The procedure is as follows:

1. Log in to the management console and create a new ECS.

   NOTE

   Ensure that the new ECS is located in the same AZ and has the same parameter settings as the original ECS.

2. (Optional) On the **Elastic Cloud Server** page, locate the row containing the original ECS, click **More** in the **Operation** column, and select **Stop**. On the displayed page, select **Force stop** and click **OK** to forcibly stop the original ECS.

   Manually refresh the **Elastic Cloud Server** page. The original ECS is stopped once the **Status** changes to **Stopped**.

   NOTE

   The ECSs running certain OSs support online data disk detaching. If your OS supports this feature, you can detach data disks from the running ECS.

3. View information about the data disks attached to the original ECS.

   NOTE

   If the original ECS has multiple data disks attached, repeat steps 4 to 6 to attach each data disk to the new ECS.

4. Click a data disk. The **Elastic Volume Service** page is displayed.
5. Select the data disk to be detached and click **Detach** in the **Operation** column. On the **Detach Disk** page, select the original ECS and click **OK** to detach the data disk from the original ECS.

   Manually refresh the **Elastic Volume Service** page. The data disk is detached from the original ECS once the **Status** changes to **Available**.

6. Select the detached data disk and click **Attach** in the **Operation** column. On the **Attach Disk** page, click the new ECS, select a device name, and click **OK** to attach the data disk to the new ECS.

   Manually refresh the EVS list. The data disk is attached to the new ECS once the **Status** value changes to **In-use**. You can then log in to the management console and view information about the data disk of the new ECS.

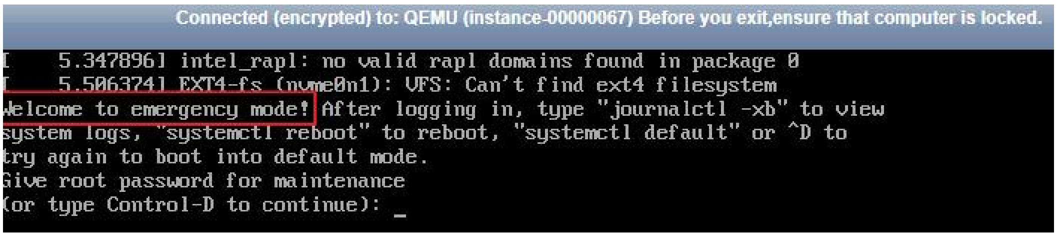
9.22 How Can I Rectify the Fault That May Occur on a Linux ECS with an NVMe SSD Disk Attached?

Symptom

When a Linux ECS with an NVMe SSD disk attached, such as a P1 ECS, becomes faulty, you must contact the administrator to remotely rebuild the ECS again.

If automatic NVMe SSD disk attachment upon ECS startup is enabled in **/etc/fstab** on the faulty ECS, the system disk recovers after the ECS is created. However, the attached NVMe SSD disk does not have a file system, and automatic NVMe SSD disk attachment upon ECS startup fails to take effect. As a result, the ECS enters the emergency mode, as shown in **Figure 9-29**.

Figure 9-29 Emergency mode



Connected (encrypted) to: QEMU (instance-00000067) Before you exit,ensure that computer is locked.

```
[    5.347896] intel_rapl: no valid rapl domains found in package 0
[    5.506374] EXT4-fs (nvme0n1): VFS: Can't find ext4 filesystem
Welcome to emergency mode! After logging in, type "journalctl -xb" to view
system logs, "systemctl reboot" to reboot, "systemctl default" or ^D to
try again to boot into default mode.
Give root password for maintenance
(or type Control-D to continue): _
```

To ensure that the new ECS is functional, you must manually delete the attachment information in **/etc/fstab**.

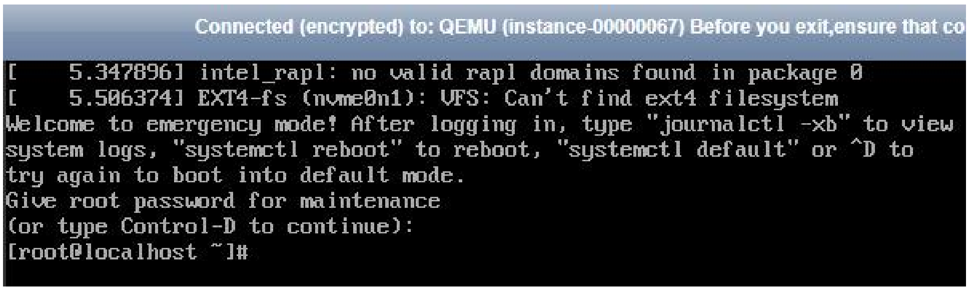
NOTE

If the NVMe SSD disk is faulty, data on it will be lost. The operations provided in this section are only used to restore automatic NVMe SSD disk attachment to an ECS, but not restoring the data on the disk.

Solution

1. Log in to the ECS.
2. Enter the password of user **root** to log in to the ECS.

Figure 9-30 Logging in to the ECS



Connected (encrypted) to: QEMU (instance-00000067) Before you exit,ensure that co

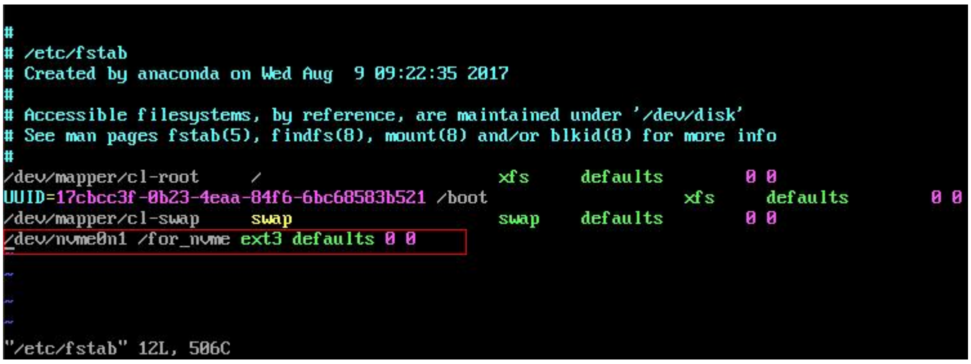
```
[    5.347896] intel_rapl: no valid rapl domains found in package 0
[    5.506374] EXT4-fs (nvme0n1): VFS: Can't find ext4 filesystem
Welcome to emergency mode! After logging in, type "journalctl -xb" to view
system logs, "systemctl reboot" to reboot, "systemctl default" or ^D to
try again to boot into default mode.
Give root password for maintenance
(or type Control-D to continue):
[root@localhost ~]#
```

3. Run the following command to edit the **/etc/fstab** file:

   vi /etc/fstab

4. Delete the attaching information of the NVMe SSD disk and save the file.

Figure 9-31 Deleting the automatic attaching information



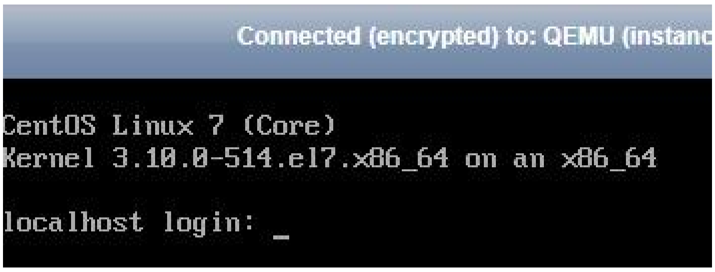
```
#
# /etc/fstab
# Created by anaconda on Wed Aug  9 09:22:35 2017
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/cl-root     /                       xfs     defaults        0 0
UUID=17cbcc3f-0b23-4eaa-84f6-6bc68583b521 /boot                   xfs     defaults        0 0
/dev/mapper/cl-swap     swap                    swap    defaults        0 0
/dev/nvme0n1 /for_nvme ext3 defaults 0 0
~
~
~
"/etc/fstab" 12L, 506C
```

5. Run the following command to restart the ECS:

   reboot

6. Verify that the ECS recovers and can be logged in.

Figure 9-32 Logging in to the ECS



```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.el7.x86_64 on an x86_64

localhost login: _
```

9.23 Why Is the Device Name of My C6 ECS in the sd* Format?

Symptom

The device name of previously purchased C6 ECSs is in vd* format, for example, vda and vdb, but the device name of newly purchased C6 ECSs is in sd* format.

This section describes the reason why the device name is changed to the sd* format and how to handle the sd* device name in common scenarios.

Root Cause

The device name of the Linux system is automatically generated based on certain rules that are related to the disk protocol and disk sequence number, which brings some uncertainties. When disks are attached to C6 ECSs, either virtio-blk or virtio-scsi is used.

- If virtio-blk is allocated, the device name format is vd*.
- If virtio-scsi is allocated, the device name format is sd*.

Disk Partitioning and Formatting

Problem: Before using an ECS for the first time, you need to partition or format the attached data disks. If the ECS device name is in sd* format, running **/dev/vd*** will fail.

Solution: Dynamically obtain the device name and then perform operations on the disk. You can dynamically obtain device names in either of the following ways:

- Method 1: Run fdisk to query the device name.

  Log in to the ECS and run the following command to query the data disk list:

  fdisk -l

  Information similar to the following is displayed, indicating the ECS has two disks attached. **/dev/vda** is the system disk, and **/dev/vdb** is the new data disk.

  ```
  [root@ecs-test-0001 ~]# fdisk -l

  Disk /dev/vda: 42.9 GB, 42949672960 bytes, 83886080 sectors
  Units = sectors of 1 × 512 = 512 bytes
  Sector size (logical/physical): 512 bytes / 512 bytes
  I/O size (minimum/optimal): 512 bytes / 512 bytes
  Disk label type: dos
  Disk identifier: 0x000bcb4e

     Device Boot      Start         End      Blocks   Id  System
  /dev/vda1   *        2048    83886079    41942016   83  Linux

  Disk /dev/vdb: 107.4 GB, 107374182400 bytes, 209715200 sectors
  Units = sectors of 1 × 512 = 512 bytes
  Sector size (logical/physical): 512 bytes / 512 bytes
  I/O size (minimum/optimal): 512 bytes / 512 bytes
  ```

  This is a convenient method to obtain the device name, but you cannot obtain the mapping between the EVS disks attached to the ECS and the device names in the OS. If you want to know the mapping, obtain the device name by referring to method 2.

- Method 2: Use serial-id or wwn to obtain the device name.

  For details, see **How Do I Obtain My Disk Device Name in the ECS OS Using the Device Identifier Provided on the Console?**.

Automatic Mounting of File Systems

You are advised to use UUIDs to identify disks in the file because they are unique identifiers for disk partitions and do not change with device names. Use the UUID of the file system to configure automatic mounting for a system disk and a data disk.

- Automatic Mounting for a System Disk
  - If a Huawei Cloud public image or a private image created from a public image is used, UUIDs are used for automatic disk mounting and no action is required.
  - If a private image created using a non-public image is used, select **Enable automatic configuration** when creating the image. Then, the system automatically uses UUIDs for automatic disk mounting.
  - If **Enable automatic configuration** is not selected when you are creating a private image, see **Changing the Disk Identifier in the fstab File to UUID**.
- Automatic Mounting for Data Disks

  If you want to configure automatic mounting for data disks, see **Creating and Mounting a File System**.

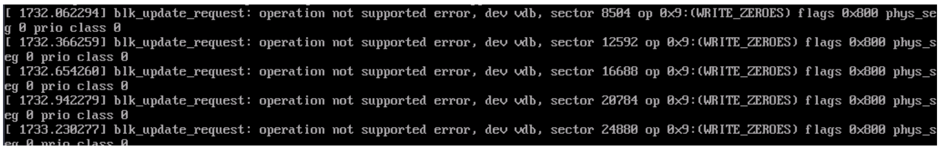
9.24 Why Are Disk Error Logs Printed After a Disk Attached to an ECS Is Formatted with the ext4 File System?

Symptom

When a VBD disk is attached to an ECS and the partition is in ext4 format, the following log may be displayed on the console:

blk_update_request: operation not supported error, dev vdb, sector 826298624 op 0x9:(WRITE_ZEROES) flags 0x800 phys_seg 0 prio class 0

Figure 9-33 Printed logs



```
[ 1732.062294] blk_update_request: operation not supported error, dev vdb, sector 8504 op 0x9:(WRITE_ZEROES) flags 0x800 phys_se
g 0 prio class 0
[ 1732.366259] blk_update_request: operation not supported error, dev vdb, sector 12592 op 0x9:(WRITE_ZEROES) flags 0x800 phys_s
eg 0 prio class 0
[ 1732.654260] blk_update_request: operation not supported error, dev vdb, sector 16688 op 0x9:(WRITE_ZEROES) flags 0x800 phys_s
eg 0 prio class 0
[ 1732.942279] blk_update_request: operation not supported error, dev vdb, sector 20784 op 0x9:(WRITE_ZEROES) flags 0x800 phys_s
eg 0 prio class 0
[ 1733.230277] blk_update_request: operation not supported error, dev vdb, sector 24880 op 0x9:(WRITE_ZEROES) flags 0x800 phys_s
eg 0 prio class 0
```

Involved OSs: Ubuntu 20.04, CentOS 8.0, CentOS 8.1, and other ECSs whose kernel versions are 4.18 or later

Root Cause

VBD disks do not support the advanced SCSI command WRITE_ZEROES.

If the ECS OS kernel version is 4.18 or later and the disk partition is formatted with the ext4 file system, the WRITE_ZEROES command is delivered. The system does not support the command and prints a log, which has no impact on the ECS performance and you can ignore it.

9.25 What Should I Do If My Linux ECS Fails to Start Due to Incorrect /etc/fstab File Configuration?

Symptom

For Linux ECSs, their automatic mounting of file systems is configured in the **/etc/fstab** file. If the automatic mounting information is incorrectly configured or unavailable, the ECS OS may fail to start after the system is restarted.

For details, see **/etc/fstab File Introduction**.

Possible Causes

- The **/etc/fstab** file was not modified before the disk is detached or reinitialized. As a result, the **/etc/fstab** file contains unnecessary automatic mounting information of file systems.
- The device name or UUID of a file system is incorrectly configured.
- The file type of a file system is incorrectly configured.
- The mount parameters are incorrect.

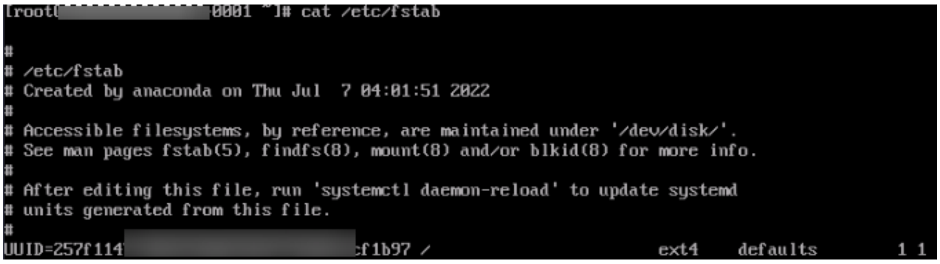
Solution

1. Log in to the ECS. For details, see **Login Overview (Linux)**.
2. Run the following command to back up the **/etc/fstab** file before modifying it:

   cp /etc/fstab /etc/fstab.bak
3. Run the following command to check the content of the **/etc/fstab** file and ensure that the mount path, device name, or UUID is correct:

   cat /etc/fstab

   Figure 9-34 Check results

```
[root[redacted]0001 ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Jul  7 04:01:51 2022
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=257f114[redacted]cf1b97 /                                ext4    defaults        1 1
```

   a. Check the mount point.

      Check that each mount point (for example, **/mnt/data**) exists and has the correct permissions and owner.

   b. Check the device or UUID.

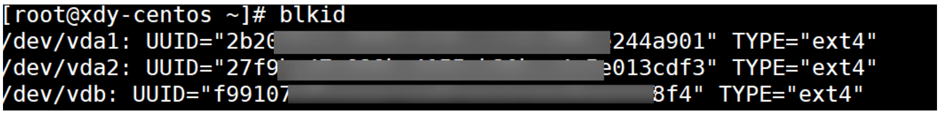
NOTE

You are advised to mount partitions using the UUID to prevent errors in the **fstab** file caused by device name changes. These changes may occur when an ECS is restarted after specifications are modified or disks mounted or unmounted.

Run the following command to obtain the device UUID and ensure that the device name (for example, **/dev/vda1**) or UUID exists and is correct:

blkid

Figure 9-35 Obtaining the device UUID



```
[root@xdy-centos ~]# blkid
/dev/vda1: UUID="2b2[redacted]244a901" TYPE="ext4"
/dev/vda2: UUID="27f9[redacted]e013cdf3" TYPE="ext4"
/dev/vdb: UUID="f99107[redacted]8f4" TYPE="ext4"
```

c. Check the mount options.

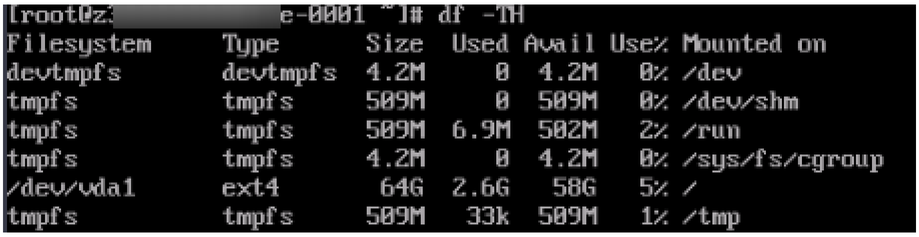
   Check whether the mount option of each mount partition is correct, for example, **defaults** and **rw**.

d. Check the mount status.

   Run the following command to check whether all file systems are correctly mounted:

   df -h

Figure 9-36 Check results



```
[root@z[redacted]e-0001 ~]# df -TH
Filesystem     Type      Size  Used Avail Use% Mounted on
devtmpfs       devtmpfs  4.2M     0  4.2M   0% /dev
tmpfs          tmpfs     509M     0  509M   0% /dev/shm
tmpfs          tmpfs     509M  6.9M  502M   2% /run
tmpfs          tmpfs     4.2M     0  4.2M   0% /sys/fs/cgroup
/dev/vda1      ext4       64G  2.6G   58G   5% /
tmpfs          tmpfs     509M   33k  509M   1% /tmp
```

Compare the **/etc/fstab** file content with the mount point details in the command output, and delete unnecessary configuration lines from the **/etc/fstab** file.

4. Run the following command to test the mount result:

   mount -a

   This command automatically mounts the file system based on the configuration in the **/etc/fstab** file.

   - If no error is displayed, the **/etc/fstab** file is correctly configured. No further action is required.
   - If an error is displayed, use a text editor (such as vi or nano) to edit the **/etc/fstab** file based on the error information, and save the modified file.

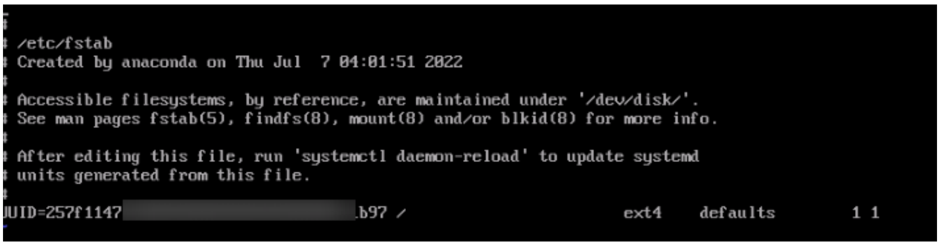
5. If the **/etc/fstab** file is modified, run the following command to restart the system to apply the modification.

   reboot

/etc/fstab File Introduction

Table 9-7 lists each field in the **/etc/fstab** file.

Figure 9-37 /etc/fstab file



```
#
# /etc/fstab
# Created by anaconda on Thu Jul  7 04:01:51 2022
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=257f1147[redacted]b97 /                       ext4    defaults        1 1
```

Table 9-7 /etc/fstab file fields

Field	Description
file system	UUID of the file system of the partition to be mounted. For example, UUID=*xxxx-xxxx*.
dir	Mount point.
type	File system type of the partition to be mounted, for example, ext4 or xfs.
options	Mount parameter. The **defaults** parameter is generally used. If multiple parameters are required, separate them with commas (,). Table 9-8 lists common mount parameters.
dump	Whether a file system is backed up with dump. ● **0**: The file system is not backed up. ● **1**: The file system is backed up.
pass	Determines the check sequence of the file systems with fsck. A smaller value indicates a higher check priority. Rule: ● **1**: Root file system ● **2** or a larger value: Other file systems ● **0**: No check is required.

Table 9-8 Mount parameters

Mount Option	Description
defaults	Uses the default mount parameters of file systems. Separate multiple parameters with commas (,). For example, the default parameters of the ext4 file type are rw,suid,dev,exec,auto,nouser,async.

Mount Option	Description
rw	Mounts a file system as read/write.
ro	Mounts a file system as read-only.
auto	Automatically mounts at startup or when the **mount -a** command is executed.
noauto	Requires manual mounting using commands.
suid	Allows the suid operation and setting of sgid bits. Generally, this parameter is used to temporarily elevate the permissions of common users when they run special tasks.
nosuid	Prevents the suid operation and sgid bits.
dev	Parses the block device on the file system.
nodev	Does not parse the block device on the file system.
exec	Allows the execution of executable files on mount points.
noexec	Prevents the execution of executable files on mount points.
nouser	Only allows the **root** user to mount file systems.
async	Asynchronous I/O
sync	Synchronous I/O
nofail	If the device does not exist when you start the ECS, the device is ignored.

10 Data Backup and Restoration

10.1 Can ECSs Automatically Recover After the Physical Host Accommodating the ECSs Becomes Faulty?

Yes. ECS can automatically recover if the physical host becomes faulty.

ECSs run on physical hosts. Although there are multiple mechanisms to ensure system reliability, fault tolerance, and high availability, host hardware might be damaged or power failures might occur. If physical hosts cannot be powered on or restarted due to damage, CPU and memory data will be lost and live migration cannot be used to recovery ECSs.

The cloud platform provides automatic recovery by default to restart ECSs through cold migration, ensuring high availability and dynamic ECS migration. If a physical host accommodating ECSs breaks down, the ECSs will automatically be migrated to a functional physical host to minimize the impact on your services. During the process, the ECSs will restart.

You can enable one-click monitoring on the Cloud Eye console so that you will be notified if any exceptions occur (if a physical host accommodating ECSs is faulty, the ECSs will automatically be migrated to a functional physical host). For details, see **One-Click Monitoring**.

NOTE

- Auto recovery does not ensure user data consistency.
- An ECS can be automatically recovered only if the physical server where the ECS resides becomes faulty. This function does not take effect if the fault is caused by the ECS itself.
- An ECS can be automatically recovered only after the physical server where the ECS resides is shut down. If the physical server is not shut down due to a fault, for example, a memory fault, auto recovery fails to take effect.
- An ECS can be automatically recovered only once within 12 hours if the physical server where the ECS resides becomes faulty.
- ECS auto recovery may fail in the following scenarios:
  - No physical server is available for migration due to a system fault.
  - The target physical server does not have sufficient temporary capacity.
- An ECS with any of the following resources cannot be automatically recovered:
  - Local disk
  - Passthrough FPGA card
  - Passthrough InfiniBand NIC

10.2 How Can I Back Up Local Disk Data?

Scenarios

For ECSs that have local disks attached, data stored in local disks may be deleted during the event execution, such as instance redeployment or local disk replacement. To ensure data security, back up local disk data before authorizing the events.

Data stored in local disks cannot be backed up directly. You need to attach an EVS disk to the ECS and then migrate the local disk data to the EVS disk.

Procedure

1. Add an EVS disk.

   Add an EVS disk based on the amount of the local disk data to be backed up.

   NOTE

   The new EVS disk must be in the same region and AZ as the ECS for which you want to back up the local disk data.

   For details, see **Adding a Disk to an ECS**.
2. Attach the EVS disk to the ECS.

   Attach the created EVS disk to the ECS.

   For details, see **Attaching an EVS Disk to an ECS**.
3. Back up local disk data.

   Back up the data stored in local disks to the new EVS disk that is attached to the ECS.
4. Detach the EVS disk from the ECS.

   After the local disk data is backed up, detach the EVS disk attached to the ECS in step 2.

For details, see **Detaching an EVS Disk from a Running ECS**.

After the event is handled, attach that EVS disk to the ECS again and restore the backup data to the local disk.

11 Network Configuration

11.1 How Can I Configure the NTP and DNS Servers for an ECS?

For Linux OSs

Take the NTP and DNS servers running SUSE as an example.

Step 1 Configure the NTP server for the ECS.

1. Log in to the Linux ECS.
2. Run the following command to switch to user **root**:

   sudo su -
3. Run the following command to edit the **ntp.conf** configuration file:

   vim /etc/ntp.conf
4. Add the following statement to configure the NTP server:

   server *Domain name or IP address of the NTP server*

   Example:

   If the IP address of the NTP server is 192.168.56.1, add the following statement:

   server 192.168.56.1
5. Run the following command to start the NTP service upon system restart:

   service ntp restart
6. Run the following command to check the status of the NTP server:

   service ntp status

   NOTE

   If you want to disable NTP, perform the following steps:

   1. Run the **service ntp stop** command to stop NTP.
   2. Run the **systemctl disable ntp** command to disable the function of automatically starting NTP upon ECS startup.

Step 2 Configure the DNS server for the ECS.

1. Log in to the Linux ECS.
2. Run the following command to switch to user **root**:

   sudo su -
3. Run the following command to edit the **resolv.conf** configuration file:

   vi /etc/resolv.conf
4. Add the following statement to configure the DNS server:

   nameserver = *IP addresses of the DNS servers*

   Example:

   If the IP addresses of the DNS servers are 8.8.8.8 and 4.4.4.4, add the following statements:

   nameserver = 8.8.8.8

   nameserver = 4.4.4.4

   NOTE

   The IP addresses of the DNS servers must be the same as those in the VPC subnet. Otherwise, the DNS modification cannot persistently take effect.
5. Run the following command to restart the network:

   rcnetwork restart

   service network restart

   /etc/init.d/network restart

----End

Windows

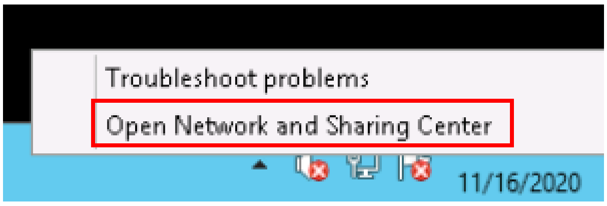
Take an ECS running Windows Server 2012 as an example.

Step 1 Log in to the Windows ECS as user **Administrator**.

Step 2 Enable the local area connection.

1. In the lower right corner of the taskbar, right-click the network connection icon.
2. Click **Open Network and Sharing Center**.

Figure 11-1 Open Network and Sharing Center



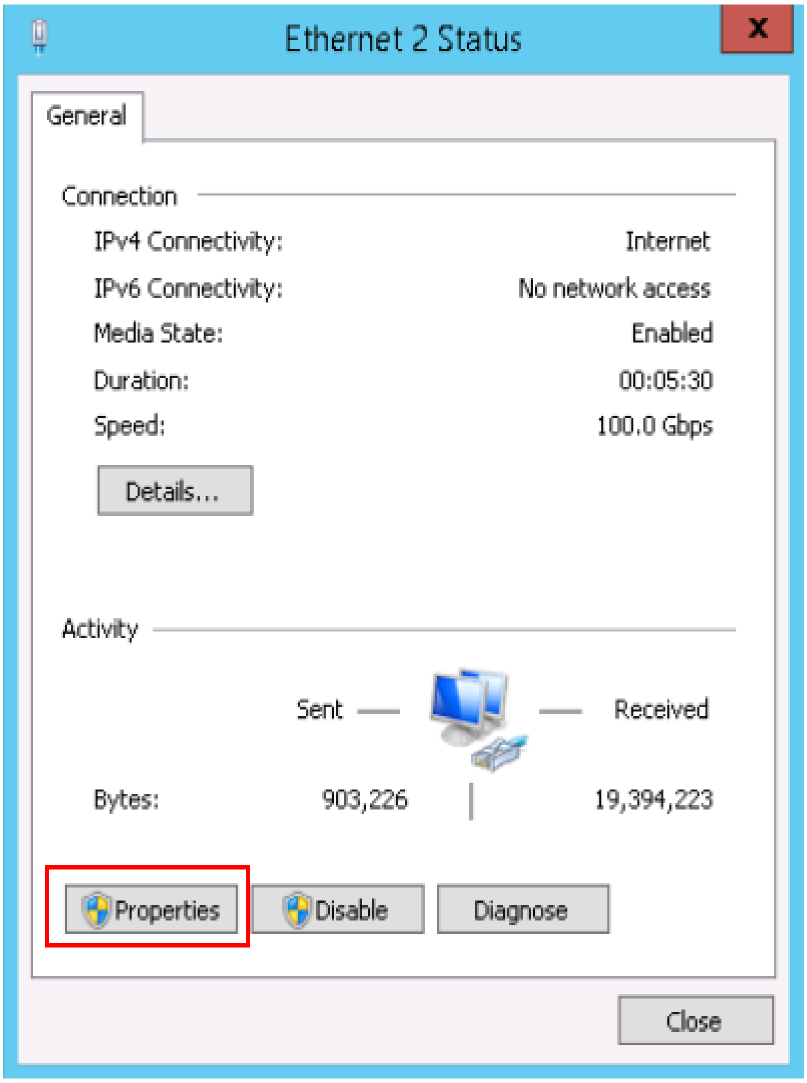
3. In the navigation pane on the left, click **Change adapter settings**.

Step 3 Configure the DNS server for the ECS.

1. Double-click network connections.

2. Click **Properties** in the lower left corner, as shown in **Figure 11-2**.

Figure 11-2 Local area connection



Ethernet 2 Status

General

Connection

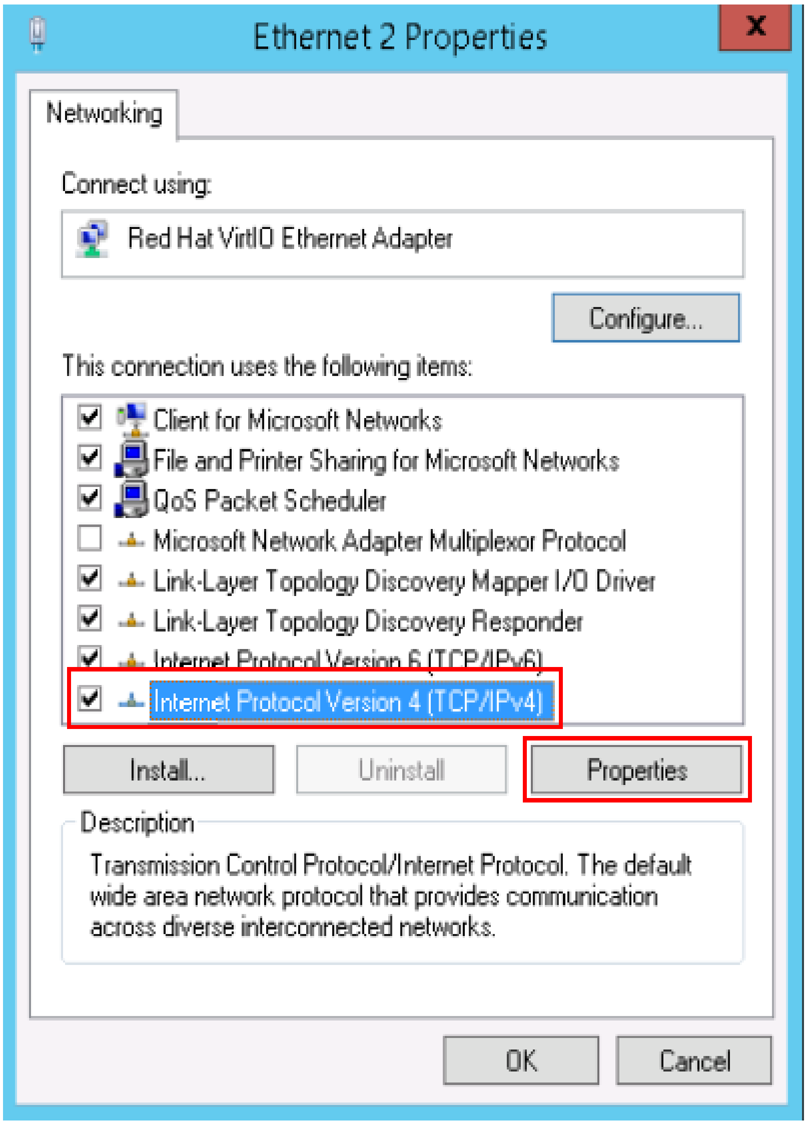
IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	00:05:30
Speed:	100.0 Gbps

Activity

	Sent	Received
Bytes:	903,226	19,394,223

3. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**, as shown in **Figure 11-3**.

Figure 11-3 Selecting a protocol type



Connect using:

Red Hat VirtIO Ethernet Adapter

This connection uses the following items:

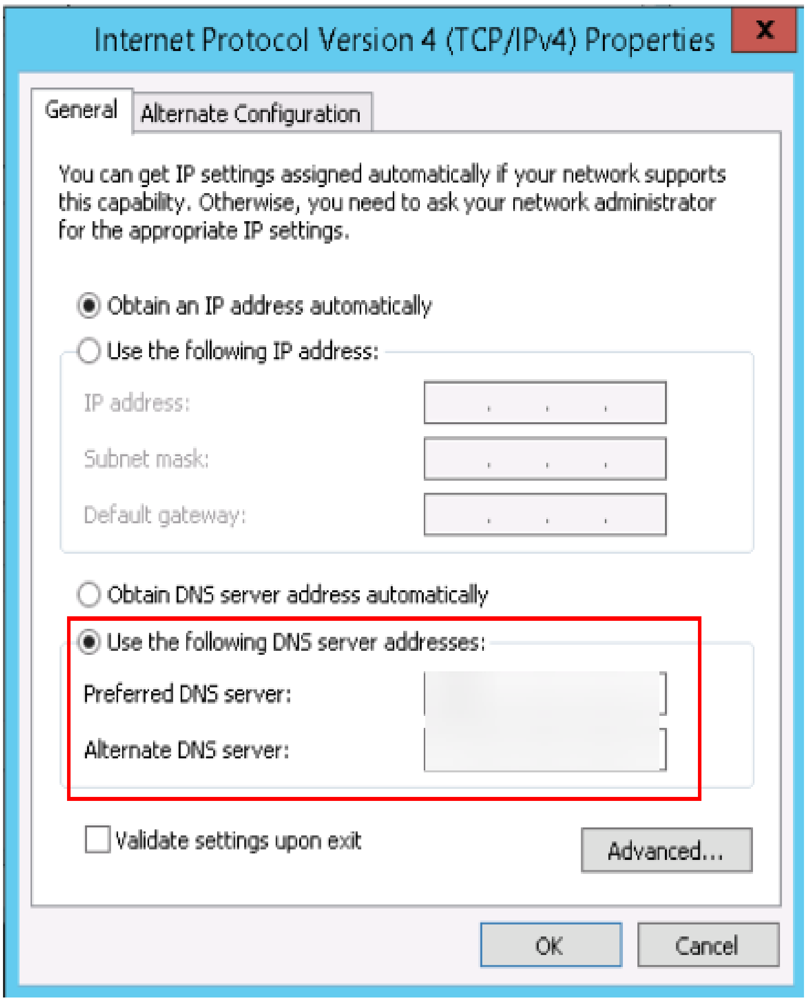
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

4. Select **Use the following DNS server addresses** and set the IP addresses of the DNS servers as prompted, as shown in **Figure 11-4**.

Figure 11-4 Setting the IP addresses of the DNS servers



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
☐ Validate settings upon exit

Step 4 Configure the NTP server for the ECS.

1. Start the **Run** dialog box. Enter **regedit** and click **OK**.
2. Modify the registry entries.
    - In **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > TimeProviders > NtpClient**, set the value of **Enabled** to **1**, indicating that the NTP client is used.
    - In **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > TimeProviders > NtpServer**, set the value of **Enabled** to **0**, indicating that the NTP server is stopped.
    - Choose the **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services** > **W32Time** > **Parameters** file and set the **NtpServer** data. For example, set its data to **ntp.myhuaweicloud.com**. Set the data of **TYPE** to **NTP**.
    - In **HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W32Time \ TimeProviders \ NtpClient**, set the value of **SpecialPollInterval** to **3600** and that of **Base** to **Decimal**, indicating the clock synchronization cycle is 3600s.
    - In **HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W32Time \ config**, set the values of **MaxPosPhaseCorrection** and **MaxNegPhaseCorrection** to **fffffff** and that of **Base** to **Hexadecimal**.

3. Open the **Run** dialog box, enter **services.msc**, and click **OK**. The **Services** window is displayed.
4. View the service named **Windows Time** and set the **Start Type** to **Automatic** to synchronize time from the NTP server.
5. Open the **Run** dialog box and run the following commands in sequence to restart the Windows Time service:

   net stop w32time

   net start w32time
6. Manually change the time on the client to make it different from that on the NTP server. One minute later, check whether the time on the client is the same as that on the NTP server. If yes, the time is synchronized.

----End

11.2 Does Huawei Cloud Provide the NTP Server and How Can I Configure It?

Yes. Huawei Cloud provides the NTP server, and you can use it only on the ECSs you have purchased on the Huawei Cloud management console.

You can use the Huawei-provided NTP server or other NTP servers. The configuration procedures are the same. This section describes how to configure the Huawei-provided NTP server on an ECS.

NOTE

ECSs created using x86 public images use chronyd for time synchronization by default. You do not need to configure the NTP server.

Background

If you use the NTP server provided by Huawei Cloud, you also need to use the DNS server. **Table 11-1** lists the NTP servers provided by Huawei Cloud in different regions.

For details about how to obtain the DNS server address, see **What Are Huawei Cloud Private DNS Server Addresses?**

Table 11-1 NTP servers

Region	NTP Server IP Address
CN North	ntp.myhuaweicloud.com
CN East	ntp.myhuaweicloud.com
CN South	ntp.myhuaweicloud.com
CN Southwest	ntp.myhuaweicloud.com
CN-Hong Kong	ntp.myhuaweicloud.com
AP-Bangkok	ntp.myhuaweicloud.com

Region	NTP Server IP Address
AP-Singapore	ntp.myhuaweicloud.com
AP-Jakarta	ntp.myhuaweicloud.com
AP-Manila	ntp.myhuaweicloud.com
ME-Riyadh	ntp.myhuaweicloud.com
AF-Cairo	ntp.myhuaweicloud.com
AF-Johannesburg	ntp.myhuaweicloud.com
Istanbul (Türkiye)	ntp.myhuaweicloud.com
LA-Mexico City1	ntp.myhuaweicloud.com
LA-Mexico City2	ntp.myhuaweicloud.com
LA-Sao Paulo1	ntp.myhuaweicloud.com
LA-Santiago	ntp.myhuaweicloud.com

Linux (chronyd)

The following section uses CentOS 7.3 as an example.

Step 1 Check whether the IP address of the DNS server is correct on the ECS.

1. Log in to the Linux ECS.
2. Run the following command to open the **resolv.conf** file:

   vi /etc/resolv.conf
3. Check whether the **nameserver** value in the file is the same as the IP address of the DNS server provided in **What Are Huawei Cloud Private DNS Server Addresses?**
   - If yes, go to step **Step 3**.
   - If no, go to step **Step 2**.

Step 2 (Optional) Configure the DNS server for the ECS.

1. Log in to the Linux ECS.
2. Run the following command to edit the **resolv.conf** configuration file:

   vi /etc/resolv.conf
3. Add the following statement to configure the DNS server:

   nameserver *IP address of the DNS server*

   Example:

   Consider the **CN North** region as an example. Add the following statement:

   nameserver 100.125.1.250

Step 3 Configure the NTP server for the ECS.

1. Log in to the Linux ECS.
2. Run the following commands to stop the chronyd process:

   systemctl stop chronyd

   systemctl disable chronyd
3. Run the following command to edit the **chrony.conf** configuration file:

   vim /etc/chrony.conf
4. Add the following statement to configure the NTP server:

   server *Domain name of the NTP server* **minpoll 4 maxpoll 10 iburst**

   Example:

   server ntp.myhuaweicloud.com minpoll 4 maxpoll 10 iburst
5. Run the following command to start the service upon system restart:

   For Euler and CentOS:

   systemctl restart chronyd

   For SUSE:

   service chronyd restart

   NOTE

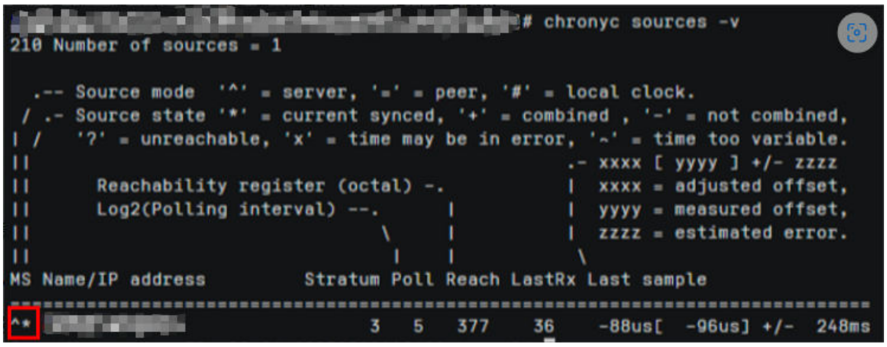
   Run the required command based on the OS running on the ECS.

   If the message "Failed to restart chronyd.service: Unit not found." is displayed, run the **yum -y install chrony** command.
6. Run the following command to check whether the time on the NTP server has been synchronized with that on the upper-layer NTP server:

   chronyc sources -v

   If "*" is displayed, the time has been synchronized.

Figure 11-5 Modification result



```
[redacted]# chronyc sources -v
210 Number of sources = 1

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current synced, '+' = combined , '-' = not combined,
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too variable.
||                                                 .- xxxx [ yyyy ] +/- zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured offset,
||                                \     |          |  zzzz = estimated error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* [redacted]                    3   5   377    36    -88us[  -96us] +/-  248ms
```

NOTE

It takes several minutes to perform NTP time synchronization for the first time.

7. Set the automatic startup of the chronyd service.

   For Euler and CentOS:

   systemctl enable chronyd

   For SUSE:

chkconfig chronyd on

----End

Linux (ntpd)

The following section uses CentOS 7.3 as an example.

Step 1 Check whether the IP address of the DNS server is correct on the ECS.

1. Log in to the Linux ECS.
2. Run the following command to open the **resolv.conf** file:
   vi /etc/resolv.conf
3. Check whether the **nameserver** value in the file is the same as the IP address of the DNS server provided in **What Are Huawei Cloud Private DNS Server Addresses?**
   - If yes, go to step **Step 3**.
   - If no, go to step **Step 2**.

Step 2 (Optional) Configure the DNS server for the ECS.

1. Log in to the Linux ECS.
2. Run the following command to edit the **resolv.conf** configuration file:
   vi /etc/resolv.conf
3. Add the following statement to configure the DNS server:
   nameserver *IP address of the DNS server*
   Example:
   Consider the **CN North** region as an example. Add the following statement:
   nameserver 100.125.1.250

Step 3 Configure the NTP server for the ECS.

1. Log in to the Linux ECS.
2. Run the following commands to stop the chronyd process:
   systemctl stop chronyd
   systemctl disable chronyd
3. Run the following command to edit the **ntp.conf** configuration file:
   vim /etc/ntp.conf
4. Add the following statement to configure the NTP server:
   server *Domain name of the NTP server*
   Example:
   server ntp.myhuaweicloud.com
5. Run the following command to start the NTP service upon system restart:
   For Euler and CentOS:
   systemctl restart ntpd
   For SUSE:
   service ntpd restart

NOTE

Run the required command based on the OS running on the ECS.

If the message "Failed to restart ntpd.service: Unit not found." is displayed, run the **yum -y install ntp** command.

6. Run the following command to check whether the time on the NTP server has been synchronized with that on the upper-layer NTP server:

   ntpq -p

   If "*" is displayed, the time has been synchronized.

   NOTE

   It takes several minutes to perform NTP time synchronization for the first time.

7. Set the automatic startup of the NTP service.

   For Euler and CentOS:

   chkconfig ntpd on

   For SUSE:

   chkconfig ntpd on

----End

Windows

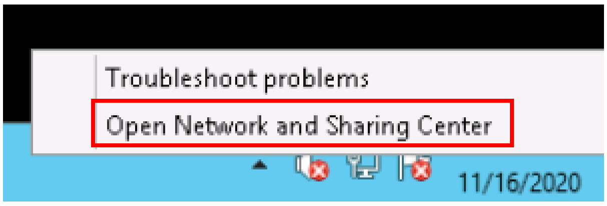
Take an ECS running Windows Server 2012 as an example.

Step 1 Log in to the Windows ECS as user **Administrator**.

Step 2 Enable the local area connection.

1. In the lower right corner of the taskbar, right-click the network connection icon.
2. Click **Open Network and Sharing Center**.

Figure 11-6 Open Network and Sharing Center

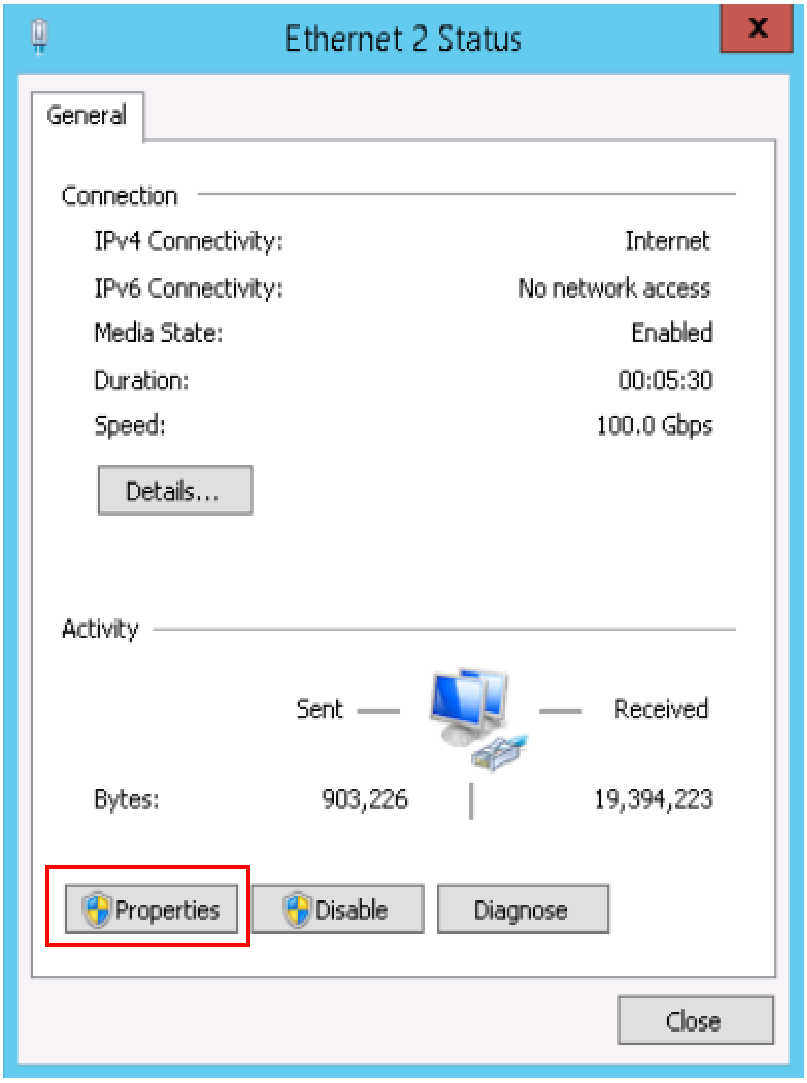


3. In the navigation pane on the left, click **Change adapter settings**.

Step 3 Configure the DNS server for the ECS.

1. Double-click network connections.
2. Click **Properties** in the lower left corner, as shown in **Figure 11-7**.

Figure 11-7 Local area connection

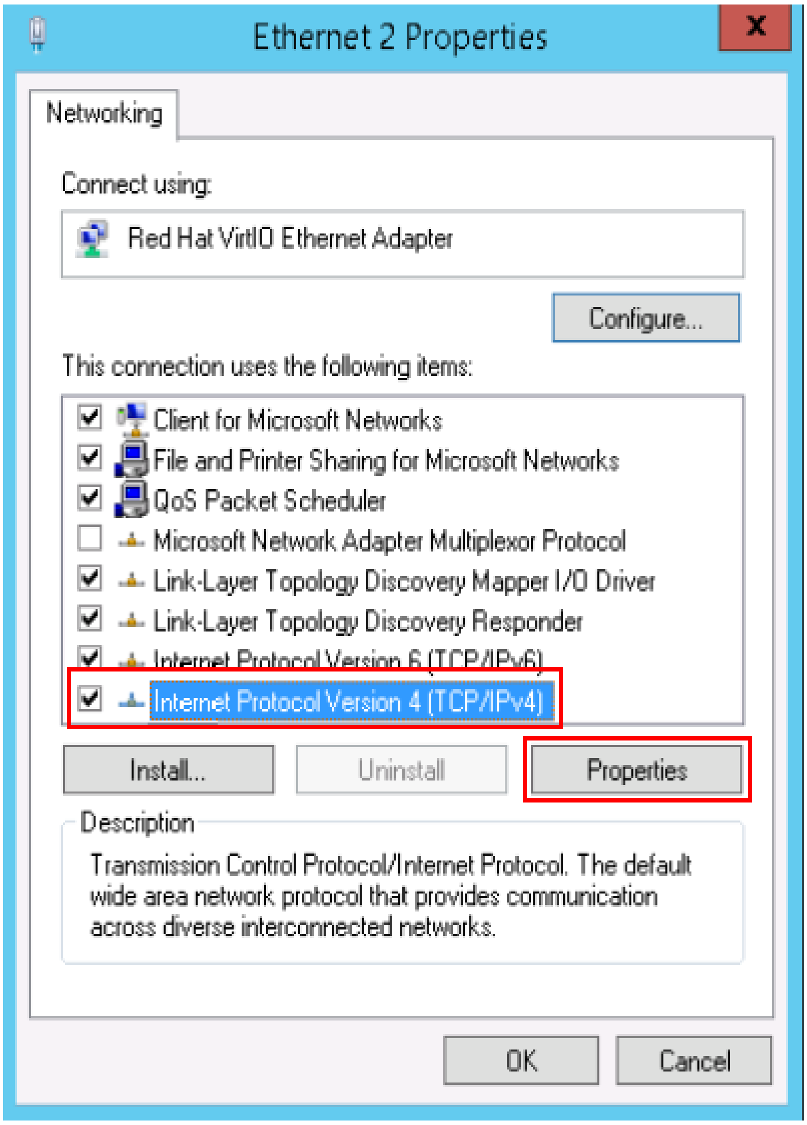


IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:05:30
Speed: 100.0 Gbps

Bytes: 903,226 19,394,223

3. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**, as shown in **Figure 11-8**.

Figure 11-8 Selecting a protocol type



Ethernet 2 Properties

Networking

Connect using:

Red Hat VirtIO Ethernet Adapter

This connection uses the following items:

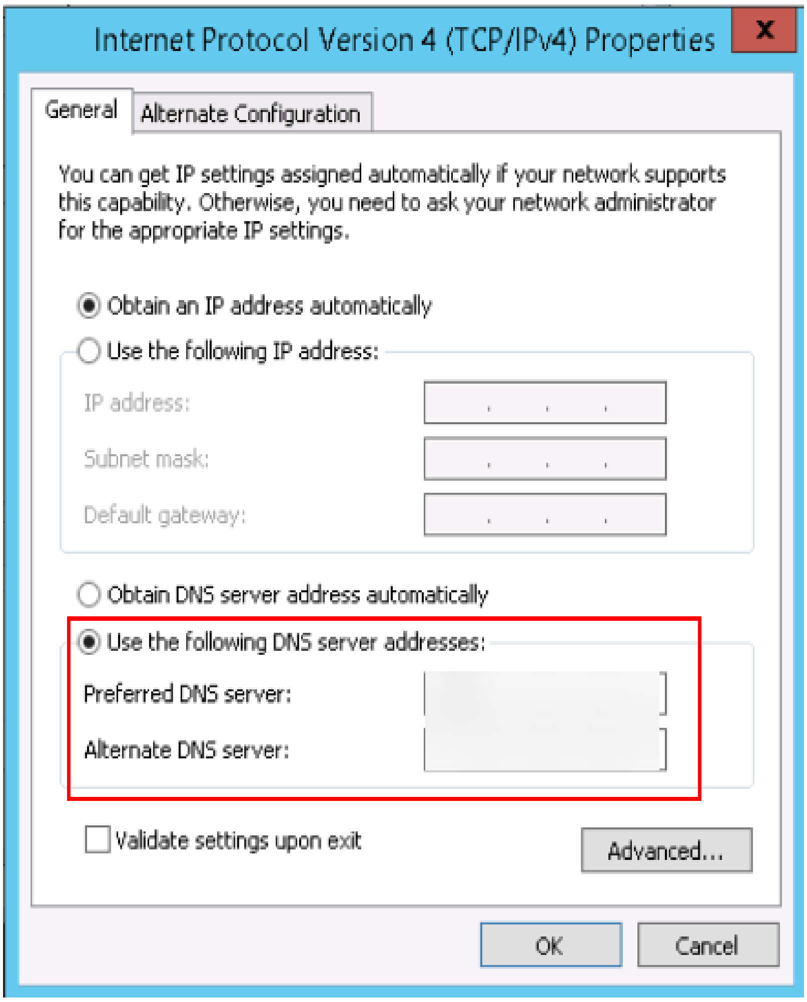
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

4. Select **Use the following DNS server addresses** and set the IP addresses of the DNS servers as prompted, as shown in **Figure 11-9**.

Figure 11-9 Setting the IP addresses of the DNS servers



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

☐ Validate settings upon exit

Step 4 Configure the NTP server for the ECS.

1. Start the **Run** dialog box. Enter **regedit** and click **OK**.
2. Modify the registry entries.
   - In **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > TimeProviders > NtpClient**, set the value of **Enabled** to **1**, indicating that the NTP client is used.
   - In **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > TimeProviders > NtpServer**, set the value of **Enabled** to **0**, indicating that the NTP server is stopped.
   - Choose the **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services** > **W32Time** > **Parameters** file and set the **NtpServer** data. For example, set its data to **ntp.myhuaweicloud.com**. Set the data of **TYPE** to **NTP**.
   - In **HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W32Time \ TimeProviders \ NtpClient**, set the value of **SpecialPollInterval** to **3600** and that of **Base** to **Decimal**, indicating the clock synchronization cycle is 3600s.
   - In **HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W32Time \ config**, set the values of **MaxPosPhaseCorrection** and **MaxNegPhaseCorrection** to **fffffff** and that of **Base** to **Hexadecimal**.

3. Open the **Run** dialog box, enter **services.msc**, and click **OK**. The **Services** window is displayed.
4. View the service named **Windows Time** and set the **Start Type** to **Automatic** to synchronize time from the NTP server.
5. Open the **Run** dialog box and run the following commands in sequence to restart the Windows Time service:

   net stop w32time

   net start w32time
6. Manually change the time on the client to make it different from that on the NTP server. One minute later, check whether the time on the client is the same as that on the NTP server. If yes, the time is synchronized.

----End

Follow-up Procedure

After the ECS is restarted, the DNS configuration is reset, and its IP address is changed to the IP address of the DNS server in the VPC subnet. Therefore, before restarting the ECS, check whether the DNS configuration in the VPC subnet is the same as the target DNS configuration. If they are different, modify the DNS configuration in the VPC subnet. For details, see **Modifying a Subnet**.

11.3 How Do I Configure DNS for an ECS?

Scenarios

Configure a DNS server for resolving the domain name of an ECS. By default, the IP address of the DNS server is automatically configured when an ECS is created. No manual configuration is needed except when the resolution fails due to a change in the DNS server IP address.

For details about DNS server IP addresses, see **What Are Huawei Cloud Private DNS Server Addresses?**

You can configure DNS for an ECS as follows:

- (Recommended) Change the DNS server address of the subnet to which the ECS belongs.
- Change the DNS server address in the ECS OS.
  - **Procedure (Linux)**
  - **Procedure (Windows)**

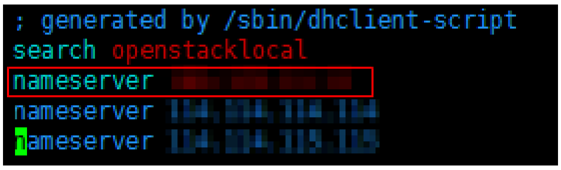
Procedure (Linux)

This section uses CentOS 7.5 as an example.

Step 1 Log in to the ECS as user **root**.

Step 2 Run the **vi /etc/resolv.conf** command to edit the **/etc/resolv.conf** file. Add the DNS server IP address above the existing nameserver information.

Figure 11-10 Configuring DNS



```
; generated by /sbin/dhclient-script
search openstacklocal
nameserver [redacted]
nameserver [redacted]
nameserver [redacted]
```

The format is as follows:

```
nameserver 100.125.1.250
```

Step 3 Press **Esc**, input **:wq**, and press **Enter** to save the changes and exit the vi editor.

Step 4 Run the following command to check whether the IP address is successfully added:

cat /etc/resolv.conf

Step 5 Run the following command to check whether an IP address can be resolved from the file system domain name:

nslookup *File system domain name*

NOTE

Obtain the file system domain name from the file system mount point.

Step 6 (Optional) In a network environment that uses the DHCP server, edit the **/etc/resolv.conf** file to prevent the file from being automatically modified upon an ECS startup, and prevent the DNS server IP address added in **Step 2** from being reset.

1. Run the following command to lock the file:

   chattr +i /etc/resolv.conf

   NOTE

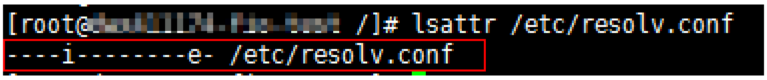
   Run the **chattr -i /etc/resolv.conf** command to unlock the file if needed.

2. Run the following command to check whether the editing is successful:

   lsattr /etc/resolv.conf

   If the information shown in **Figure 11-11** is displayed, the file is locked.

Figure 11-11 A locked file



```
[root@[redacted] /]# lsattr /etc/resolv.conf
----i--------e- /etc/resolv.conf
```

----End

Procedure (Windows)

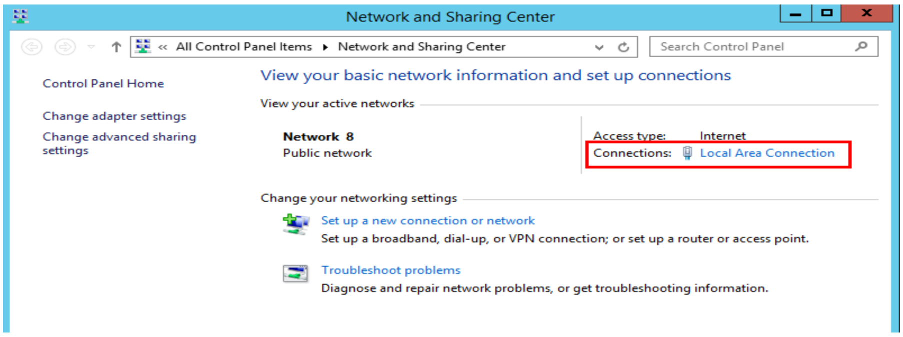
This section uses Windows Server 2012 as an example.

Step 1 Go to the ECS console and log in to the ECS running Windows Server 2012.

Step 2 Click **This PC** in the lower left corner.

Step 3 On the page that is displayed, right-click **Network** and choose **Properties** from the drop-down list. The **Network and Sharing Center** page is displayed, as shown in **Figure 11-12**. Click **Local Area Connection**.

Figure 11-12 Page for network and sharing center


Network and Sharing Center
« All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your active networks
Network 8
Public network
Access type: Internet
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Troubleshoot problems

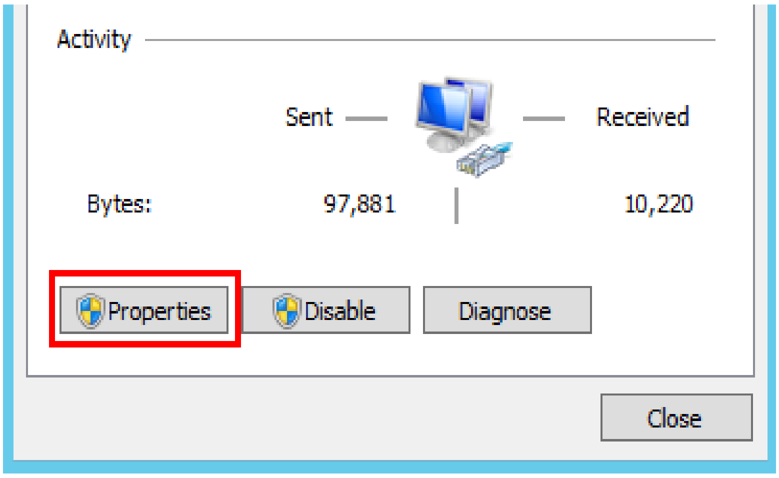
View your basic network information and set up connections

Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Diagnose and repair network problems, or get troubleshooting information.

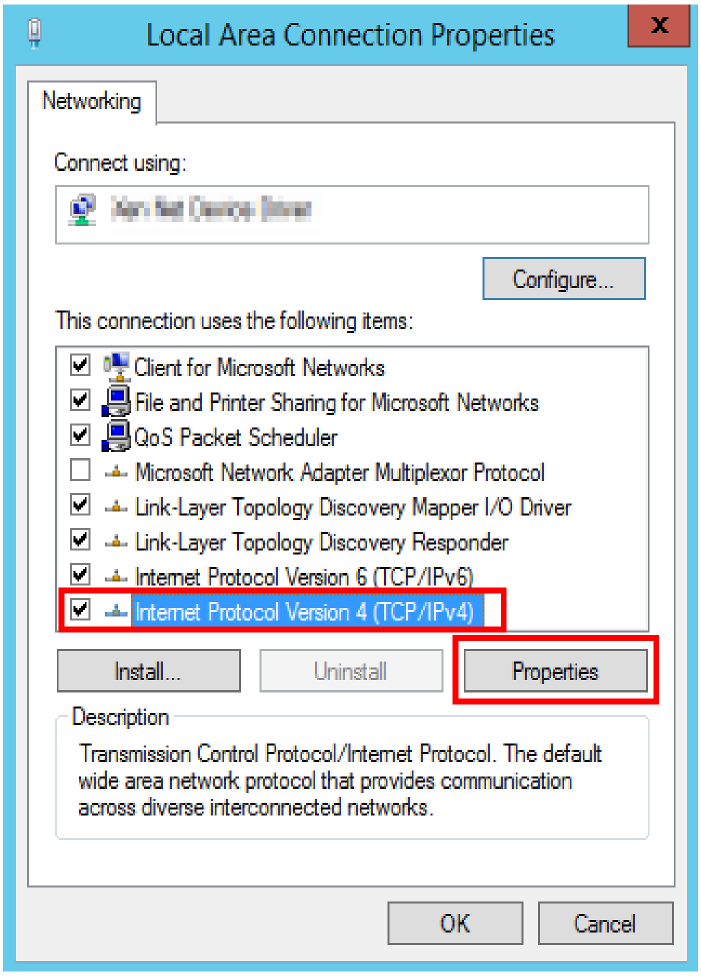
Step 4 In the **Activity** area, select **Properties**. See **Figure 11-13**.

Figure 11-13 Local area connection



Step 5 In the **Local Area Connection Properties** dialog box that is displayed, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. See **Figure 11-14**.

Figure 11-14 Local area connection properties



Connect using: [redacted]

This connection uses the following items:

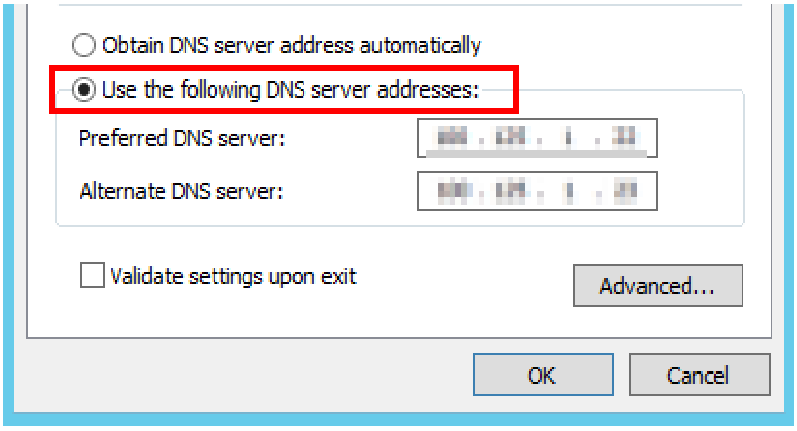
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Step 6 In the dialog box that is displayed, select **Use the following DNS server addresses:** and configure DNS, as shown in **Figure 11-15**. The DNS server IP address is 100.125.1.250. After completing the configuration, click **OK**.

Figure 11-15 Configuring DNS on Windows



○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: [redacted]

Alternate DNS server: [redacted]

☐ Validate settings upon exit

----End

11.4 Can the ECSs of Different Accounts in Different VPCs Communicate over an Intranet?

No. The ECSs of different accounts in different VPCs cannot communicate with each other over an intranet.

To enable the communication over an intranet, use the methods provided in the following table.

Scenario	Billing	Method
In the same region	Free of charge	Use VPC peering to enable the communication over an intranet. • **VPC Peering Connection Overview** • **Creating a VPC Peering Connection with a VPC in Another Account**
In different regions	Billed	Use Cloud Connect to enable the communication over an intranet. • **What Is Cloud Connect?** • **Using a Cloud Connection to Connect VPCs in Different Regions and Accounts**
In the same region	Billed	Use VPC Endpoint to enable the communication over an intranet. • **What Is VPC Endpoint?** • **Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts** • **What Are the Differences Between VPC Endpoints and VPC Peering Connections?**
In different regions	Billed	Use VPN to enable the communication over an intranet. • **What Is VPN?** • **Does a VPN Allow for Communications Between Two VPCs?**

11.5 Will My ECSs Be Deployed in the Same Subnet?

You can configure whether ECSs are in the same subnet when purchasing them.

When purchasing ECSs, you can set a VPC and primary network interface to customize the subnet for the ECSs.

You can also create a VPC and subnet in advance and deploy the ECSs in that subnet when purchasing ECSs.

11.6 How Do I Change the CIDR Block of an ECS Subnet?

Scenarios

You want to change the CIDR block of an ECS subnet. After you create a subnet, you cannot directly change its CIDR block.

To change a CIDR block, you need to change the subnet.

Prerequisites

The ECS has been stopped.

Procedure

1. Log in to the management console.
2. Under **Compute**, click **Elastic Cloud Server**.
3. In the search box above the ECS list, enter the ECS name, IP address, or ID, and click for search.
4. Click the name of the ECS whose subnet needs to be modified.

   The page providing details about the ECS is displayed.
5. Click the **NICs** tab. Locate the row containing the NIC and click **Modify Private IP**.

   The **Modify Private IP** dialog box is displayed.
6. Change the subnet and private IP address of the primary NIC as required.

   NOTE

   - You can only change to a subnet within the same VPC.
   - If you do not specify the target private IP address, the system will automatically assign one to the primary NIC.

   For example, the original subnet is **subnet-demo (192.168.0.0/24)** and the new subnet is **subnet-fe21 (192.168.6.0/25)**. Therefore, you change the ECS subnet CIDR block by changing the ECS subnet.

11.7 How Do I Configure Port Mapping?

Symptom

It is expected that the EIP and port on ECS 1 accessed from the public network can be automatically redirected to the EIP and port on ECS 2.

Windows

For example, to redirect port 8080 on ECS 1 bound with EIP 192.168.10.43 to port 18080 on ECS 2 bound with EIP 192.168.10.222, perform the following operations on ECS 1.

NOTE

Ensure that the desired ports have been enabled on the ECS security group and firewall.

1. Open the **cmd** window on the ECS and run the following command: The ECS running Windows Server 2012 is used as an example.

   netsh interface portproxy add v4tov4 listenaddress=192.168.10.43 listenport=8080 connectaddress=192.168.10.222 connectport=18080

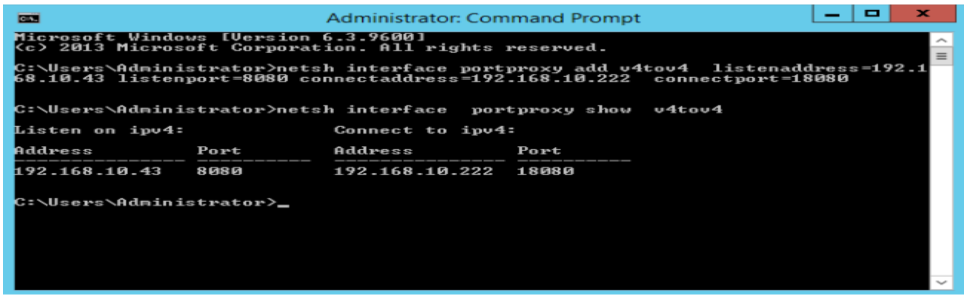
   To cancel port redirection, run the following command:

   netsh interface portproxy delete v4tov4 listenaddress=192.168.10.43 listenport=8080

2. Run the following command to view all port redirections configured on the ECS:

   netsh interface portproxy show v4tov4

Figure 11-16 Port redirections on Windows



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netsh interface portproxy add v4tov4  listenaddress=192.1
68.10.43 listenport=8080 connectaddress=192.168.10.222  connectport=18080

C:\Users\Administrator>netsh interface  portproxy show  v4tov4

Listen on ipv4:             Connect to ipv4:

Address         Port        Address         Port
--------------- ----------  --------------- ----------
192.168.10.43   8080        192.168.10.222  18080

C:\Users\Administrator>_
```

Linux

For example, to redirect port 1080 on ECS 1 to port 22 on ECS 2 with the following configurations:

Private IP address and EIP of ECS 1: 192.168.72.10 and 123.xxx.xxx.456

Private IP address of ECS 2: 192.168.72.20

NOTE

- Ensure that the desired ports have been enabled on the ECS security group and firewall.
- Ensure that the source/destination check function is disabled.

  On the ECS details page, click **Network Interfaces** and disable **Source/Destination Check**.

  By default, the source/destination check function is enabled. When this function is enabled, the system checks whether source IP addresses contained in the packets sent by ECSs are correct. If the IP addresses are incorrect, the system does not allow the ECSs to send the packets. This mechanism prevents packet spoofing, thereby improving system security. However, this mechanism prevents the packet sender from receiving returned packets. You need to disable the source/destination check.
- The operations involve modifying kernel parameters, which may cause kernel instability. Evaluate risks before performing this operation.

Step 1 Log in to Linux ECS 1.

1. Run the following command to modify the configuration file:

   vi /etc/sysctl.conf
2. Add **net.ipv4.ip_forward = 1** to the file.
3. Run the following command to complete the modification:

   sysctl -p /etc/sysctl.conf

Step 2 Run the following commands to add rules to the **nat** table in **iptables** so that the access to port 1080 on ECS 1 can be redirected to port 22 on ECS 2:

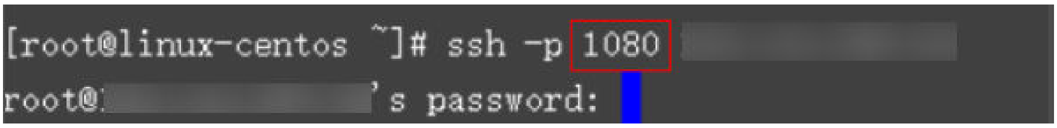
iptables -t nat -A PREROUTING -d 192.168.72.10 -p tcp --dport 1080 -j DNAT --to-destination 192.168.72.20:22

iptables -t nat -A POSTROUTING -d 192.168.72.20 -p tcp --dport 22 -j SNAT --to 192.168.72.10

Step 3 Run the following command to log in to port 1080 on ECS 1 for check:

ssh -p 1080 123.xxx.xxx.456

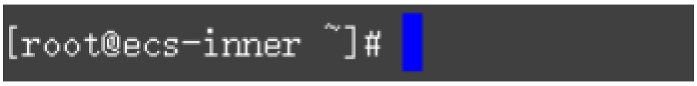
Figure 11-17 Port redirections on Linux



```
[root@linux-centos ~]# ssh -p 1080 [redacted]
root@[redacted]'s password:
```

Enter the password to log in to ECS 2 with hostname **ecs-inner**.

Figure 11-18 Logging in to ECS 2



```
[root@ecs-inner ~]#
```

----End

11.8 How Can I Obtain the MAC Address of My ECS?

This section describes how to obtain the MAC address of an ECS.

NOTE

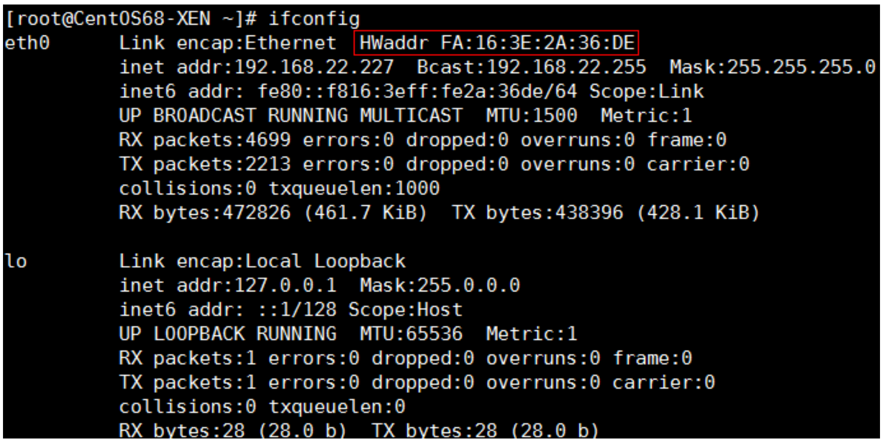
The MAC address of an ECS cannot be changed.

Linux (CentOS 6)

1. Log in to the Linux ECS.
2. Run the following command to view the MAC address of the ECS:

   ifconfig

   Figure 11-19 Obtaining the MAC address



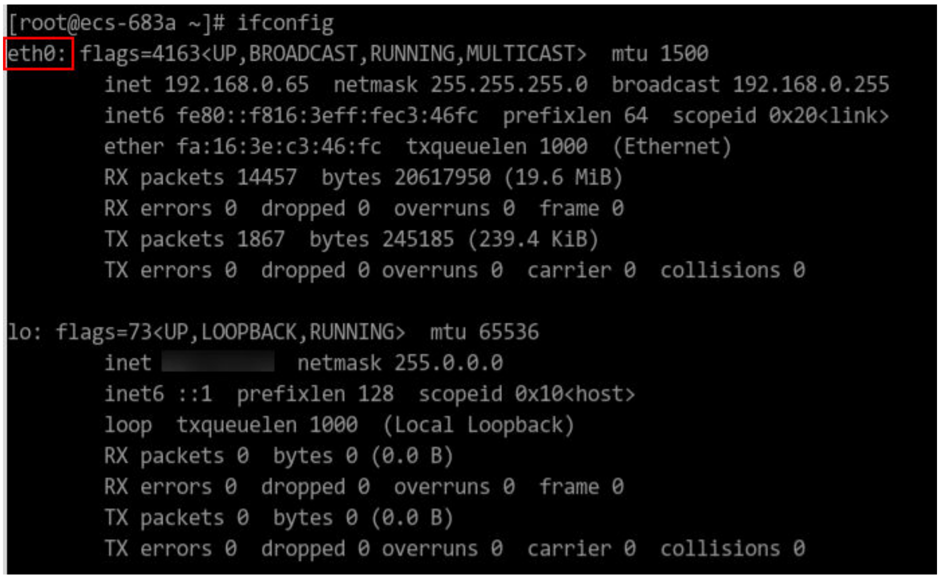
```
[root@CentOS68-XEN ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr FA:16:3E:2A:36:DE
          inet addr:192.168.22.227  Bcast:192.168.22.255  Mask:255.255.255.0
          inet6 addr: fe80::f816:3eff:fe2a:36de/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4699 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2213 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:472826 (461.7 KiB)  TX bytes:438396 (428.1 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28 (28.0 b)  TX bytes:28 (28.0 b)
```

Linux (CentOS 7)

1. Log in to the Linux ECS.
2. Run the following command to view the MAC address of the ECS:

   ifconfig

   Figure 11-20 Obtaining the NIC information

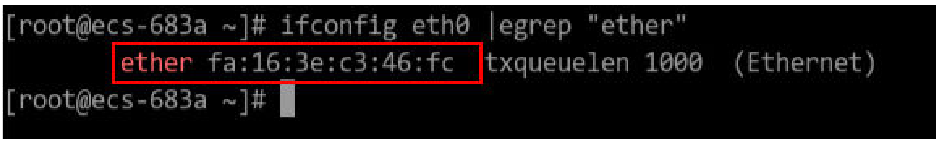


```
[root@ecs-683a ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.65  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::f816:3eff:fec3:46fc  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:c3:46:fc  txqueuelen 1000  (Ethernet)
        RX packets 14457  bytes 20617950 (19.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1867  bytes 245185 (239.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet [redacted]  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. Run the following command to view the MAC address of NIC **eth0**:

ifconfig eth0 |egrep "ether"

Figure 11-21 Obtaining the MAC address of eth0

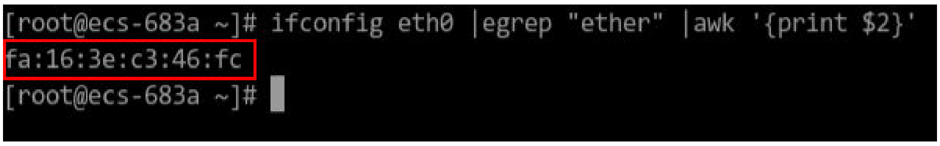


```
[root@ecs-683a ~]# ifconfig eth0 |egrep "ether"
        ether fa:16:3e:c3:46:fc  txqueuelen 1000  (Ethernet)
[root@ecs-683a ~]#
```

4. Obtain the returned MAC address.

   ifconfig eth0 |egrep "ether" |awk '{print $2}'

Figure 11-22 Obtaining the MAC address of eth0

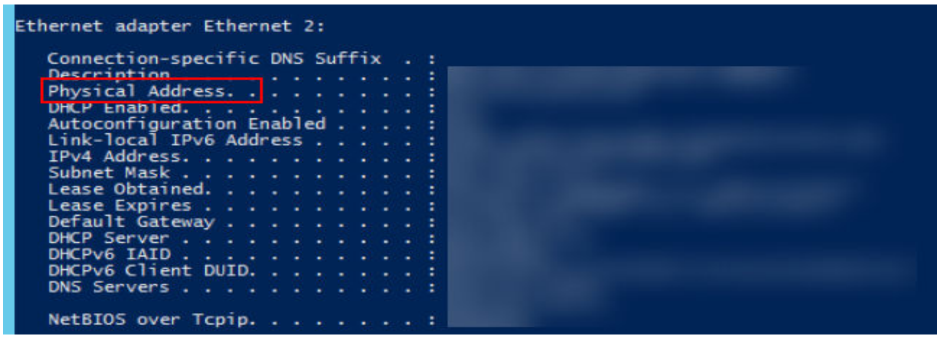


```
[root@ecs-683a ~]# ifconfig eth0 |egrep "ether" |awk '{print $2}'
fa:16:3e:c3:46:fc
[root@ecs-683a ~]#
```

Windows

1. Press **Win+R** to start the **Run** text box.
2. Enter **cmd** and click **OK**.
3. Run the following command to view the MAC address of the ECS:

   ipconfig /all



```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . :
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . :
   Autoconfiguration Enabled . . . . :
   Link-local IPv6 Address . . . . . :
   IPv4 Address. . . . . . . . . . . :
   Subnet Mask . . . . . . . . . . . :
   Lease Obtained. . . . . . . . . . :
   Lease Expires . . . . . . . . . . :
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . :
   DHCPv6 Client DUID. . . . . . . . :
   DNS Servers . . . . . . . . . . . :

   NetBIOS over Tcpip. . . . . . . . :
```

[redacted]

11.9 How Can I View and Modify Kernel Parameters of a Linux ECS?

This document describes common Linux kernel parameters and how to view and modify them.

⚠ CAUTION

Modify the kernel parameters only if the parameter settings affect your services. If the parameter settings must be modified, perform the following:

- Ensure that the target parameter settings meet service requirements.
- Modify the correct kernel parameters. For details about common kernel parameters, see **Table 11-2**.
- Back up key ECS data before modifying kernel parameter settings.

Background

Table 11-2 Common Linux kernel parameters

Parameter	Description
net.core.rmem_default	Specifies the default size (in bytes) of the window for receiving TCP data.
net.core.rmem_max	Specifies the maximum size (in bytes) of the window for receiving TCP data.
net.core.wmem_default	Specifies the default size (in bytes) of the window for transmitting TCP data.
net.core.wmem_max	Specifies the maximum size (in bytes) of the window for transmitting TCP data.
net.core.netdev_max_backlog	Specifies the maximum number of packets that can be sent to a queue when the rate at which each network port receives packets is faster than the rate at which the kernel processes these packets.
net.core.somaxconn	Defines the maximum length of the listening queue for each port in the system. This parameter applies globally.
net.core.optmem_max	Specifies the maximum size of the buffer allowed by each socket.
net.ipv4.tcp_mem	Uses the TCP stack to show memory usage in memory pages (4 KB generally). The first value is the lower limit of memory usage. The second value is the upper limit of the load added to the buffer when the memory is overloaded. The third value is the upper limit of memory usage. When this value is reached, packets can be discarded to reduce memory usage. For a large BDP, increase the parameter value as needed. The unit of this parameter is memory page but not byte.

Parameter	Description
net.ipv4.tcp_rmem	Specifies the memory used by sockets for automatic optimization. The first value is the minimum number of bytes allocated to the socket buffer for receiving data. The second value is the default value, which is overwritten by **rmem_default**. The buffer size can increase to this value when the system load is not heavy. The third value is the maximum number of bytes allocated to the socket buffer for receiving data. This value is overwritten by **rmem_max**.
net.ipv4.tcp_wmem	Specifies the memory used by sockets for automatic optimization. The first value is the minimum number of bytes allocated to the socket buffer for transmitting data. The second value is the default value, which is overwritten by **wmem_default**. The buffer size can increase to this value when the system load is not heavy. The third value is the maximum number of bytes allocated to the socket buffer for transmitting data. This value is overwritten by **wmem_max**.
net.ipv4.tcp_keepalive_time	Specifies the interval at which keepalive detection messages are sent in seconds for checking TCP connections.
net.ipv4.tcp_keepalive_intvl	Specifies the interval at which keepalive detection messages are resent in seconds when no response is received.
net.ipv4.tcp_keepalive_probes	Specifies the maximum number of keepalive detection messages that are sent to determine a TCP connection failure.
net.ipv4.tcp_sack	Enables selective acknowledgment (value **1** indicates enabled). This configuration allows the transmitter to resend only lost packets, thereby improving system performance. However, this configuration will increase the CPU usage. You are suggested to enable selective acknowledgment for WAN communication.
net.ipv4.tcp_fack	Enables forwarding acknowledgment for selective acknowledgment (SACK), thereby reducing congestion. You are suggested to enable forwarding acknowledgment.

Parameter	Description
net.ipv4.tcp_timestamps	Specifies a TCP timestamp, which will add 12 bytes in the TCP packet header. This configuration calculates RTT using RFC1323, a more precise retransmission method upon timeout than retransmission. You are suggested to enable this parameter for higher system performance.
net.ipv4.tcp_window_scaling	Enables RFC1323-based window scaling by setting the parameter value to **1** if the TCP window is larger than 64 KB. The maximum TCP window is 1 GB. This parameter takes effect only when window scaling is enabled on both ends of the TCP connection.
net.ipv4.tcp_syncookies	Specifies whether to enable TCP synchronization (**syncookie**). This configuration prevents socket overloading when a large number of connections are attempted to set up. **CONFIG_SYN_COOKIES** must be enabled in the kernel for compilation. The default value is **0**, indicating that TCP synchronization is disabled.
net.ipv4.tcp_tw_reuse	Specifies whether a **TIME-WAIT** socket (**TIME-WAIT** port) can be used for new TCP connections. **NOTE** This parameter is valid only for clients and takes effect only when **net.ipv4.tcp_timestamps** is enabled. This parameter cannot be set to **1** if NAT is enabled. Otherwise, an error will occur in remote ECS logins. For details, see **Why Are Connections to a Linux ECS Using SSH or to Applications on the ECS Interrupted Occasionally?**
net.ipv4.tcp_tw_recycle	Allows fast recycle of **TIME-WAIT** sockets. **NOTE** This parameter is valid only when **net.ipv4.tcp_timestamps** is enabled. Do not set this parameter to **1** if NAT is enabled. Otherwise, an error will occur during remote ECS logins. For details, see **Why Are Connections to a Linux ECS Using SSH or to Applications on the ECS Interrupted Occasionally?**
net.ipv4.tcp_fin_timeout	Specifies the time (in seconds) during which a socket TCP connection that is disconnected from the local end remains in the **FIN-WAIT-2** state. Process suspension may be caused by the disconnection from the peer end, continuous connection from the peer end, or other reasons.
net.ipv4.ip_local_port_range	Specifies local port numbers allowed by TCP/UDP.

Parameter	Description
net.ipv4.tcp_max_syn_backlog	Specifies the maximum number of connection requests that are not acknowledged by the peer end and that can be stored in the queue. The default value is **1024**. If the server is frequently overloaded, try to increase the value.
net.ipv4.tcp_low_latency	This option should be disabled if the TCP/IP stack is used for high throughput, low latency.
net.ipv4.tcp_westwood	Enables the congestion control algorithm on the transmitter end to evaluate throughput and improve the overall bandwidth utilization. You are suggested to enable the congestion control algorithm for WAN communication.
net.ipv4.tcp_bic	Enables binary increase congestion for fast long-distance networks so that the connections with operations being performed at a rate of Gbit/s can be functional. You are suggested to enable binary increase congestion for WAN communication.
net.ipv4.tcp_max_tw_buckets	Specifies the number of TIME_WAIT buckets, which defaults to **180000**. If the number of buckets exceeds the default value, extra ones will be cleared.
net.ipv4.tcp_synack_retries	Specifies the number of times that SYN+ACK packets are retransmitted in **SYN_RECV** state.
net.ipv4.tcp_abort_on_overflow	When this parameter is set to **1**, if the system receives a large number of requests within a short period of time but fails to process them, the system will send reset packets to terminate the connections. It is recommended that you improve system processing capabilities by optimizing the application efficiency instead of performing reset operations. Default value: **0**
net.ipv4.route.max_size	Specifies the maximum number of routes allowed by the kernel.
net.ipv4.ip_forward	Forward packets between interfaces.
net.ipv4.ip_default_ttl	Specifies the maximum number of hops that a packet can pass through.
net.netfilter.nf_conntrack_tcp_timeout_established	Clears iptables connections that are inactive for a specific period of time.
net.netfilter.nf_conntrack_max	Specifies the maximum value of hash entries.

Viewing Kernel Parameters

- Method 1: Run the cat command in **/proc/sys** to view file content.

  /proc/sys/ is a pseudo directory generated after the Linux kernel is started. The **net** folder in this directory stores all kernel parameters that have taken effect in the system. The directory tree structure is determined based on complete parameter names. For example, **net.ipv4.tcp_tw_recycle** corresponds to the **/proc/sys/net/ipv4/tcp_tw_recycle** file, and the content of the file is the parameter value.

  Example:

  To view the **net.ipv4.tcp_tw_recycle** value, run the following command:

  cat /proc/sys/net/ipv4/tcp_tw_recycle

- Method 2: Use the **/etc/sysctl.conf** file.

  Run the following command to view all parameters that have taken effect in the system:

  /usr/sbin/sysctl -a

  ```
  net.ipv4.tcp_syncookies = 1
  net.ipv4.tcp_max_tw_buckets = 4096
  net.ipv4.tcp_tw_reuse = 1
  net.ipv4.tcp_tw_recycle = 1
  net.ipv4.tcp_keepalive_time = 1800
  net.ipv4.tcp_fin_timeout = 30
  ......
  net.ipv4.tcp_keepalive_time = 1200
  net.ipv4.ip_local_port_range = 1024 65000
  net.ipv4.tcp_max_syn_backlog = 8192
  net.ipv4.tcp_rmem = 16384 174760 349520
  net.ipv4.tcp_wmem = 16384 131072 262144
  net.ipv4.tcp_mem = 262144 524288 1048576
  ......
  ```

Modifying Kernel Parameter Settings

- Method 1: Run the echo command in **/proc/sys** to modify the file for the target kernel parameters.

  The parameter values changed using this method take effect only during the current running and will be reset after the system is restarted. To make the modification take effect permanently, see method 2.

  /proc/sys/ is a pseudo directory generated after the Linux kernel is started. The **net** folder in this directory stores all kernel parameters that have taken effect in the system. The directory tree structure is determined based on complete parameter names. For example, **net.ipv4.tcp_tw_recycle** corresponds to the **/proc/sys/net/ipv4/tcp_tw_recycle** file, and the content of the file is the parameter value.

  Example:

  To change the **net.ipv4.tcp_tw_recycle** value to **0**, run the following command:

  echo "0" > /proc/sys/net/ipv4/tcp_tw_recycle

- Method 2: Use the **/etc/sysctl.conf** file.

  The parameter values changed using this method take effect permanently.

  a. Run the following command to change the value of a specified parameter:

/sbin/sysctl -w kernel.domainname="*example.com***"**

Example:

sysctl -w net.ipv4.tcp_tw_recycle="0"

b. Run the following command to change the parameter value in the **/etc/sysctl.conf** file:

vi /etc/sysctl.conf

c. Run the following command for the configuration to take effect:

/sbin/sysctl -p

11.10 Why Is the NIC Not Working?

Symptom

The NIC equipped on a D1 or H1 ECS does not work.

Possible Causes

The NIC driver has not been correctly installed.

Solution

D1 and H1 ECSs use passthrough network interfaces to improve network performance. You must install the passthrough network interface driver on the ECSs or the image that is used for creating the ECSs.

NOTE

If you mount the CD/DVD-ROM driver over a VPN, ensure that the VPN bandwidth is greater than 8 Mbit/s.

Step 1 Obtain the passthrough NIC driver.

Passthrough NIC driver versions vary depending on the OS. For details, see **Table 11-3**.

Table 11-3 NIC driver versions and OSs

NIC Driver Version	OS	How to Obtain
ixgbevf 2.16.4	CentOS 7.2 64-bit	**https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/2.16.4/**

Step 2 Log in to the ECS.

Step 3 Install the passthrough NIC driver on the ECS. In this procedure, CentOS 7.2 64-bit is used as an example.

1. Configure the passthrough NIC.

Not all ECS OSs identify passthrough NICs using the standard NIC naming rule of **eth***x*, where *x* is a number. If this is the case, you must configure the ECS so that it can identify the passthrough NIC. The procedure is as follows:

   a. Run the following command to view all NICs on the ECS and identify the passthrough NIC:

      ifconfig -a

   b. Run the following command to switch to the directory where configuration files are stored:

      cd /etc/sysconfig/network-scripts/

   c. Run the following command to create a configuration file for the passthrough NIC:

      cp ifcfg-eth0 ifcfg-*NIC_name*

      In the preceding command, *NIC_name* specifies the name of the passthrough NIC.

   d. Use the vi editor to edit this configuration file:

      vi ifcfg-*NIC_name*

   e. Set the **DEVICE** parameter in the configuration file to the name of the passthrough NIC. The following is an example configuration:

```
DEVICE="NIC_name"
BOOTPROTO="dhcp"
ONBOOT="yes"
STARTMODE="onboot"
```

   f. Run the following command to restart the network service and allow the configuration to take effect:

      service network restart

2. Upload the obtained passthrough NIC driver to a directory on the ECS, for example, **/home**.
3. Switch to user **root** on the ECS CLI and open the target directory.

   In this example, the passthrough NIC driver is stored in the **/home** directory. Run the **cd** */home* command to switch to the target directory.
4. Run the following command to decompress the software package.

   tar -zxvf *ixgbevf-2.16.4***.tar.gz**
5. Run the following command to switch to the generated **src** directory:

   cd *ixgbevf-2.16.4***/src**
6. Run the following commands to install the driver:

   make

   make install
7. Run the following command to restart the ECS to make the drive take effect:

   reboot
8. Switch to user **root** on the ECS CLI and open the **src** directory, for example, by running the **cd** */home/ixgbevf-2.16.4/src* command. Then, run the following commands to check whether the driver has been installed:

   rmmod *ixgbevf*

   insmod ./*ixgbevf***.ko**

   ethtool -i *NIC_name*

In the preceding command, *NIC_name* specifies the passthrough NIC name, for example, **ens5**.

NOTE

- After you run the **rmmod ixgbevf** command, the system may display an error message. This message does not affect the installation of the passthrough NIC driver and can be ignored.
- *NIC_name* after **ethtool -i** specifies the passthrough NIC name.

9. Check the driver status based on the displayed information.

   In this example, the driver is installed if **driver** is **ixgbevf** and **version** is **2.16.4**.

----End

11.11 Why Can't I Use DHCP to Obtain a Private IP Address?

Symptom

You attempt to use DHCP to obtain a private IP address, but you cannot obtain the IP address.

- For Linux, a private IP address cannot be assigned.
- For Windows, a private IP address is changed to an IP address in the 169.254 network segment, which is different from the private IP address displayed on the ECS console.

NOTE

You are advised to use a public image to create an ECS. All public images support DHCP continuous discovery mode.

Solution (Linux)

The following uses CentOS 7.2 as an example. For solutions about other OSs, see the corresponding help documentation.

1. Log in to the ECS and run the following command:

   ps -ef | grep dhclient

2. If the dhclient process does not exist, restart the NIC or run any of the following commands to initiate a DHCP request:

   dhclient eth0, **ifdown eth0 + ifup eth0**, or **dhcpcd eth0**

3. If the DHCP client does not send any requests for a long time, for example, the issue recurs after the NIC is restarted, do the following:

   a. Run the following command to configure a static IP:

      vi /etc/sysconfig/network-scripts/ifcfg-eth0

      ```
      BOOTPROTO=static
      IPADDR=192.168.1.100 #IP address (modified)
      NETMASK=255.255.255.0 #Mask (modified)
      GATEWAY=192.168.1.1 #Gateway IP address (modified)
      ```

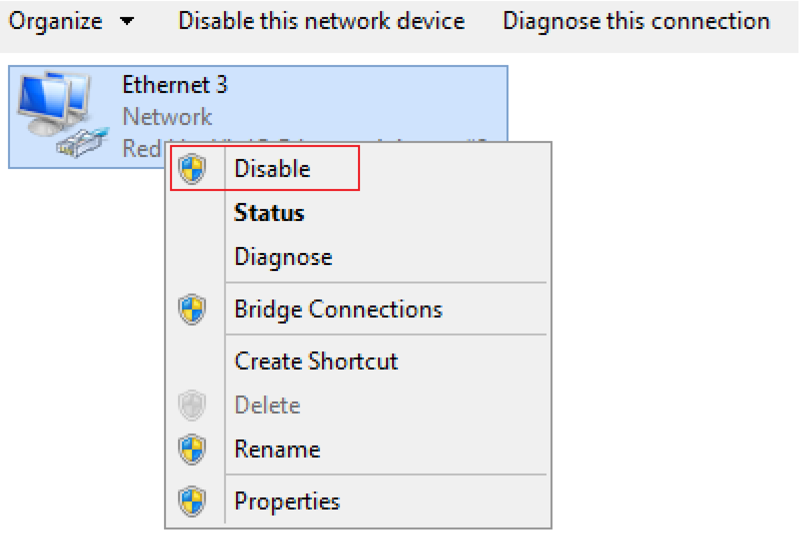
   b. Restart the ECS to make the network settings take effect.
   c. Select an image in which DHCP runs stably.

4. If the fault persists, obtain the messages in **/var/log/messages** on the affected ECS, use the MAC address of the affected NIC to filter the desired log, and check whether there is any process that prevents DHCP from obtaining an IP address.
5. If the fault persists, contact technical support.

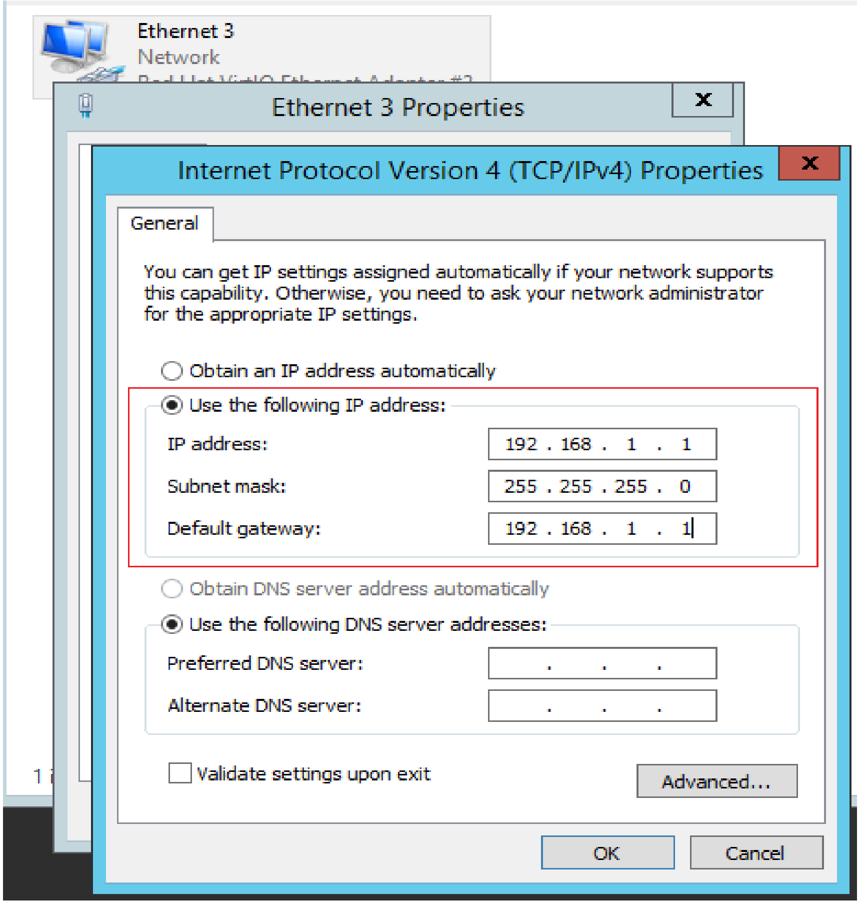
Solution (Windows)

The following uses Windows 2012 as an example. For solutions about other OSs, see the corresponding help documentation.

1. Right-click a local area connection and choose **Disable** from the shortcut menu. Then, choose **Enable**.



2. If the DHCP client does not send any requests for a long time, for example, the issue recurs after the NIC is restarted, do the following:
   a. Right-click **Local Area Connection** and choose **Properties** from the shortcut menu.
   b. In the displayed dialog box, select **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties**, and modify parameter settings.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit

c. Restart the ECS to make the network settings take effect.

3. If the fault persists, contact technical support.

11.12 How Can I Test the Network Performance of Linux ECSs?

Use netperf and iperf3 to test network performance between ECSs. The test operations include preparations, TCP bandwidth test, UDP PPS test, and latency test.

Background

- Tested ECS: an ECS that is tested for network performance. Such an ECS functions as the client (TX end) or server (RX end) in netperf tests.
- Auxiliary ECSs: an ECS that is used to exchange test data with the tested ECS. The auxiliary ECS functions as the client (TX end) or server (RX end) in netperf tests.
- **Table 11-4** and **Table 11-5** list the common netperf and iperf3 parameters.

Table 11-4 Common netperf parameters

Parameter	Description
-p	Port number
-H	IP address of the RX end
-t	Protocol used in packet transmitting, the value of which is **TCP_STREAM** in bandwidth tests
-l	Test duration
-m	Data packet size, which is suggested to be **1440** in bandwidth tests

Table 11-5 Common iperf3 parameters

Parameter	Description
-p	Port number
-c	IP address of the RX end
-u	UDP packets
-b	TX bandwidth
-t	Test duration
-l	Data packet size, which is suggested to be **16** in PPS tests
-A	ID of the vCPU used by iperf3 In this section, the maximum number of 16 vCPUs is used as an example for each ECS. If an ECS has 8 vCPUs, the **-A** value ranges from 0 to 7.

Test Preparations

Step 1 Prepare ECSs.

Ensure that both type and specifications of the tested ECS and auxiliary ECSs are the same. In addition, ensure that these ECSs are deployed in the same ECS group with anti-affinity enabled.

Table 11-6 Preparations

Category	Quantity	Image	Specifications	IP Address
Tested ECS	1	CentOS 7.4 64-bit (recommended)	N/A	192.168.2.10

Category	Quantity	Image	Specifications	IP Address
Auxiliary ECS	8	CentOS 7.4 64-bit (recommended)	At least 8 vCPUs	192.168.2.11-192.168.2.18

Step 2 Install the netperf, iperf3, and sar test tools on both the tested ECS and auxiliary ECSs.

Table 11-7 lists the procedures for installing these tools.

Table 11-7 Installing test tools

Tool	Procedure
netperf	1. Run the following command to install gcc: **yum -y install unzip gcc gcc-c++** 2. Run the following command to download the netperf installation package: **wget https://github.com/HewlettPackard/netperf/archive/refs/tags/netperf-2.7.0.zip** 3. Run the following commands to decompress the installation package and install netperf: **unzip netperf-2.7.0.zip** **cd netperf-netperf-2.7.0/** **./configure && make && make install**
iperf3	1. Run the following command to download the iperf3 installation package: **wget --no-check-certificate https://codeload.github.com/esnet/iperf/zip/master -O iperf3.zip** 2. Run the following commands to decompress the installation package and install iperf3: **unzip iperf3.zip** **cd iperf-master/** **./configure && make && make install**
sar	Run the following command to install sar: **yum -y install sysstat**

Step 3 Enable NIC multi-queue.

Perform the following operations on both tested ECS and auxiliary ECSs.

1. Run the following command to check the number of queues supported by the ECSs:

   ethtool -l eth0 | grep -i Pre -A 5 | grep Combined

2. Run the following command to enable NIC multi-queue:

   ethtool -L eth0 combined *X*

In the preceding command, *X* is the number of queues obtained in **Step 3.1**.

----End

TCP Bandwidth Test (Using netperf)

Perform the test on multiple flows. This section considers 16 flows that are evenly distributed to eight ECSs, as an example.

NOTE

The TCP bandwidth test uses the multi-flow model.

- When testing the TCP transmission (TX) bandwidth, use the one-to-many model to ensure that the capability of the receiver is sufficient.
- When testing the TCP receiver (RX) bandwidth, use the many-to-one model to ensure that the capability of the sender is sufficient.

Step 1 Test the TCP TX bandwidth.

1. Run the following commands on all auxiliary ECSs to start the netserver process:

```
netserver -p 12001
netserver -p 12002
```

   In the preceding commands, **-p** specifies the listening port.

2. Start the netperf process on the tested ECS and specify a netserver port for each auxiliary ECS. For details about common netperf parameters, see **Table 11-4**.

```
##The IP address is for the first auxiliary ECS.
netperf -H 192.168.2.11 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
netperf -H 192.168.2.11 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &

##The IP address is for the second auxiliary ECS.
netperf -H 192.168.2.12 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
netperf -H 192.168.2.12 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &

##The IP address is for the third auxiliary ECS.
netperf -H 192.168.2.13 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
netperf -H 192.168.2.13 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &

##The IP address is for the fourth auxiliary ECS.
netperf -H 192.168.2.14 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
netperf -H 192.168.2.14 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &

##The IP address is for the fifth auxiliary ECS.
netperf -H 192.168.2.15 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
netperf -H 192.168.2.15 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &

##The IP address is for the sixth auxiliary ECS.
netperf -H 192.168.2.16 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
netperf -H 192.168.2.16 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &

##The IP address is for the seventh auxiliary ECS.
```

```
netperf -H 192.168.2.17 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
netperf -H 192.168.2.17 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

##The IP address is for the eighth auxiliary ECS.

```
netperf -H 192.168.2.18 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
netperf -H 192.168.2.18 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

Step 2 Test the TCP RX bandwidth.

1. Start the netserver process on the tested ECS.

   ##The port number is for the first auxiliary ECS.

   ```
   netserver -p 12001
   netserver -p 12002
   ```

   ##The port number is for the second auxiliary ECS.

   ```
   netserver -p 12003
   netserver -p 12004
   ```

   ##The port number is for the third auxiliary ECS.

   ```
   netserver -p 12005
   netserver -p 12006
   ```

   ##The port number is for the fourth auxiliary ECS.

   ```
   netserver -p 12007
   netserver -p 12008
   ```

   ##The port number is for the fifth auxiliary ECS.

   ```
   netserver -p 12009
   netserver -p 12010
   ```

   ##The port number is for the sixth auxiliary ECS.

   ```
   netserver -p 12011
   netserver -p 12012
   ```

   ##The port number is for the seventh auxiliary ECS.

   ```
   netserver -p 12013
   netserver -p 12014
   ```

   ##The port number is for the eighth auxiliary ECS.

   ```
   netserver -p 12015
   netserver -p 12016
   ```

2. Start the netperf process on all auxiliary ECSs.

   Log in to auxiliary ECS 1.

   ```
   netperf -H 192.168.2.10 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
   netperf -H 192.168.2.10 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
   ```

   Log in to auxiliary ECS 2.

   ```
   netperf -H 192.168.2.10 -p 12003 -t TCP_STREAM -l 300 -- -m 1440 &
   netperf -H 192.168.2.10 -p 12004 -t TCP_STREAM -l 300 -- -m 1440 &
   ```

Log in to auxiliary ECS 3.

netperf -H 192.168.2.10 -p 12005 -t TCP_STREAM -l 300 -- -m 1440 &

netperf -H 192.168.2.10 -p 12006 -t TCP_STREAM -l 300 -- -m 1440 &

Log in to auxiliary ECS 4.

netperf -H 192.168.2.10 -p 12007 -t TCP_STREAM -l 300 -- -m 1440 &

netperf -H 192.168.2.10 -p 12008 -t TCP_STREAM -l 300 -- -m 1440 &

Log in to auxiliary ECS 5.

netperf -H 192.168.2.10 -p 12009 -t TCP_STREAM -l 300 -- -m 1440 &

netperf -H 192.168.2.10 -p 12010 -t TCP_STREAM -l 300 -- -m 1440 &

Log in to auxiliary ECS 6.

netperf -H 192.168.2.10 -p 12011 -t TCP_STREAM -l 300 -- -m 1440 &

netperf -H 192.168.2.10 -p 12012 -t TCP_STREAM -l 300 -- -m 1440 &

Log in to auxiliary ECS 7.

netperf -H 192.168.2.10 -p 12013 -t TCP_STREAM -l 300 -- -m 1440 &

netperf -H 192.168.2.10 -p 12014 -t TCP_STREAM -l 300 -- -m 1440 &

Log in to auxiliary ECS 8.

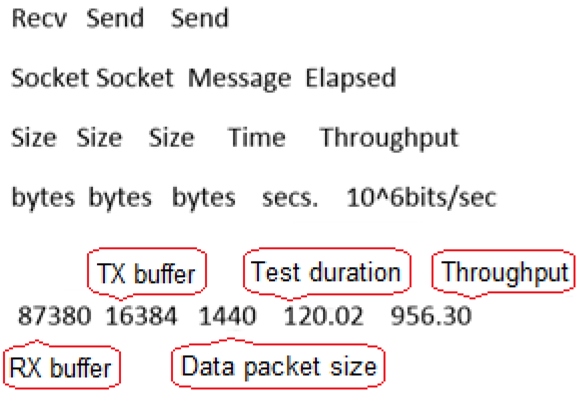
netperf -H 192.168.2.10 -p 12015 -t TCP_STREAM -l 300 -- -m 1440 &

netperf -H 192.168.2.10 -p 12016 -t TCP_STREAM -l 300 -- -m 1440 &

Step 3 Analyze the test result.

After the test is complete, the output of the netperf process on one TX end is shown in **Figure 11-23**. The final result is the sum of the test results of the netperf processes on all TX ends.

Figure 11-23 Output of the netperf process on one TX end



```
Recv  Send   Send

Socket Socket  Message  Elapsed

Size   Size    Size     Time     Throughput

bytes  bytes   bytes    secs.    10^6bits/sec

87380  16384   1440     120.02   956.30
```

NOTE

There are a large number of netperf processes. To facilitate statistics collection, it is a good practice to run the following command to view test data on the tested ECS using sar:

sar -n DEV 1 60

----End

UDP PPS Test (Using iperf3)

Step 1 Test the UDP TX PPS.

1. Log in to an auxiliary ECS.
2. Run the following commands on all auxiliary ECSs to start the server process:

   ```
   iperf3 -s -p 12001 &
   iperf3 -s -p 12002 &
   ```

   In the preceding commands, **-p** specifies the listening port.
3. Start the client process on the tested ECS. For details about common iperf3 parameters, see **Table 11-5**.

   ```
   ##Auxiliary ECS 1
   iperf3 -c 192.168.2.11 -p 12001 -u -b 100M -t 300 -l 16 -A 0 &
   iperf3 -c 192.168.2.11 -p 12002 -u -b 100M -t 300 -l 16 -A 1 &
   ##Auxiliary ECS 2
   iperf3 -c 192.168.2.12 -p 12001 -u -b 100M -t 300 -l 16 -A 2 &
   iperf3 -c 192.168.2.12 -p 12002 -u -b 100M -t 300 -l 16 -A 3 &

   ##Auxiliary ECS 3
   iperf3 -c 192.168.2.13 -p 12001 -u -b 100M -t 300 -l 16 -A 4 &
   iperf3 -c 192.168.2.13 -p 12002 -u -b 100M -t 300 -l 16 -A 5 &

   ##Auxiliary ECS 4
   iperf3 -c 192.168.2.14 -p 12001 -u -b 100M -t 300 -l 16 -A 6 &
   iperf3 -c 192.168.2.14 -p 12002 -u -b 100M -t 300 -l 16 -A 7 &

   ##Auxiliary ECS 5
   iperf3 -c 192.168.2.15 -p 12001 -u -b 100M -t 300 -l 16 -A 8 &
   iperf3 -c 192.168.2.15 -p 12002 -u -b 100M -t 300 -l 16 -A 9 &

   ##Auxiliary ECS 6
   iperf3 -c 192.168.2.16 -p 12001 -u -b 100M -t 300 -l 16 -A 10 &
   iperf3 -c 192.168.2.16 -p 12002 -u -b 100M -t 300 -l 16 -A 11 &

   ##Auxiliary ECS 7
   iperf3 -c 192.168.2.17 -p 12001 -u -b 100M -t 300 -l 16 -A 12 &
   iperf3 -c 192.168.2.17 -p 12002 -u -b 100M -t 300 -l 16 -A 13 &

   ##Auxiliary ECS 8
   iperf3 -c 192.168.2.18 -p 12001 -u -b 100M -t 300 -l 16 -A 14 &
   iperf3 -c 192.168.2.18 -p 12002 -u -b 100M -t 300 -l 16 -A 15 &
   ```

Step 2 Test the UDP RX PPS.

1. Start the server process on the tested ECS. For details about common iperf3 parameters, see **Table 11-5**.

```
##The port number is for the first auxiliary ECS.
iperf3 -s -p 12001 -A 0 -i 60 &
iperf3 -s -p 12002 -A 1 -i 60 &

##The port number is for the second auxiliary ECS.
iperf3 -s -p 12003 -A 2 -i 60 &
iperf3 -s -p 12004 -A 3 -i 60 &

##The port number is for the third auxiliary ECS.
iperf3 -s -p 12005 -A 4 -i 60 &
iperf3 -s -p 12006 -A 5 -i 60 &

##The port number is for the fourth auxiliary ECS.
iperf3 -s -p 12007 -A 6 -i 60 &
iperf3 -s -p 12008 -A 7 -i 60 &

##The port number is for the fifth auxiliary ECS.
iperf3 -s -p 12009 -A 8 -i 60 &
iperf3 -s -p 12010 -A 9 -i 60 &

##The port number is for the sixth auxiliary ECS.
iperf3 -s -p 12011 -A 10 -i 60 &
iperf3 -s -p 12012 -A 11 -i 60 &

##The port number is for the seventh auxiliary ECS.
iperf3 -s -p 12013 -A 12 -i 60 &
iperf3 -s -p 12014 -A 13 -i 60 &

##The port number is for the eighth auxiliary ECS.
iperf3 -s -p 12015 -A 14 -i 60 &
iperf3 -s -p 12016 -A 15 -i 60 &
```

2. Start the client process on all auxiliary ECSs. For details about common iperf3 parameters, see **Table 11-5**.

   Log in to auxiliary ECS 1.

```
iperf3 -c 192.168.2.10 -p 12001 -u -b 100M -t 300 -l 16 -A 0 &
iperf3 -c 192.168.2.10 -p 12002 -u -b 100M -t 300 -l 16 -A 1 &
```

   Log in to auxiliary ECS 2.

```
iperf3 -c 192.168.2.10 -p 12003 -u -b 100M -t 300 -l 16 -A 0 &
iperf3 -c 192.168.2.10 -p 12004 -u -b 100M -t 300 -l 16 -A 1 &
```

   Log in to auxiliary ECS 3.

```
iperf3 -c 192.168.2.10 -p 12005 -u -b 100M -t 300 -l 16 -A 0 &
iperf3 -c 192.168.2.10 -p 12006 -u -b 100M -t 300 -l 16 -A 1 &
```

   Log in to auxiliary ECS 4.

iperf3 -c 192.168.2.10 -p 12007 -u -b 100M -t 300 -l 16 -A 0 &

iperf3 -c 192.168.2.10 -p 12008 -u -b 100M -t 300 -l 16 -A 1 &

Log in to auxiliary ECS 5.

iperf3 -c 192.168.2.10 -p 12009 -u -b 100M -t 300 -l 16 -A 0 &

iperf3 -c 192.168.2.10 -p 12010 -u -b 100M -t 300 -l 16 -A 1 &

Log in to auxiliary ECS 6.

iperf3 -c 192.168.2.10 -p 12011 -u -b 100M -t 300 -l 16 -A 0 &

iperf3 -c 192.168.2.10 -p 12012 -u -b 100M -t 300 -l 16 -A 1 &

Log in to auxiliary ECS 7.

iperf3 -c 192.168.2.10 -p 12013 -u -b 100M -t 300 -l 16 -A 0 &

iperf3 -c 192.168.2.10 -p 12014 -u -b 100M -t 300 -l 16 -A 1 &

Log in to auxiliary ECS 8.

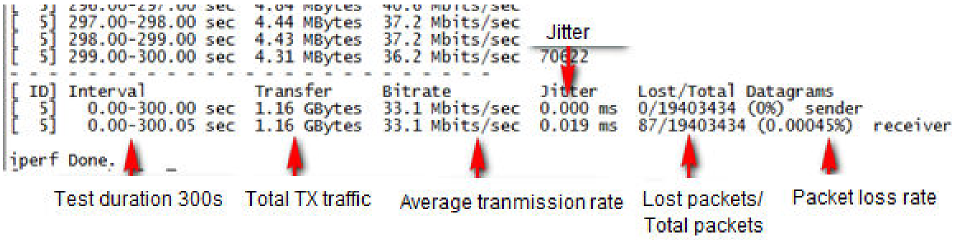
iperf3 -c 192.168.2.10 -p 12015 -u -b 100M -t 300 -l 16 -A 0 &

iperf3 -c 192.168.2.10 -p 12016 -u -b 100M -t 300 -l 16 -A 1 &

Step 3 Analyze the test result.

Figure 11-24 shows an example of the UDP PPS test result.

Figure 11-24 UDP PPS test result



```
[  5] 297.00-298.00 sec  4.44 MBytes  37.2 Mbits/sec
[  5] 298.00-299.00 sec  4.43 MBytes  37.2 Mbits/sec
[  5] 299.00-300.00 sec  4.31 MBytes  36.2 Mbits/sec  70622
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-300.00 sec  1.16 GBytes  33.1 Mbits/sec  0.000 ms  0/19403434 (0%)  sender
[  5]   0.00-300.05 sec  1.16 GBytes  33.1 Mbits/sec  0.019 ms  87/19403434 (0.00045%)  receiver

iperf Done.
```

NOTE

There are a large number of iperf3 processes. To facilitate statistics collection, it is a good practice to run the following command to view test data on the tested ECS using sar:

sar -n DEV 1 60

----End

Latency Test

Step 1 Run the following command to start the qperf process on the tested ECS:

qperf &

Step 2 Log in to auxiliary ECS 1 and run the following command to perform a latency test:

qperf 192.168.2.10 -m 64 -t 60 -vu udp_lat

After the test is complete, the **lat** value in the command output is the latency between ECSs.

----End

11.13 What Should I Do If NIC Flapping Occurs After My ECS Specifications Are Modified?

Symptom

Take a Linux ECS as an example. After the user modified ECS specifications and ran the **ifconfig** command, the user found that the original eth0 and eth1 NICs were changed to eth2 and eth3 NICs, indicating that NIC flapping occurred.

Root Cause

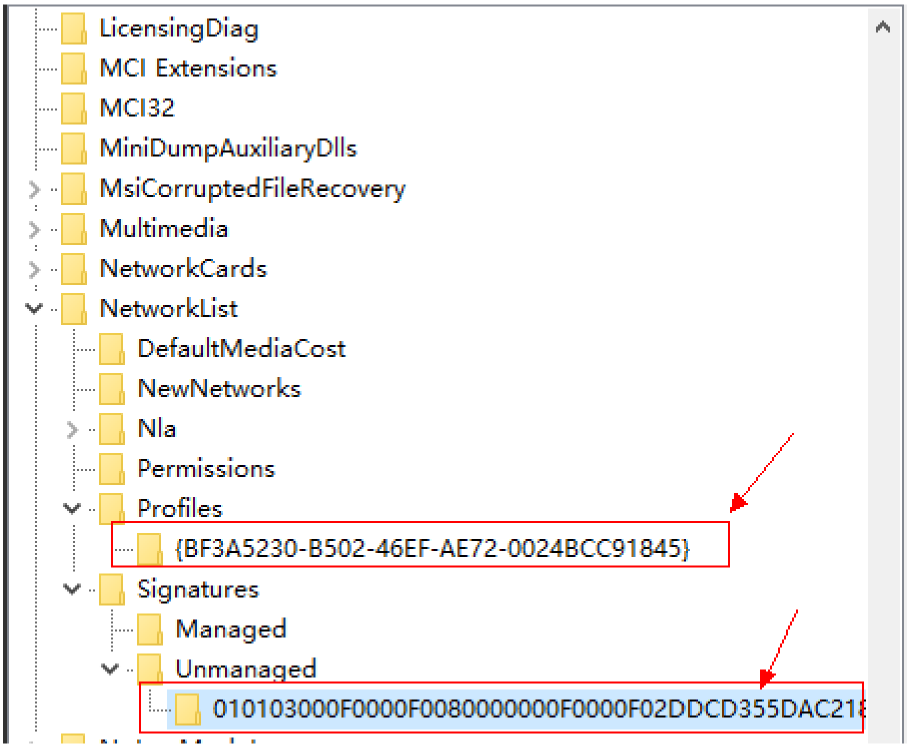
NIC flapping occurs because NIC retaining is enabled in the image from which the ECS is created.

Solution to Windows

For a Windows ECS, delete the directories in the following registries and restart the ECS to resolve this issue:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged



Solution to Linux

For a Linux ECS, perform the following operations and restart the ECS to resolve this issue:

1. Run the following command to view the files in the network rule directory:
   ```
   ls -l /etc/udev/rules.d
   ```
2. Run the following commands to delete the files with both **persistent** and **net** included in file names from the network rule directory:
   ```
   rm -fr /etc/udev/rules.d/*net*persistent*.rules
   ```
   ```
   rm -fr /etc/udev/rules.d/*persistent*net*.rules
   ```
3. Run the following command to check whether the initrd image file with a name starting with **initrd** and ending with **default** contains both **persistent** and **net** network rules (change the italic data in the following command to the actual OS version):
   ```
   lsinitrd /boot/initrd-2.6.32.12-0.7-default |grep persistent|grep net
   ```
   - If yes, go to steps **4** and **5**.
   - If no, no further action is required.
4. Run the following command to back up the initrd image file (change the italic data in the following command to the actual OS version):
   ```
   cp /boot/initrd-2.6.32.12-0.7-default /boot/initrd-2.6.32.12-0.7-default_bak
   ```
5. Run the following command to regenerate the initrd image file:
   ```
   mkinitrd
   ```

Perform the following operations when an OS, such as Ubuntu, uses the initramfs image:

1. Run the following command to check whether the initramfs image file with a name starting with **initrd** and ending with **generic** contains both **persistent** and **net** network rules:
   ```
   lsinitramfs /boot/initrd.img-3.19.0-25-generic|grep persistent|grep net
   ```
   - If yes, go to steps **2** and **3**.
   - If no, no further action is required.
2. Run the following command to back up the initrd image file:
   ```
   cp /boot/initrd.img-3.19.0-25-generic /boot/initrd.img-3.19.0-25-generic_bak
   ```
3. Run the following command to regenerate the initramfs image file:
   ```
   update-initramfs -u
   ```

11.14 Will NICs Added to an ECS Start Automatically?

Based on test results, if the ECS runs CentOS 7.0, NICs added to the ECS cannot start automatically. You must start the NICs manually.

11.15 How Can I Check Whether the Network Communication Is Normal Between Two ECSs Equipped with an InfiniBand NIC Driver?

For high-performance H2 ECSs equipped with an InfiniBand NIC driver (InfiniBand ECSs for short), perform the following operations to check whether the driver installation is successful and whether the network communication between the ECSs is normal.

NOTE

During the check, if your ECS has no command tool installed, such as ibstat, obtain the tool from the installation package for the InfiniBand NIC driver and install the tool.

Step 1 Check whether the NICs of the InfiniBand ECSs are functional.

1. Log in to the ECS.
2. Run the following command to check whether the NIC is functional:

   ibstat

   - If it is functional, go to step **Step 2**.
   - If it is not functional, contact customer service for technical support.

Step 2 Check whether the network communication between two InfiniBand ECSs is normal.

1. Log in to one InfiniBand ECS and run the following command:

   ib_write_bw -x 0 --pkey_index 0

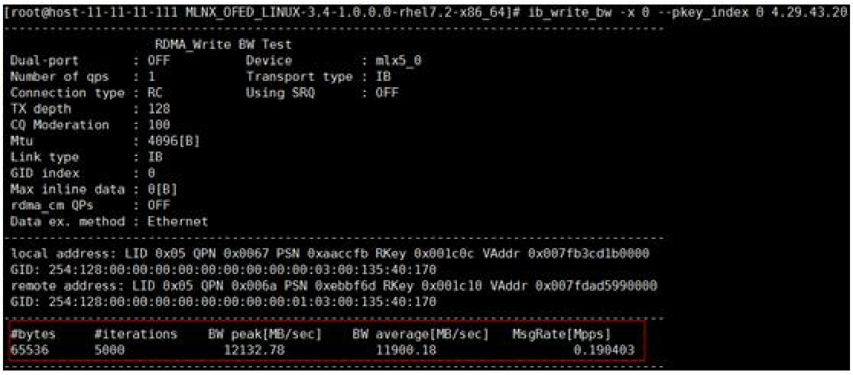
2. Log in to the other InfiniBand ECS and run the following command:

   ib_write_bw -x 0 --pkey_index 0*ip_addr*

   In the preceding command, *ip_addr* is the NIC IP address of the first InfiniBand ECS.

3. Check whether the terminal display is correct.

Figure 11-25 Normal network communication



```
[root@host-11-11-11-111 MLNX_OFED_LINUX-3.4-1.0.0.0-rhel7.2-x86_64]# ib_write_bw -x 0 --pkey_index 0 4.29.43.20
---------------------------------------------------------------------------------------
                    RDMA_Write BW Test
 Dual-port       : OFF          Device         : mlx5_0
 Number of qps   : 1            Transport type : IB
 Connection type : RC           Using SRQ      : OFF
 TX depth        : 128
 CQ Moderation   : 100
 Mtu             : 4096[B]
 Link type       : IB
 GID index       : 0
 Max inline data : 0[B]
 rdma_cm QPs     : OFF
 Data ex. method : Ethernet
---------------------------------------------------------------------------------------
 local address: LID 0x05 QPN 0x0067 PSN 0xaaccfb RKey 0x001c0c VAddr 0x007fb3cd1b0000
 GID: 254:128:00:00:00:00:00:00:00:00:00:03:00:135:40:170
 remote address: LID 0x05 QPN 0x006a PSN 0xebbf6d RKey 0x001c10 VAddr 0x007fdad5990000
 GID: 254:128:00:00:00:00:00:00:00:00:01:03:00:135:40:170
---------------------------------------------------------------------------------------
 #bytes     #iterations    BW peak[MB/sec]    BW average[MB/sec]   MsgRate[Mpps]
 65536      5000             12132.78           11900.18             0.190403
---------------------------------------------------------------------------------------
```

   - If the terminal display is shown in **Figure 11-25**, the network communication between the two InfiniBand ECSs is normal.

- If the InfiniBand network is inaccessible, contact customer service for technical support.

----End

11.16 How Can I Manually Configure an IP Address for an InfiniBand NIC?

IP over InfiniBand (IPoIB) allows IP data transmission over InfiniBand. For SUSE high-performance H2 and HL1 ECSs, if IPoIB is required, you must manually configure an IP address for the InfiniBand NIC after installing the InfiniBand NIC driver.

Prerequisites

The InfiniBand NIC driver has been installed on the high-performance H2 or HL1 ECSs.

Background

To prevent IP address conflict of the InfiniBand NICs configured for the ECSs of a tenant, determine the IP address to be configured for an InfiniBand NIC according to the IP addresses available in the VPC. The method is as follows:

For example, if the first two eight-bits of the IP address (specified by **IPADDR**) to be configured for the InfiniBand NIC are consistently **169.254**, the latter two eight-bits must be the same as those of the **eth0** IP address, and the subnet mask must be the same as that of the **eth0** NIC.

An example is provided as follows:

If the IP address of the **eth0** NIC is 192.168.0.100/24, the IP address to be configured for the InfiniBand NIC is 169.254.0.100/24.

Procedure

1. Log in to the ECS.
2. Run the following command to switch to user **root**:

   sudo su -
3. Run the following command to edit the **/etc/sysconfig/network/ifcfg-ib0** file:

   vi /etc/sysconfig/network/ifcfg-ib0
4. Enter the following information:

   DEVICE=ib0

   BOOTPROTO=static

   IPADDR=*IP address to be configured for the InfiniBand NIC*

   NETMASK=*Subnet mask*

   STARTMODE=auto

NOTE

For instructions about how to obtain the IP address and subnet mask for an InfiniBand NIC, see **Background**.

5. Run the following command to restart the network for the configuration to take effect:

   service network restart

11.17 How Can I Handle the Issue that a Windows 7 ECS Equipped with an Intel 82599 NIC Reports an Error in SR-IOV Scenarios?

Symptom

When the 20.4.1 driver package downloaded at Intel website **https://downloadcenter.intel.com/search?keyword=Intel++Ethernet+Connections+CD** was installed in a Windows 7 64bit ECS with SR-IOV passthrough enabled, the system displayed the message "No Intel adapter found".

Cause Analysis

The OS identifies an Intel 82599 passthrough NIC without a driver installed as an Ethernet controller. When the 20.4.1 driver package was installed, the OS did not identify the Intel NIC, leading to the error.

Solution

Run **Autorun.exe** in the folder where the 20.4.1 driver package is stored. Install a driver on the NIC before installing the driver package so that the NIC can be identified as an Intel 82599 virtual function (VF) device by the OS. Use either of the following methods to install the driver:

- Method 1: Update the version.
  a. Download the 18.6 driver package at the Intel website.
  b. Run **Autorun.exe**.
  c. Run **Autorun.exe** in the folder where the 20.4.1 driver package is stored to update the driver.
- Method 2: Use the device manager.
  a. Start the Windows resource manager. Right-click **Computer** and choose **Manage** from the shortcut menu. In the **Device Manager** window, locate the NIC. When the NIC has no driver installed, the NIC locates in **Other devices** and is named **Ethernet Controller**.
  b. Right-click **Ethernet Controller** and choose **Update Driver Software**.
  c. Click **Browse**, select the path where the driver package is stored, and click **Next**.
  d. Locate the NIC in **Network Adapter** of **Device Manager**.
  e. Run **Autorun.exe** to install the 20.4.1 driver package.

11.18 How Can I Add a Static Route to a CentOS 6.5 OS?

Scenarios

After the system restarts, non-static routes are lost, affecting network availability. To prevent this issue from occurring, you must add static routes to the system.

Procedure

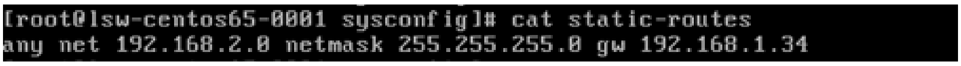
The following section uses a CentOS 6.5 OS as an example.

1. Log in to the ECS.
2. Create or modify the static route configuration file.

   If the **static-routes** configuration file is not in the **/etc/sysconfig/** directory, create this file. If such a file is available, run the following command to add a static route into this file:

   any net *192.168.2.0* **netmask** *255.255.255.0* **gw** *192.168.1.34*

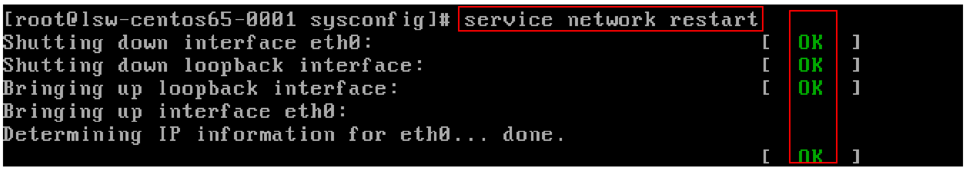
   After the configuration, save and exit the file. The following figure shows the modified file content.

```
[root@lsw-centos65-0001 sysconfig]# cat static-routes
any net 192.168.2.0 netmask 255.255.255.0 gw 192.168.1.34
```

3. Run the following command to restart the network service to make the static route take effect:

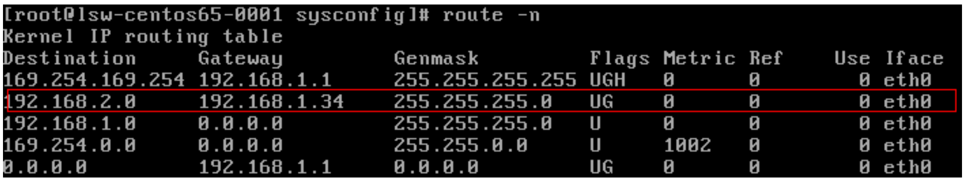
   service network restart

```
[root@lsw-centos65-0001 sysconfig]# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:
Determining IP information for eth0... done.
                                                           [  OK  ]
```

4. Run the following command to view routes:

   route -n

```
[root@lsw-centos65-0001 sysconfig]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
169.254.169.254 192.168.1.1     255.255.255.255 UGH   0      0        0 eth0
192.168.2.0     192.168.1.34    255.255.255.0   UG    0      0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
```

12 EIP

12.1 Can Multiple EIPs Be Bound to an ECS?

Scenarios

Multiple EIPs can be bound to an ECS, but this operation is not recommended.

If an ECS has multiple network interfaces attached and you want to bind multiple EIPs to this ECS, you need to configure policy-based routes for these network interfaces so that these extension network interfaces can communicate with external networks.

Operation Guide

Table 12-1 provides the operation guides on how to configure policy-based routes for Linux and Windows ECSs.

Table 12-1 Operation instructions on how to configure policy-based routes

OS Type	IP Address Version	Procedure
Linux	IPv4	Take an ECS running CentOS 8.0 (64-bit) as an example. **Configuring Policy-based Routes for a Linux ECS with Multiple Network Interfaces (IPv4/IPv6)**
	IPv6	
Windows	IPv4	Take an ECS running Windows Server 2012 (64-bit) as an example. **Configuring Policy-based Routes for a Windows ECS with Multiple Network Interfaces (IPv4/IPv6)**
	IPv6	

12.2 Can an ECS Without an EIP Bound Access the Internet?

Yes.

You can use the NAT Gateway service to allow ECSs in a VPC to access the Internet using an EIP. The SNAT function provided by the NAT Gateway service allows the ECSs in a VPC to access the Internet without requiring an EIP. Additionally, SNAT supports a large number of concurrent connections for applications that have a large number of requests and connections. For more information about NAT Gateway, see *NAT Gateway Service Overview*.

12.3 What Should I Do If an EIP Cannot Be Pinged?

Symptom

After you purchase an EIP and bind it to an ECS, the local host or other cloud servers cannot ping the EIP of the ECS.

Fault Locating

Checking EIPs

- Check whether the EIP is blocked. For details, see **How Do I Unblock an EIP?**
- Check whether the EIP is frozen. For details, see **Why Are My EIPs Frozen? How Do I Unfreeze My EIPs?**

Checking EIP Connectivity

The following fault causes are sequenced based on their occurrence probability.

If the fault persists after you have ruled out a cause, check other causes.

Figure 12-1 Method of locating the failure to ping an EIP

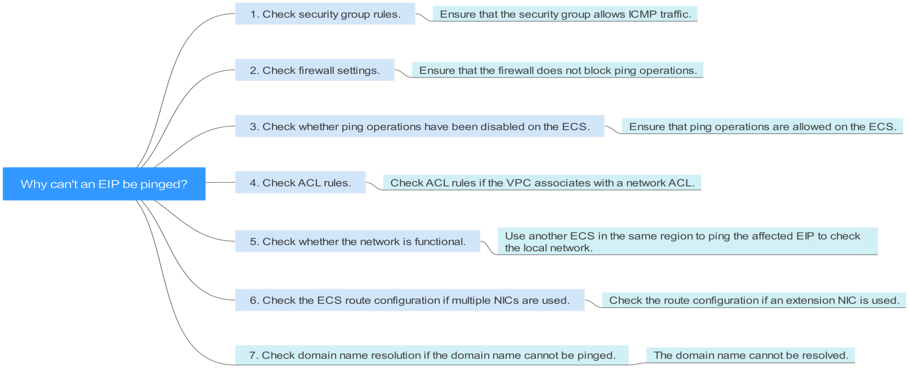

Why can't an EIP be pinged?
1. Check security group rules.
Ensure that the security group allows ICMP traffic.
2. Check firewall settings.
Ensure that the firewall does not block ping operations.
3. Check whether ping operations have been disabled on the ECS.
Ensure that ping operations are allowed on the ECS.
4. Check ACL rules.
Check ACL rules if the VPC associates with a network ACL.
5. Check whether the network is functional.
Use another ECS in the same region to ping the affected EIP to check the local network.
6. Check the ECS route configuration if multiple NICs are used.
Check the route configuration if an extension NIC is used.
7. Check domain name resolution if the domain name cannot be pinged.
The domain name cannot be resolved.

Table 12-2 Method of locating the failure to ping an EIP

Possible Causes	Solution
ICMP access rules are not added to the security group.	Add ICMP access rules to the security group. For details, see **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 ECS.	Allow ping operations on the ECS. For details, see **Checking Whether Ping Operations Have Been Disabled on the ECS**.
Network ACL is associated.	If the VPC is associated with a network ACL, check the network ACL rules. For details, see **Checking Network ACL Rules**.
A network exception occurred.	Use another ECS in the same region to check whether the local network is functional. For details, see **Checking Whether the Network Is Normal**.
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 ECS Route Configuration If Multiple NICs Are Used**.
The domain name is not ICP licensed.	If the domain name cannot be pinged or cannot be resolved, see **Checking Domain Name Resolution If the Domain Name Cannot Be Pinged** to resolve this issue.

Checking Security Group Rules

ICMP is used for the ping command. Check whether the security group accommodating the ECS allows ICMP traffic.

1. Log in to the **management console**.
2. Click 📍 in the upper left corner and select a region and project.
3. Click ≡ . Under **Compute**, click **Elastic Cloud Server**.
4. On the **Elastic Cloud Server** page, click the name of the target ECS.

   The page providing details about the ECS 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** page.
7. On the **Outbound Rules** page, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.

Table 12-3 Security group rules

Transfer Direction	Type	Protocol/Port Range	Destination
Outbound	IPv4	ICMP/Any	0.0.0.0/0 0.0.0.0/0 indicates all IP addresses.

8. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

Table 12-4 Security group rules

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

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

Checking Firewall Settings

If a firewall is enabled on the ECS, check whether the firewall blocks the ping operations.

Linux

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

   firewall-cmd --state

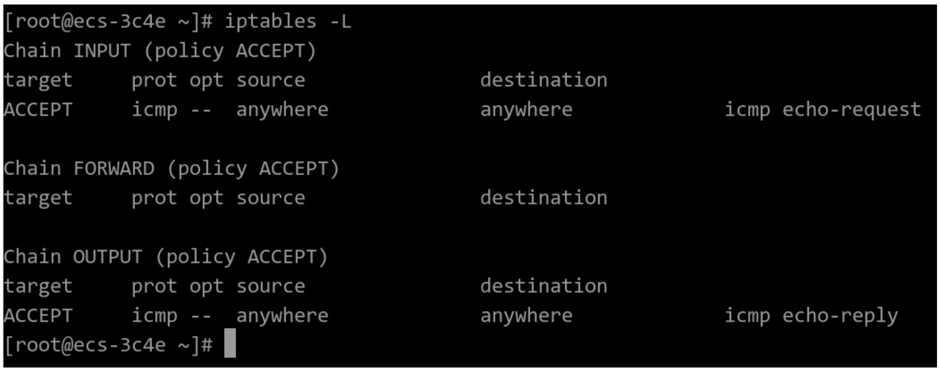
   If **running** is displayed in the command output, the firewall has been enabled.

2. Check whether there is any ICMP rule blocking the ping operations.

   iptables -L

   If the command output shown in **Figure 12-2** is displayed, there is no ICMP rule blocking the ping operations.

Figure 12-2 Checking firewall rules



```
[root@ecs-3c4e ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
[root@ecs-3c4e ~]#
```

If the ping operations are 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 ECS, 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 step **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)**

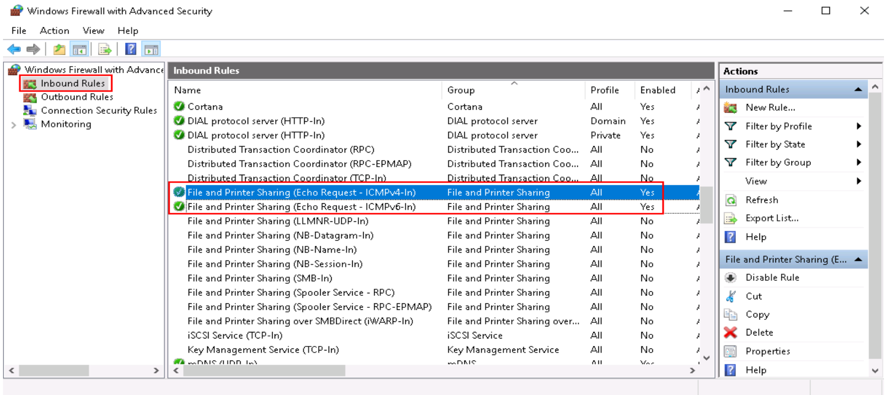
      Outbound Rules: **File and Printer Sharing (Echo Request - ICMPv4-Out)**

      If IPv6 is enabled, enable the following rules:

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

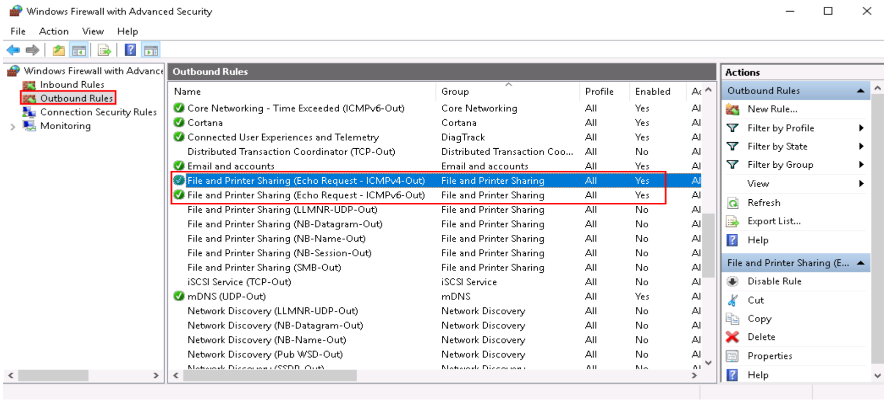
      Outbound Rules: **File and Printer Sharing (Echo Request - ICMPv6-Out)**

Figure 12-3 Inbound Rules



Name	Group	Profile	Enabled
✓ Cortana	Cortana	All	Yes
✓ DIAL protocol server (HTTP-In)	DIAL protocol server	Domain	Yes
✓ DIAL protocol server (HTTP-In)	DIAL protocol server	Private	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	All	No
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All	Yes
✓ File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All	Yes
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	No
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All	No
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	All	No
File and Printer Sharing over SMBDirect (iWARP-In)	File and Printer Sharing over...	All	No
iSCSI Service (TCP-In)	iSCSI Service	All	No
Key Management Service (TCP-In)	Key Management Service	All	No

Figure 12-4 Outbound Rules



Name	Group	Profile	Enabled	Ac
Core Networking - Time Exceeded (ICMPv6-Out)	Core Networking	All	Yes	Al
Cortana	Cortana	All	Yes	Al
Connected User Experiences and Telemetry	DiagTrack	All	Yes	Al
Distributed Transaction Coordinator (TCP-Out)	Distributed Transaction Coo...	All	No	Al
Email and accounts	Email and accounts	All	Yes	Al
File and Printer Sharing (Echo Request - ICMPv4-Out)	File and Printer Sharing	All	Yes	Al
File and Printer Sharing (Echo Request - ICMPv6-Out)	File and Printer Sharing	All	Yes	Al
File and Printer Sharing (LLMNR-UDP-Out)	File and Printer Sharing	All	No	Al
File and Printer Sharing (NB-Datagram-Out)	File and Printer Sharing	All	No	Al
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	All	No	Al
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	All	No	Al
File and Printer Sharing (SMB-Out)	File and Printer Sharing	All	No	Al
iSCSI Service (TCP-Out)	iSCSI Service	All	No	Al
mDNS (UDP-Out)	mDNS	All	Yes	Al
Network Discovery (LLMNR-UDP-Out)	Network Discovery	All	No	Al
Network Discovery (NB-Datagram-Out)	Network Discovery	All	No	Al
Network Discovery (NB-Name-Out)	Network Discovery	All	No	Al
Network Discovery (Pub WSD-Out)	Network Discovery	All	No	Al

Checking Whether Ping Operations Have Been Disabled on the ECS

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 ECS kernel parameters.

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:

     ```
     net.ipv4.icmp_echo_ignore_all=0
     ```

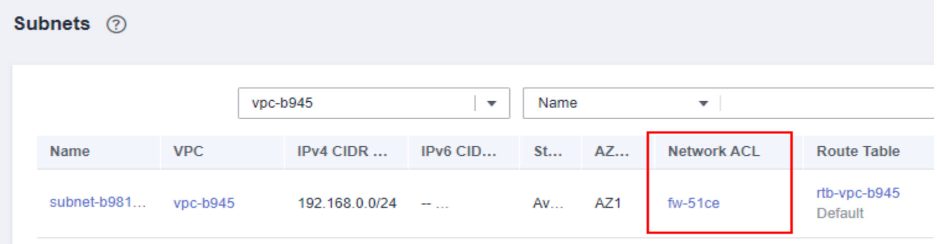
Checking Network ACL Rules

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

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

   If an ACL name is displayed, the network ACL has been associated with the ECS.

Figure 12-5 Network ACL



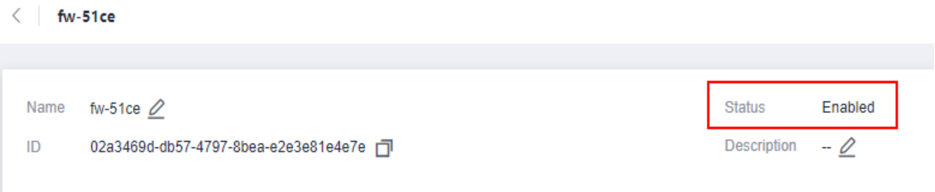
Subnets

vpc-b945 | Name

Name	VPC	IPv4 CIDR ...	IPv6 CID...	St...	AZ...	Network ACL	Route Table
subnet-b981...	vpc-b945	192.168.0.0/24	-- ...	Av...	AZ1	fw-51ce	rtb-vpc-b945 Default

2. Click the ACL name to view its status.

Figure 12-6 Enabled network ACL

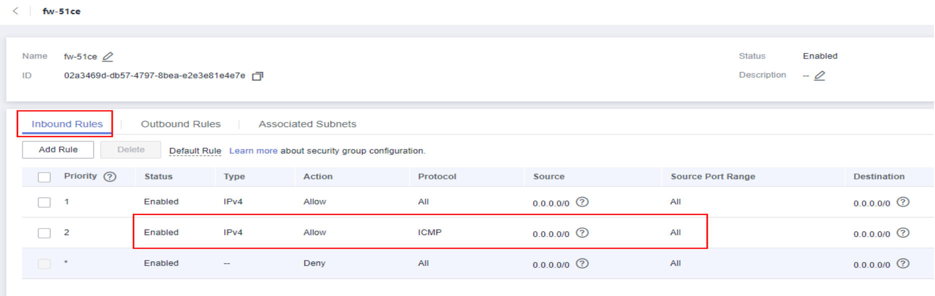


fw-51ce

Name fw-51ce
ID 02a3469d-db57-4797-8bea-e2e3e81e4e7e
Status Enabled
Description --

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

Figure 12-7 Adding an ICMP rule



fw-51ce

Name fw-51ce
ID 02a3469d-db57-4797-8bea-e2e3e81e4e7e
Status Enabled
Description --

Default Rule Learn more about security group configuration.

☐	Priority	Status	Type	Action	Protocol	Source	Source Port Range	Destination
☐	1	Enabled	IPv4	Allow	All	0.0.0.0/0	All	0.0.0.0/0
☐	2	Enabled	IPv4	Allow	ICMP	0.0.0.0/0	All	0.0.0.0/0
☐	*	Enabled	--	Deny	All	0.0.0.0/0	All	0.0.0.0/0

NOTE

The default network ACL rule denies all incoming and outgoing packets. If a network ACL is disabled, the default rule is still effective.

Checking Whether the Network Is Normal

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

   Use another ECS 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 is caused by packet loss or long delay, which may be caused by link congestion, link node faults, or heavy load on the ECS.

   For details, see **How Do I Troubleshoot a Ping Failure or Packet Loss Using a Link Test?**

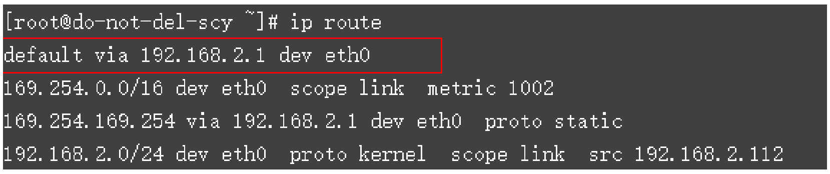
Checking the ECS Route Configuration If Multiple NICs Are Used

Generally, the default route of an OS will preferentially select the primary NIC. If an extension NIC is selected in a route and the network malfunctions, this issue is typically caused by incorrect route configuration.

- If the ECS has multiple NICs, check whether the default route is available.
  a. Log in to the ECS and run the following command to check whether the default route is available:

     ip route

     Figure 12-8 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 ECS has multiple NICs and the EIP is bound to an extension NIC, configure policy routing on the ECS for network communication with the extension NIC.

  For details, see **How Do I Configure Policy-Based Routes for an ECS with Multiple NICs?**

Checking Domain Name Resolution If the Domain Name Cannot Be Pinged

If you can ping the EIP but not the domain name, the possible cause is that an error occurred in domain name resolution.

1. Check the domain name resolution.

   If the domain name records are incorrectly configured, the domain name may fail to be resolved.

   Switch to the DNS management console to view details about the domain name resolution.

2. Check the DNS server configuration.

   If the system shows no server found after you ping a 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**.

12.4 Why Can I Remotely Access an ECS But Cannot Ping It?

Symptom

You can remotely access an ECS, but when you ping the EIP bound to the ECS, the ping operation fails.

Possible Causes

A desired inbound rule is not added for the security group, and ICMP is not enabled.

Solution

1. Log in to the **management console**.
2. Under **Compute**, click **Elastic Cloud Server**.
3. On the **Elastic Cloud Server** page, click the name of the target ECS.

   The ECS details page is displayed.
4. Click the **Security Groups** tab, expand the information of the security group, and click the security group ID.
5. On the **Inbound Rules** tab of the **Security Group** page, click **Add Rule**.
6. Add an inbound rule for the security group and enable ICMP.
   - **Protocol**: **ICMP**
   - **Source**: **IP address 0.0.0.0/0**

12.5 Why Is Outbound Access on TCP Port 25 Blocked?

Symptom

You cannot access an external address on TCP port 25. For example, running the **Telnet smtp.***.com 25** command fails.

Cause

For security reasons, TCP port 25 is disabled in the outbound direction by default.

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

NOTE

Outbound traffic over TCP port 25 is only blocked in CN North-Beijing1.

Solution

Use port 465 supported by the third-party email service provider.

12.6 How Do I Query the Egress Public IP Address of My ECS?

Scenarios

After servers are migrated to the cloud, they usually use EIPs to access the Internet.

You can log in to the management console and view the EIP bound to the ECS in the ECS list. For details, see **Viewing ECS Details (List View)**.

If you want to query the EIP bound to the ECS without logging in to the management console, do as follows.

This section uses an ECS running CentOS 7.5 as an example.

Procedure

1. **Log in to an ECS**.
2. Run any of the following commands to query the EIP of the ECS:
   - **curl icanhazip.com**
   - **curl ifconfig.me**
   - **curl ipinfo.io/ip**
   - **curl ipecho.net/plain**
   - **curl www.trackip.net/i**

12.7 Why My EIPs Are Frozen? How Do I Unfreeze My EIPs?

EIP resources are frozen in the following situations:

- **In arrears**
  - Yearly/Monthly EIPs

    If you do not renew yearly/monthly EIPs after the grace period ends, the EIPs enter a retention period and are frozen. Frozen EIPs cannot be used, modified, or released. If you still do not renew your EIPs before the retention period ends, they will be released and cannot be restored. To ensure the availability of your EIPs, renew them before they expire.
  - Pay-per-use EIPs

    If your pay-per-use EIPs are still in arrears after the grace period ends, the EIPs enter the retention period and are frozen. Frozen EIPs cannot be used, modified, or released. If you still do not top up and pay off the arrears before the retention period ends, the EIPs will be released and cannot be restored. To ensure the availability of your EIPs, top up your account and pay off the arrears before they expire.

  - Frozen EIPs will be available after you renew them or top up your account. You can renew your resources on the management console. For more details, see **Renewal Management**.

- **Attacks**

  EIPs will be frozen if their associated instances have security violations, such as attacks. Frozen EIPs are unavailable and cannot be modified or released. To unfreeze EIPs, **create a service ticket**.

  You can change an EIP for an instance by referring to **Changing an EIP**.

- **Violations**

  The server bound to the EIP is suspected of violations and the EIP is frozen by the national supervision department. If you have confirmed that you have not been involved in any violation, contact the national supervision department to file an appeal. If the appeal is successful, Huawei Cloud will receive an unsealing instruction to unfreeze your resources.

  You can change an EIP for an instance by referring to **Changing an EIP**.

13 Password and Key Pair

13.1 How Can I Change the Password for Logging In to a Linux ECS?

Solution

1. Use the existing key file to log in to the Linux ECS as user **root**.
2. Run the following command to reset the password of user **root**:

   passwd

   To reset the password of another user, replace **passwd** with **passwd** *username*.
3. Enter the new password as prompted.

   ```
   New password:
   Retype new password:
   ```

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

   ```
   passwd: all authentication tokens updates successfully
   ```

13.2 What Is the Default Password for Logging In to a Linux ECS?

The default username for logging in to an ECS running Linux (such as CentOS or Ubuntu) is **root**, and the password is the one you set during the ECS creation.

If you forgot the login password or did not set a password when creating the ECS, you can **reset the password**.

13.3 How Can I Set the Validity Period of the Image Password?

If an ECS cannot be logged in because of expired image password, you can contact the administrator for handling.

If the ECS can still be logged in, you can perform the following operations to set the password validity period.

Procedure

The following operations use EulerOS 2.2 as an example.

1. Log in to the ECS.
2. Run the following command to check the password validity period:

   vi /etc/login.defs

   The value of parameter **PASS_MAX_DAYS** is the password validity period.
3. Run the following command to change the value of parameter **PASS_MAX_DAYS**:

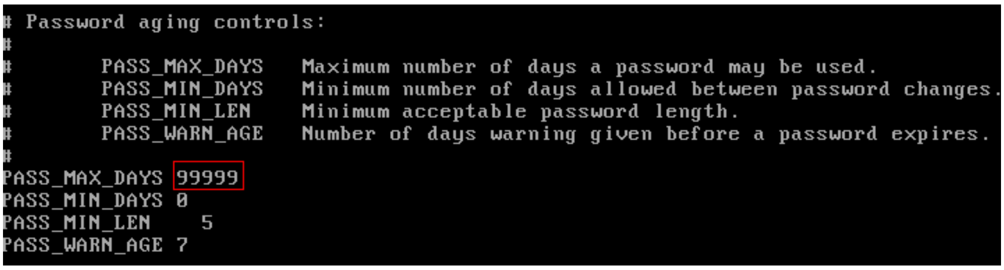
   chage -M *99999 user_name*

   99999 is the password validity period, and *user_name* is the system user, for example, user **root**.

   NOTE

   You are advised to configure the password validity period as needed and change it at a regular basis.
4. Run command **vi /etc/login.defs** to verify that the configuration has taken effect.

Figure 13-1 Configuration verification



```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_MIN_LEN    5
PASS_WARN_AGE 7
```

13.4 How Can I Reset the Password for Logging In to an ECS in the OS?

Scenarios

This section describes how to reset the password for logging in to an ECS in the OS when the password is about to expire, the password is forgotten, or you are logging in to the ECS for the first time. It is a good practice to change the initial password upon the first login.

You are advised to reset the ECS login password on the management console by referring to **Resetting the Password for Logging In to an ECS on the Management Console**.

Prerequisites

The ECS can be logged in.

Background

Table 13-1 shows the ECS password complexity requirements.

Table 13-1 Password complexity requirements

Password complexity requirements	ECS Creation	Password Reset
Length	Must contain 8 to 26 characters.	Must contain 8 to 26 characters.
Characters	Must contain at least three of the supported four character types.	Must contain at least three of the supported four character types.
Security	• Cannot contain the username or the username spelled backwards. • Cannot contain more than two consecutive characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)	• Cannot contain the username or the username spelled backwards. • Cannot contain more than two consecutive characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)
Other	None	Cannot start with a slash (/) for Windows ECSs.
Supported Characters	Uppercase letters	Uppercase letters
	Lowercase letters	Lowercase letters
	Digits	Digits
	• Special characters for Linux ECSs: !@$%^-_=+[{}]:,./?~#* • Special characters for Windows ECSs: !@$%^-_=+[{()}]:,./?~#*	• Online password reset: @%-_=+[]:./^,{}? (only applied to Linux) $@%-_=+[]:./,? (only applied to Windows) • Offline password reset: Special characters for Linux ECSs: !@%-_=+[]:./? Special characters for Windows ECSs: !@%-_=+[]:./?

Windows

1. Log in to the ECS.

   For details, see **Logging In to a Windows ECS**.
2. Press **Win+R** to start the **Run** dialog box.
3. Enter **cmd** to open the command-line interface (CLI) window.
4. Enter a new password that meets the requirements listed in **Table 13-1**.

   net user Administrator *New password*

Linux

1. Use the existing key file to log in to the ECS as user **root** through SSH.

   For details, see **Login Using an SSH Key**.
2. Run the following command to reset the password of user **root**:

   passwd

   To reset the password of another user, replace **passwd** with **passwd username**.
3. Enter a new password that meets the requirements listed in **Table 13-1** as prompted.

   ```
   New password:
   Retype new password:
   ```

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

   ```
   passwd: all authentication tokens updates successfully
   ```

13.5 Resetting the Password of a Windows ECS by Attaching a System Disk to a Temporary ECS

Scenarios

If no password was set when you create an ECS, or if the password has been lost or expired, you can reset it.

Generally, you can reset the password on the console. For details, see **Resetting the Password for Logging In to an ECS on the ECS Console**.

If the password cannot be reset on the console or the reset password does not take effect, the one-click password reset plug-in may be missing, the COC may not be enabled and authorized, or UniAgent may not be installed. In this case, you can reset the password by referring to this section.

This section only applies to Windows ECSs. For Linux ECSs, see **Resetting the Password of a Linux ECS by Attaching a System Disk to a Temporary ECS**.

Constraints

- The method described in this section only can be used to change the password of a local Windows account; it cannot be used to change a domain account password.
- The system disk needs to be detached. To prevent data loss of the system disk, back up the system disk or create a snapshot for the system disk first.

Prerequisites

- A backup or snapshot has been created for the system disk. For details, see **Backing Up an ECS** or **Creating an EVS Snapshot**.
- A temporary Linux ECS running Ubuntu 14.04 or later is available. It is located in the same AZ and has the same CPU architecture as the target ECS.

  NOTE

  - Currently, this operation can be performed only for Ubuntu 16.04 and Ubuntu 18.04 public images.
  - You can select an existing ECS or purchase a temporary ECS.

    After the password of the purchased ECS is reset, you are advised to delete the ECS to avoid additional billing.
- You have bound an EIP to the temporary ECS and configured the apt-get source.
- You have used either of the following methods to install **ntfs-3g** and **chntpw** software packages on the temporary ECS:

  Method 1:

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

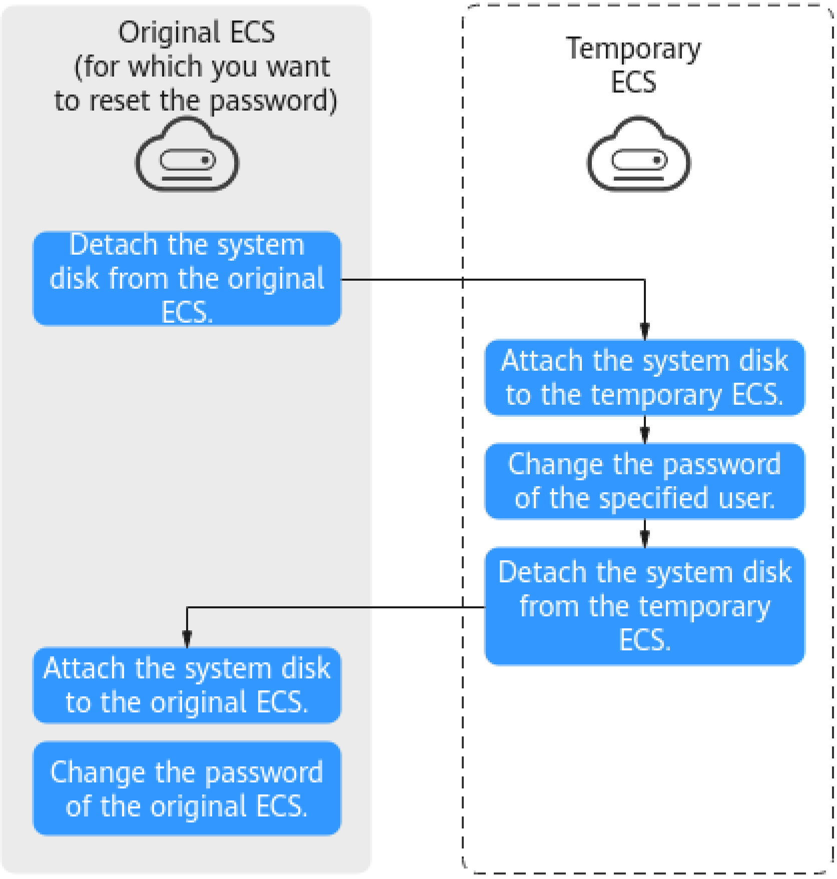
  ```
  sudo apt-get install ntfs-3g chntpw
  ```

  Method 2:

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

Process Flow

Figure 13-2 Process flow of resetting a password


Original ECS
(for which you want to reset the password)
Temporary ECS
Detach the system disk from the original ECS.
Attach the system disk to the temporary ECS.
Change the password of the specified user.
Detach the system disk from the temporary ECS.
Attach the system disk to the original ECS.
Change the password of the original ECS.

Procedure

1. Stop the original ECS and detach the system disk.
   a. Log in to the **management console**.
   b. Click in the upper left corner and select a region and project.
   c. Click . Under **Compute**, click **Elastic Cloud Server**.
   d. Stop the original Windows ECS, switch to the ECS details page, and click the **Disks** tab.

      NOTE

      Do not forcibly stop the Windows ECS. Otherwise, password reset may fail.
   e. Locate the row containing the system disk to be detached and click **Detach** to detach the system disk from the ECS.
2. Attach the system disk to the temporary ECS.
   a. On the details page of the temporary ECS, click the **Disks** tab.
   b. Click **Attach Disk**. In the displayed dialog box, select the system disk detached in step **1.e** and attach it to the temporary ECS.

c. Remotely log in to the temporary ECS.

d. Run the following command to view the directory of the system disk attached to the temporary ECS:

   fdisk -l

e. Run the following command to mount the file system of the detached system disk to the temporary ECS:

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

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

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

   If the following error information is returned in the command output, 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.d*

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

   ntfsfix /dev/xvde2

3. Change the password of the specified user 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 the specified user:

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

   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 ECS, detach the system disk, and attach the system disk to the original Windows ECS.

   a. Stop the temporary ECS, go to the ECS details page, and click the **Disks** tab.

   b. Click **Detach** to detach the data disk temporarily attached in step 2.b.

   c. On the details page of the original Windows ECS, click the **Disks** tab.

   d. Click **Attach Disk**. In the displayed dialog box, select the data disk detached in step **4.b** and attach it to the original ECS as the system disk.

5. Start the original Windows ECS and set a new login password.
   a. Click **Start** to start the original Windows ECS. 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 set a new password. The new password must meet the password complexity requirements described in **Application Scenarios for Using Passwords**.

      net user Administrator *<new-password>*

13.6 Resetting the Password of a Linux ECS by Attaching a System Disk to a Temporary ECS

Scenarios

If no password was set when you create an ECS, or if the password has been lost or expired, you can reset it.

Generally, you can reset the password on the console. For details, see **Resetting the Password for Logging In to an ECS on the ECS Console**.

If the password cannot be reset on the console or the reset password does not take effect, the one-click password reset plug-in may be missing, the COC may not be enabled and authorized, or UniAgent may not be installed. In this case, you can reset the password by referring to this section.

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

This section only applies to Linux ECSs. For Windows ECSs, see **Resetting the Password of a Windows ECS by Attaching a System Disk to a Temporary ECS**.

Constraints

- The system disk needs to be detached. To prevent data loss of the system disk, back up the system disk or create a snapshot for the system disk first.
- The operation depends on the **changepasswd.sh** script. Only ECSs created using public images are supported.

  For ECSs created using private images or other non-public images, see **Resetting the Password in the ECS OS**.

Prerequisites

- A backup or snapshot has been created for the system disk. For details, see **Backing Up an ECS** or **Creating an EVS Snapshot**.
- A temporary Linux ECS is available. It is located in the same AZ and has the same CPU architecture as the target ECS.

NOTE

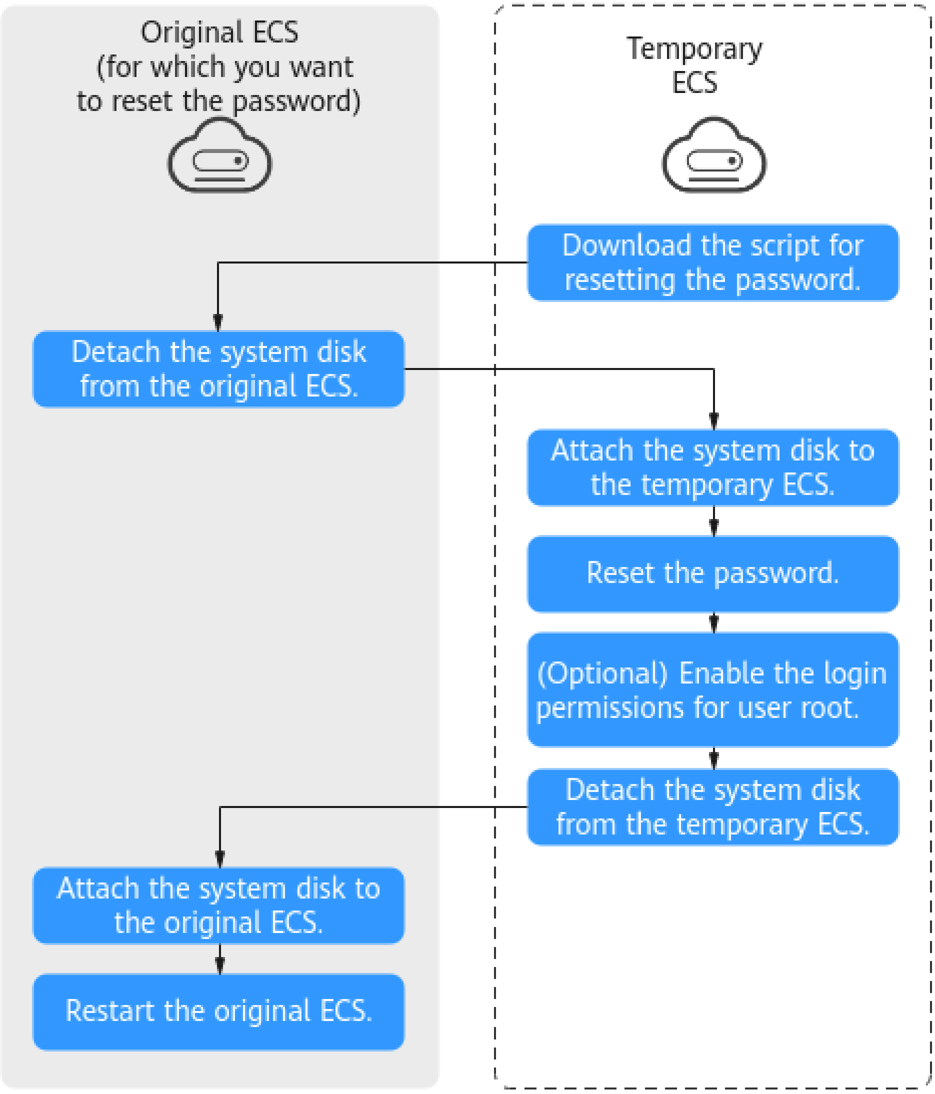
You can select an existing ECS or purchase a temporary ECS.

After the password of the purchased ECS is reset, you are advised to delete the ECS to avoid additional billing.

- You have bound an EIP to the temporary ECS.

Process Flow

Figure 13-3 Process flow of resetting a password


Original ECS (for which you want to reset the password)
Temporary ECS
Download the script for resetting the password.
Detach the system disk from the original ECS.
Attach the system disk to the temporary ECS.
Reset the password.
(Optional) Enable the login permissions for user root.
Detach the system disk from the temporary ECS.
Attach the system disk to the original ECS.
Restart the original ECS.

Procedure

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

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

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

2. Stop the original Linux ECS, detach the system disk from it, and attach the system disk to the temporary ECS.
   a. Log in to the **management console**.
   b. Click 📍 in the upper left corner and select a region and project.
   c. Click ☰ . Under **Compute**, click **Elastic Cloud Server**.
   d. Stop the original ECS, go to the ECS details page, and click the **Disks** tab.

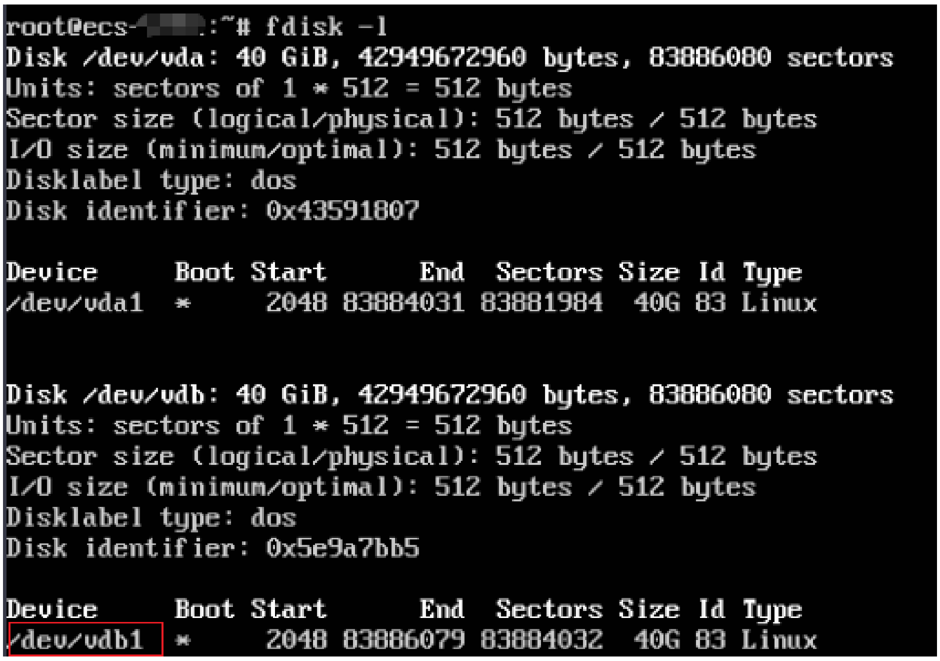
   NOTE

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

   e. Locate the row containing the system disk to be detached and click **Detach** to detach the system disk from the ECS.
3. Attach the system disk to the temporary ECS.
   a. On the details page of the temporary ECS, click the **Disks** tab.
   b. Click **Attach Disk**. In the displayed dialog box, select the system disk detached in step 2.e and attach it to the temporary ECS.
4. Log in to the temporary ECS remotely and reset the password.
   a. Locate the row containing the temporary ECS 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 ECS now attached to the temporary ECS:

   fdisk -l

Figure 13-4 Viewing the directory of the system disk



```
root@ecs-[redacted]:~# fdisk -l
Disk /dev/vda: 40 GiB, 42949672960 bytes, 83886080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x43591807

Device     Boot Start      End  Sectors Size Id Type
/dev/vda1  *     2048 83884031 83881984  40G 83 Linux


Disk /dev/vdb: 40 GiB, 42949672960 bytes, 83886080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x5e9a7bb5

Device     Boot Start      End  Sectors Size Id Type
/dev/vdb1  *     2048 83886079 83884032  40G 83 Linux
```

   c. Run the following commands in the directory where the **changepasswd.sh** 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 ECS. The LVM2 tool is recommended, which can be installed by running the **yum install lvm2** command.

   > **NOTE**
   >
   > If the original ECS and the temporary ECS 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 **4.b** as prompted.

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

```
set password success.
```

5. (Optional) Enable remote root login for non-root users.

   vi /etc/ssh/sshd_config

   Modify the following settings:

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

     Alternatively, uncomment **PasswordAuthentication yes**.

   - Change **PermitRootLogin no** to **PermitRootLogin yes**.

     Alternatively, uncomment **PermitRootLogin yes**.

   - Change the value of **AllowUsers** to **root**.

     Search for **AllowUsers** in the file. If **AllowUsers** is missing, add **AllowUsers root** at the end of the file.

6. Stop the temporary ECS, detach the system disk, attach the system disk to the original Linux ECS, and restart the original Linux ECS.

   a. Stop the temporary ECS, go to the ECS details page, and click the **Disks** tab.

   b. Click **Detach** to detach the data disk temporarily attached in step **3**.

   c. On the details page of the original Linux ECS, click the **Disks** tab.

   d. Click **Attach Disk**. In the displayed dialog box, select the data disk detached in **6.b**.

7. Restart the original Linux ECS.

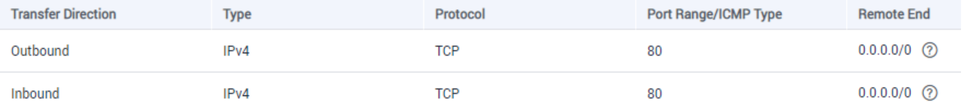
13.7 What Should I Do If the System Displays a Message Indicating that the Password Is Incorrect When I Remotely Log In to My ECS?

Solution

Check the network configuration of the ECS and determine whether the fault is caused by a **Cloud-Init** failure.

- Verify that port 80 is bypassed in both inbound and outbound directions in the security group to which the target ECS belongs.

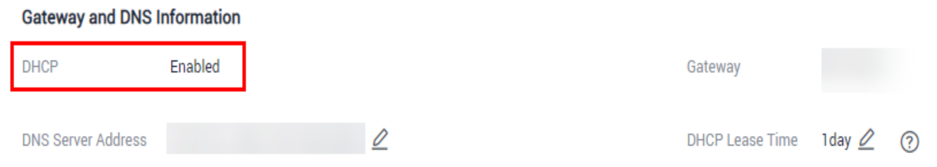
Figure 13-5 Port 80



Transfer Direction	Type	Protocol	Port Range/ICMP Type	Remote End
Outbound	IPv4	TCP	80	0.0.0.0/0
Inbound	IPv4	TCP	80	0.0.0.0/0

- Verify that DHCP is enabled in the subnet to which the target ECS belongs.

Figure 13-6 Checking DHCP status



Gateway and DNS Information

DHCP Enabled

Gateway

DNS Server Address

DHCP Lease Time 1day

NOTE

After verifying the preceding configurations, restart the ECS, wait for 3 to 5 minutes, and remotely log in to the ECS using a password or key.

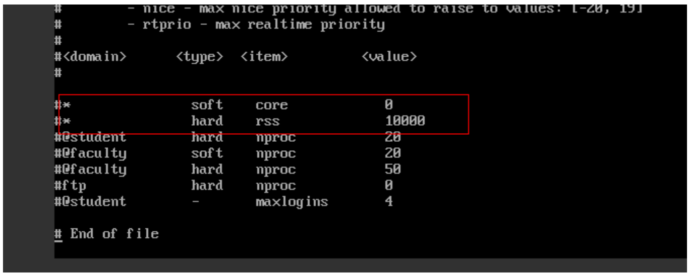
13.8 What Should I Do If I Cannot Log In to My ECS Using the Initial Password After I Use It for a Period of Time?

Solution

Check whether the remote login page can be displayed.

- If the login page cannot be displayed, an error may have occurred in the GuestOS process on the ECS. In such a case, contact customer service for troubleshooting.
- If the login page can be displayed, log in to the OS in single-user mode for troubleshooting. The procedure is as follows:
  - Check whether the password can be changed in single-user mode.

    If the password can be changed, change it and contact customer service to check whether the password has been maliciously changed due to an attack.
  - If the password cannot be changed, verify that the values of **hard** and **soft** in **/etc/security/limits.conf** are not greater than 65535.

    ```
    #        - nice - max nice priority allowed to raise to values: [-20, 19]
    #        - rtprio - max realtime priority
    #
    #<domain>      <type>  <item>         <value>
    #

    #*               soft    core            0
    #*               hard    rss             10000
    #@student        hard    nproc           20
    #@faculty        soft    nproc           20
    #@faculty        hard    nproc           50
    #ftp             hard    nproc           0
    #@student        -       maxlogins       4

    # End of file
    ```

    Change the password in single-user mode and try to log in to the ECS again.

13.9 What Should I Do If I Failed to Log In to the ECS Using the New Password That Was Reset Offline?

Scenarios

You cannot use the new password that you set offline to log in to the ECS.

NOTE

Ensure that the one-click password reset plug-in is not blocked by security software. Otherwise, the offline password reset function is unavailable.

After the password is reset offline, you must restart the ECS for the new password to take effect.

Windows

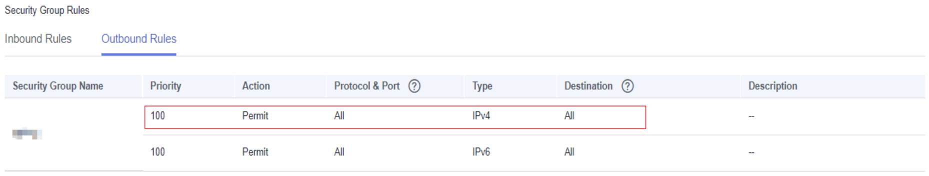
Perform the following operations to locate the fault:

Step 1 Check whether port 80 in the outbound direction of the security group is permitted.

1. Log in to the **management console**.
2. Select the target ECS to switch to the page that provides details about the ECS.
3. On the **Security Groups** tab, check whether the outbound rule allows access from port 80.

   In the default security group rule, all ports are allowed in the outbound direction.

   Figure 13-7 All ports allowed in the outbound direction

Security Group Name	Priority	Action	Protocol & Port ⓘ	Type	Destination ⓘ	Description
[redacted]	100	Permit	All	IPv4	All	--
	100	Permit	All	IPv6	All	--

Step 2 Check whether DHCP is enabled in the VPC of the ECS.

1. On the ECS details page, click the VPC name to navigate to the VPC console.
2. In the VPC list, click the VPC name.
3. In the **Networking Components** area, click the number in the **Subnets** row to go to the **Subnets** page.
4. In the subnet list, click the subnet name to view its details.
5. In the **Gateway and DNS Information** area, check whether DHCP is enabled.

Step 3 If both the security group and DHCP are properly configured but offline password reset fails to take effect, use the original password to log in to the ECS.

- If the original password is invalid, reset the password. For details, see **Resetting the Password of a Windows ECS by Attaching a System Disk to a Temporary ECS**.

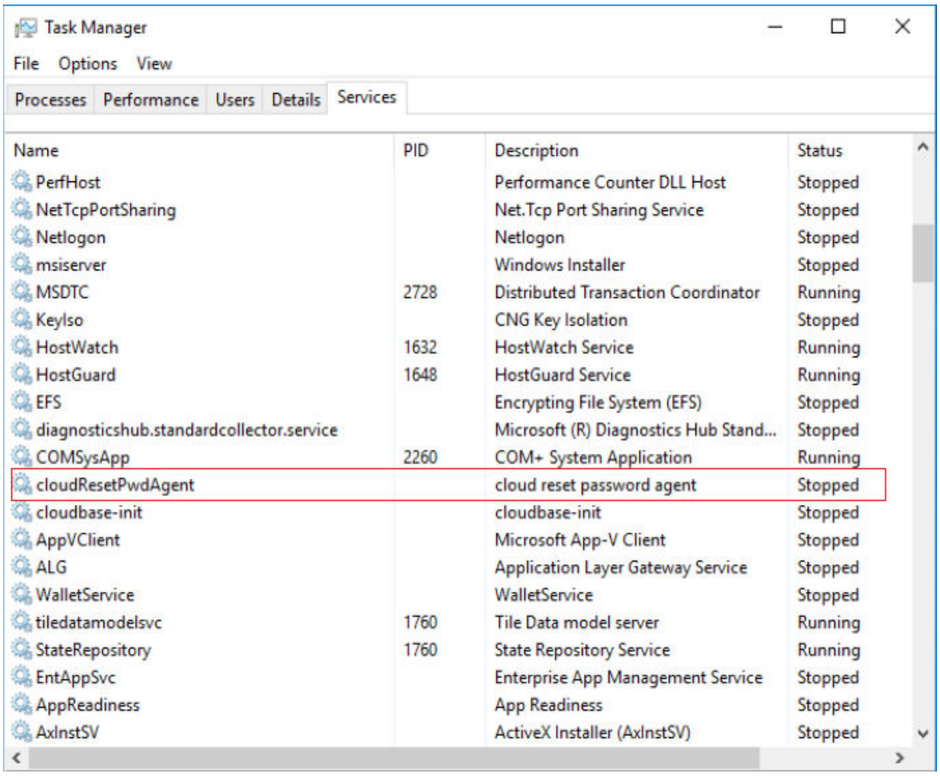
- If the original password is valid, use it to log in to the ECS and reset the password. For details, see **Resetting the Password for Logging In to an ECS in the OS**.

Step 4 Check whether the password reset plug-in CloudResetPwdAgent has been installed on the ECS. To do so, perform the following operations:

Start the **Task Manager** and check whether **cloudResetPwdAgent** is displayed on the **Services** tab. As shown in the **Figure 13-8**, the password reset plug-in has been installed on the ECS. If no, the one-click password reset plug-in has not been installed on the ECS.

For details, see **Installing the One-Click Password Reset Plug-in on an ECS**.

Figure 13-8 Successful plug-in installation



Name	PID	Description	Status
PerfHost		Performance Counter DLL Host	Stopped
NetTcpPortSharing		Net.Tcp Port Sharing Service	Stopped
Netlogon		Netlogon	Stopped
msiserver		Windows Installer	Stopped
MSDTC	2728	Distributed Transaction Coordinator	Running
KeyIso		CNG Key Isolation	Stopped
HostWatch	1632	HostWatch Service	Running
HostGuard	1648	HostGuard Service	Running
EFS		Encrypting File System (EFS)	Stopped
diagnosticshub.standardcollector.service		Microsoft (R) Diagnostics Hub Stand...	Stopped
COMSysApp	2260	COM+ System Application	Running
cloudResetPwdAgent		cloud reset password agent	Stopped
cloudbase-init		cloudbase-init	Stopped
AppVClient		Microsoft App-V Client	Stopped
ALG		Application Layer Gateway Service	Stopped
WalletService		WalletService	Stopped
tiledatamodelsvc	1760	Tile Data model server	Running
StateRepository	1760	State Repository Service	Running
EntAppSvc		Enterprise App Management Service	Stopped
AppReadiness		App Readiness	Stopped
AxInstSV		ActiveX Installer (AxInstSV)	Stopped

----End

Linux

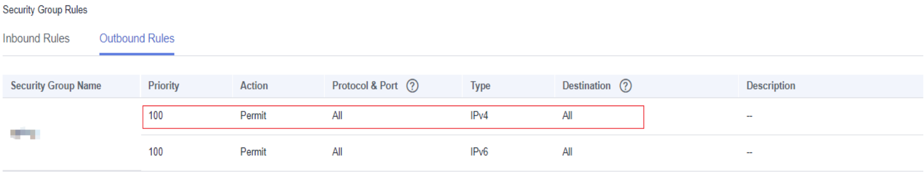
Perform the following operations to locate the fault:

Step 1 Check whether port 80 in the outbound direction of the security group is permitted.

1. Log in to the **management console**.
2. Select the target ECS to switch to the page that provides details about the ECS.
3. On the **Security Groups** tab, check whether the outbound rule allows access from port 80.

In the default security group rule, all ports are allowed in the outbound direction.

Figure 13-9 All ports allowed in the outbound direction



Security Group Rules

Security Group Name	Priority	Action	Protocol & Port	Type	Destination	Description
[redacted]	100	Permit	All	IPv4	All	--
	100	Permit	All	IPv6	All	--

Step 2 Check whether DHCP is enabled in the VPC of the ECS.

1. On the ECS details page, click the VPC name to navigate to the VPC console.
2. In the VPC list, click the VPC name.
3. In the **Networking Components** area, click the number in the **Subnets** row to go to the **Subnets** page.
4. In the subnet list, click the subnet name to view its details.
5. In the **Gateway and DNS Information** area, check whether DHCP is enabled.

Step 3 If both the security group and DHCP are properly configured but offline password reset fails to take effect, use the original password to log in to the ECS.

- If the original password is invalid, enter single-user mode and reset the password.

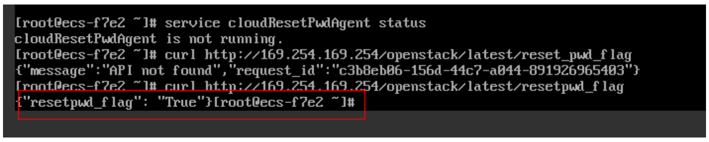
  For details, see **Resetting the Password for Logging In to an ECS in the OS**.

- If the original password can be used, perform the following operations for further check:

  a. Use the original password to log in to the ECS.

  b. Run the **curl http://169.254.169.254/openstack/latest/resetpwd_flag** command to check whether the one-click password reset function is available.

     - If the returned value is **true**, the password can be reset offline.
     - If any other value is returned, the password cannot be reset offline.



```
[root@ecs-f7e2 ~]# service cloudResetPwdAgent status
cloudResetPwdAgent is not running.
[root@ecs-f7e2 ~]# curl http://169.254.169.254/openstack/latest/reset_pwd_flag
{"message":"API not found","request_id":"c3b8eb06-156d-44c7-a044-891926965403"}
[root@ecs-f7e2 ~]# curl http://169.254.169.254/openstack/latest/resetpwd_flag
{"resetpwd_flag": "True"}[root@ecs-f7e2 ~]#
```

Step 4 Check whether **CloudResetPwdAgent** has been installed.

1. Check whether the **CloudrResetPwdAgent** directory is available in the root directory on the ECS.
   - If the directory is available, go to step **Step 4.2**.
   - If the directory is not available, the one-click password reset plug-in has not been installed on the ECS.

     For details, see **Installing the One-Click Password Reset Plug-in on an ECS**.
2. Run the following command to check the CloudResetPwdAgent status:

   service cloudResetPwdAgent status

If the command output is "unrecognized service", the one-click password reset plug-in has not been installed on the ECS.

For details, see **Installing the One-Click Password Reset Plug-in on an ECS**.

----End

13.10 Why Am I Seeing the Message Indicating That the Port Is Used by a One-Click Password Reset Plug-in?

Symptom

When you attempt to run an application on an ECS, the system displays a message indicating that the required port is used by a one-click password reset plug-in.

Possible Causes

If an ECS works in AUTO mode, when its one-click password reset plug-in starts, the plug-in randomly uses a port, which may be a service port.

NOTE

The one-click password reset plug-in has been upgraded to work in PIPE mode by default.

- Newly created ECSs run in PIPE mode by default, and their one-click password reset plug-ins will not use service ports.
- Existing ECSs still work in AUTO mode, in which the plug-ins randomly select idle ports with the smallest port numbers ranging from 31000 to 32999.

Method 1 (Recommended): Modifying the wrapper Files of the One-Click Password Reset Plug-in for the PIPE Mode

In the wrapper files, change **AUTO (SOCKET)** to **PIPE**. After the change, the plug-in will not use service ports.

1. Open CloudResetPwdAgent configuration files.
   - Linux

     /CloudrResetPwdAgent/conf/wrapper.conf and **/CloudResetPwdUpdateAgent/conf/wrapper.conf**
   - Windows

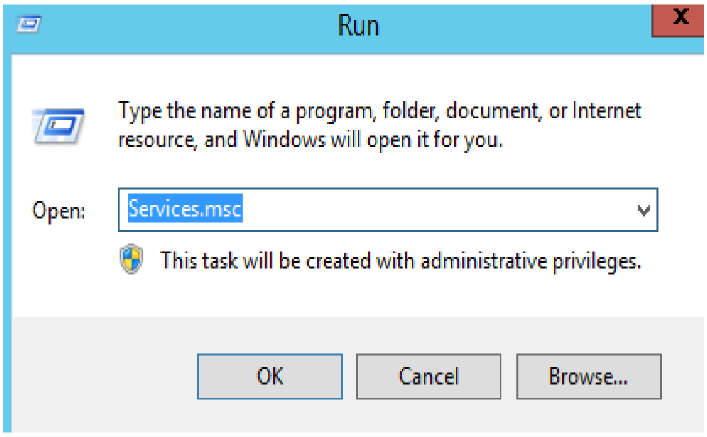
     C:\CloudrResetPwdAgent\conf\wrapper.conf and **C:\CloudResetPwdUpdateAgent\conf\wrapper.conf**
2. Add the following data to the end of the files:

   wrapper.backend.type=PIPE
3. Restart CloudResetPwdUpdateAgent.
   - Linux

     /CloudResetPwdUpdateAgent/bin/cloudResetPwdUpdateAgent.script restart

- Windows
  1. Press **Win+R** to start the **Run** text box.
  2. Enter **Services.msc** and click **OK**.

     Figure 13-10 Run

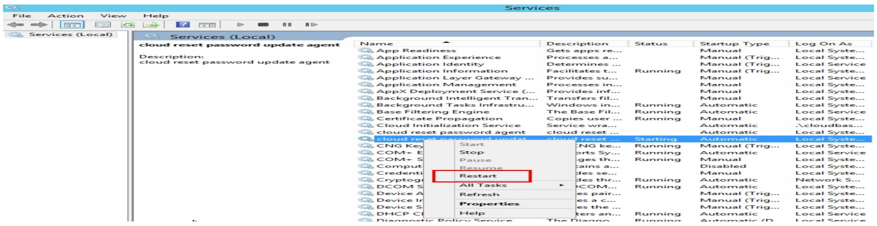
     Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

     Open: Services.msc

     This task will be created with administrative privileges.

  3. Right-click **cloud reset password update agent** and choose **Restart** from the shortcut menu.

     Figure 13-11 Services (Local)

     Services (Local)

     cloud reset password update agent

     Description:
     cloud reset password update agent

Name	Description	Status	Startup Type	Log On As
App Readiness	Gets apps re...		Manual	Local Syste...
Application Experience	Processes a...		Manual (Trig...	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...		Manual	Local Syste...
Background Intelligent Tran...	Transfers fil...		Manual	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Certificate Propagation	Copies user ...	Running	Manual	Local Syste...
Cloud Initialization Service	Service wra...		Automatic	.\cloudbas...
cloud reset password agent	cloud reset ...		Automatic	Local Syste...
cloud reset password updat	cloud reset ...	Starting	Automatic	Local Syste...
CNG Key	NG ke...	Running	Manual (Trig...	Local Syste...
COM+ E	rts Sy...	Running	Automatic	Local Service
COM+ S	ges th...	Running	Manual	Local Syste...
Comput	ains a...		Disabled	Local Syste...
Credenti	des se...		Manual	Local Syste...
Cryptogr	des thr...	Running	Automatic	Network S...
DCOM S	COM...	Running	Automatic	Local Syste...
Device A	es pair...		Manual (Trig...	Local Syste...
Device Ir	es a c...		Manual (Trig...	Local Syste...
Device S	es the ...		Manual (Trig...	Local Syste...
DHCP Cl	ters an...	Running	Automatic	Local Service

Method 2: Modifying the Configuration to Change the Port Range

Modify the CloudResetPwdAgent configuration to change the default port range (31000–32999) for the password reset plug-in so that the service port is out of the port range.

For example, to change the port range for the password reset plug-in to 40000–42000, perform the following operations:

1. Open CloudResetPwdAgent configuration files.
   - Linux

     /CloudrResetPwdAgent/conf/wrapper.conf and **/CloudResetPwdUpdateAgent/conf/wrapper.conf**
   - Windows

     C:\CloudrResetPwdAgent\conf\wrapper.conf and **C:\CloudResetPwdUpdateAgent\conf\wrapper.conf**
2. Add the following data to the configuration files:

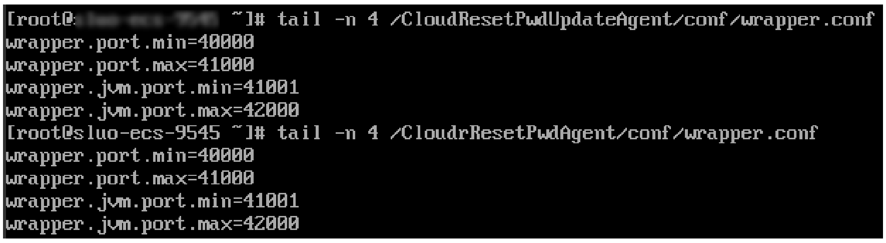
   wrapper.port.min=40000

   wrapper.port.max=41000

   wrapper.jvm.port.min=41001

wrapper.jvm.port.max=42000

Figure 13-12 Modifying the configuration files

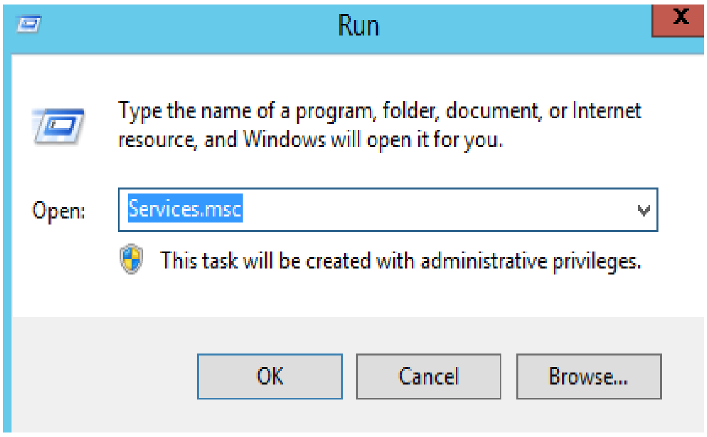


```
[root@[redacted] ~]# tail -n 4 /CloudResetPwdUpdateAgent/conf/wrapper.conf
wrapper.port.min=40000
wrapper.port.max=41000
wrapper.jvm.port.min=41001
wrapper.jvm.port.max=42000
[root@sluo-ecs-9545 ~]# tail -n 4 /CloudrResetPwdAgent/conf/wrapper.conf
wrapper.port.min=40000
wrapper.port.max=41000
wrapper.jvm.port.min=41001
wrapper.jvm.port.max=42000
```

3. Restart CloudResetPwdUpdateAgent.
   - Linux

     /CloudResetPwdUpdateAgent/bin/cloudResetPwdUpdateAgent.script restart
   - Windows
     i. Press **Win+R** to start the **Run** text box.
     ii. Enter **Services.msc** and click **OK**.

     Figure 13-13 Run



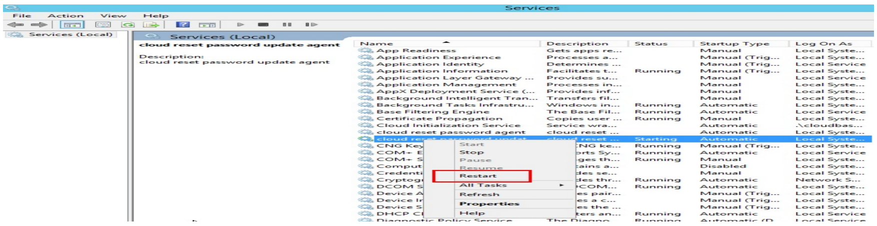
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: Services.msc

This task will be created with administrative privileges.

     iii. Right-click **cloud reset password update agent** and choose **Restart** from the shortcut menu.

     Figure 13-14 Services (Local)



cloud reset password update agent

Description:
cloud reset password update agent

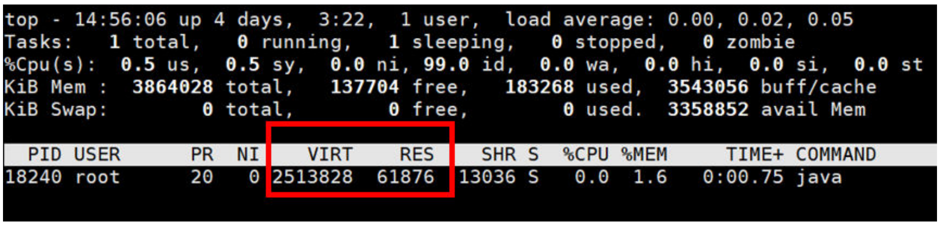
Name	Description	Status	Startup Type	Log On As
App Readiness	Gets apps re...		Manual	Local Syste...
Application Experience	Processes a...		Manual (Trig...	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...		Manual	Local Syste...
Background Intelligent Tran...	Transfers fil...		Manual	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Certificate Propagation	Copies user ...	Running	Manual	Local Syste...
Cloud Initialization Service	Service wra...		Automatic	.\cloudbas...
cloud reset password agent	cloud reset ...		Automatic	Local Syste...
cloud reset password updat	cloud reset ...	Starting	Automatic	Local Syste...
CNG Key	NG ke...	Running	Manual (Trig...	Local Syste...
COM+ E	orts Sy...	Running	Automatic	Local Service
COM+ S	ges th...	Running	Manual	Local Syste...
Comput	ains a...		Disabled	Local Syste...
Credenti	des se...		Manual	Local Syste...
Cryptogr	des thr...	Running	Automatic	Network S...
DCOM S	COM...	Running	Automatic	Local Syste...
Device A	es pair...		Manual (Trig...	Local Syste...
Device Ir	es a c...		Manual (Trig...	Local Syste...
Device S	es the ...		Manual (Trig...	Local Syste...
DHCP Cl	ters an...	Running	Automatic	Local Service
Diagnostic Policy Service	The Diagno...	Running	Automatic (D...	Local Service

13.11 Why Does the One-Click Password Reset Plug-in Use Too Much VIRT and SHR?

Symptom

The one-click password reset plug-in uses too much VIRT and SHR.

Figure 13-15 Viewing the virtual memory usage



```
top - 14:56:06 up 4 days,  3:22,  1 user,  load average: 0.00, 0.02, 0.05
Tasks:   1 total,   0 running,   1 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.5 us,  0.5 sy,  0.0 ni, 99.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3864028 total,   137704 free,   183268 used,  3543056 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  3358852 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
18240 root      20   0 2513828  61876  13036 S   0.0  1.6   0:00.75 java
```

Root Causes

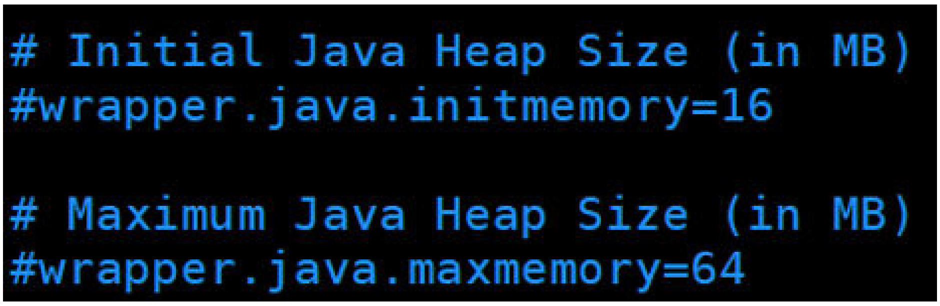
Memory used by applications is from the glibc memory pool. In versions earlier than glibc 2.10, there is only one memory pool named main arena. In glibc 2.10 and later versions, there is a memory pool named thread arena. Therefore, applications can use memory from two memory pools, which results in high usage of VIRT and SHR. You can limit the memory that can be used by the one-click password reset plug-in.

Procedure

1. Modify the parameters of the one-click password reset plug-in.
   a. Run the following command to view the configuration file.

      vim /CloudResetPwdUpdateAgent/conf/wrapper.conf

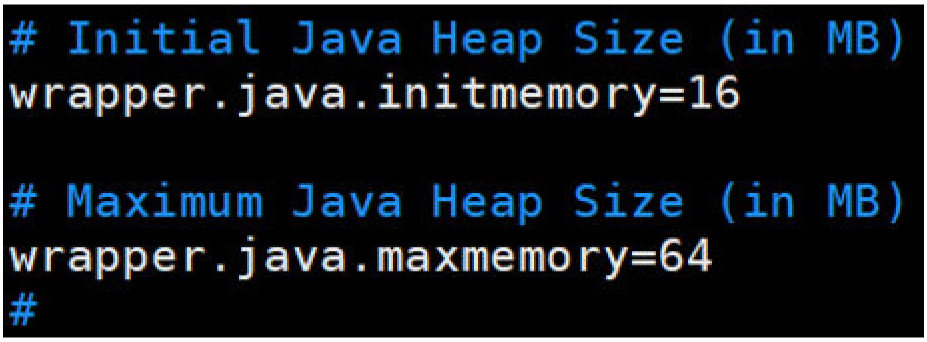
      Figure 13-16 wrapper.conf before modification

      ```
      # Initial Java Heap Size (in MB)
      #wrapper.java.initmemory=16

      # Maximum Java Heap Size (in MB)
      #wrapper.java.maxmemory=64
      ```

   b. Delete the comment tag (#) at the beginning of **wrapper.java.initmemory=16** and **wrapper.java.maxmemory=64**.

Figure 13-17 wrapper.conf after modification



```
# Initial Java Heap Size (in MB)
wrapper.java.initmemory=16

# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=64
#
```

2. Run the following commands to restart the one-click password reset plug-in.

   cd /CloudResetPwdUpdateAgent/bin/

   ./cloudResetPwdUpdateAgent.script restart

13.12 Disabling SELinux

NOTE

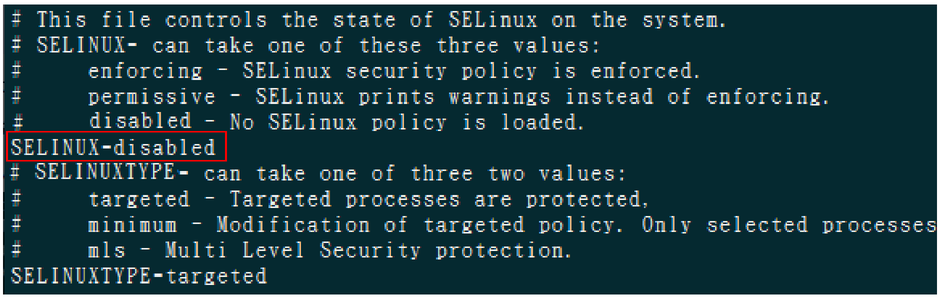
SUSE does not have the SELinux configuration files. You can skip this section.

Procedure

1. Use the vi editor to open **/etc/selinux/config**.

   vi /etc/selinux/config

2. Press **i** to enter insert mode and set the value of **SELINUX** to **disabled**.



```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

3. Press **Esc** and enter **:wq** to save and exit the file.
4. Run the following command to restart the cloud server to apply the change:

   reboot

13.13 What Should I Do If the One-Click Password Reset Plug-ins Installed on a Linux ECS Fail to Be Started?

Scenarios

The one-click password reset plug-ins installed on a Linux ECS fail to be started.

Symptom

When a user ran **sudo sh setup.sh** to install one-click password reset plug-ins, the following error message is displayed:

```
begin install CloudResetPwdAgent
===============cp LinuxCloudResetPwdAgent======================
===============vi /etc/profile======================
===============begin install CloudrResetPwdAgent===================
Detected RHEL or Fedora:
Installing the cloudResetPwdAgent daemon using systemd...
creating default service file...
Reading file /etc/systemd/system/cloudResetPwdAgent.service
Job for cloudResetPwdAgent.service failed because the control process exited with error code.
See "systemctl status cloudResetPwdAgent.service" and "journalctl -xe" for details.
Failed to start service cloudResetPwdAgent
/CloudResetPwdAgent/CloudResetPwdAgent.Linux
cloudResetPwdAgent install successfully.
```

In the **/var/log/message** file, the following error information is displayed:

```
systemd[1]: Starting cloudResetPwdAgent...
systemd[2324]: cloudResetPwdAgent.service: Failed to execute command: Permission denied
systemd[2324]: cloudResetPwdAgent.service: Failed at step EXEC spawning /CloudrResetPwdAgent/bin/./
cloudResetPwdAgent.script: Permission denied
systemd[1]: cloudResetPwdAgent.service: Control process exited, code=exited status=203
systemd[1]: cloudResetPwdAgent.service: Failed with result 'exit-code'.
systemd[1]: Failed to start cloudResetPwdAgent.
```

The password reset plug-ins can be executed in the root directory only after Security-Enhanced Linux (SELinux) is disabled.

Solution

Step 1 Disable SELinux temporarily.

setenforce 0

Step 2 **Disable SELinux** permanently.

Step 3 Install the password reset plug-ins again.

sudo sh setup.sh

- If "cloudResetPwdAgent install successfully." is displayed and "Failed to start service cloudResetPwdAgent" is not displayed, the installation is successful.
- If the installation failed, check whether the installation environment meets requirements and install the plug-in again.

----End

13.14 How Can I Obtain the Key Pair Used by My ECS?

Symptom

You have created multiple key pairs, and you are trying to find the key pair to log in to the target ECS.

Procedure

1. Log in to the **management console**.
2. Click in the upper left corner and select a region and project.
3. Under **Compute**, click **Elastic Cloud Server**.
4. On the **Elastic Cloud Server** page, select the target ECS.
5. Click the name of the target ECS.

   The page providing details about the ECS is displayed.
6. Obtain the **Key Pair** value.

   The value is the key pair used by the ECS.

13.15 How Can I Use a Key Pair?

Symptom

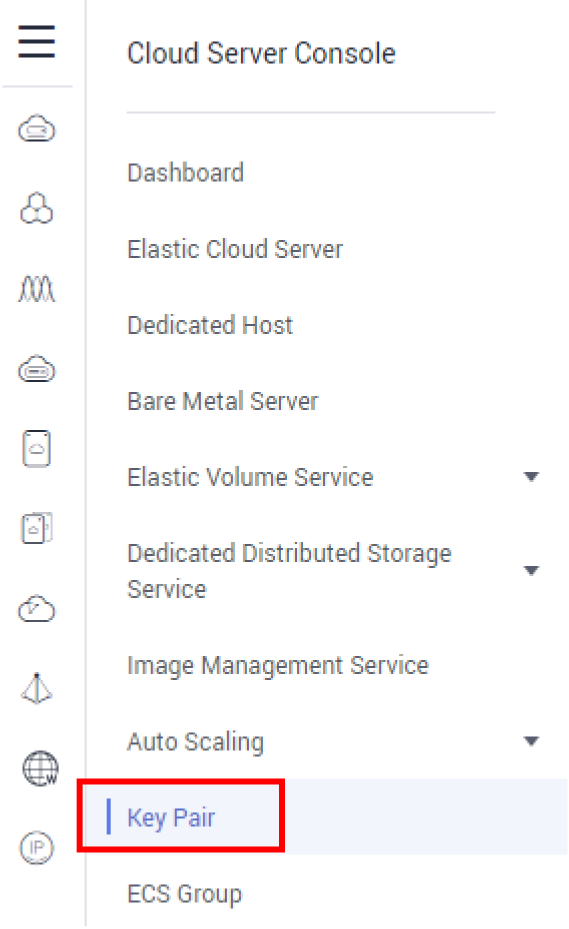
When you purchase an ECS, the system asks you to select a login mode. If you select **Key pair**, you are required to select an existing key pair or create a new pair.

If no key pair is available, create one on the management console.

Solution

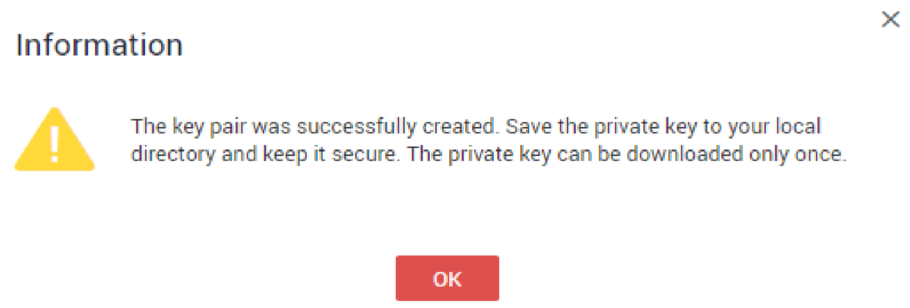
1. In the navigation pane of the ECS console, choose **Key Pair**. Then, click **Create Key Pair**.

Figure 13-18 Creating a key pair



2. After the key pair is created, download the private key to a local directory.

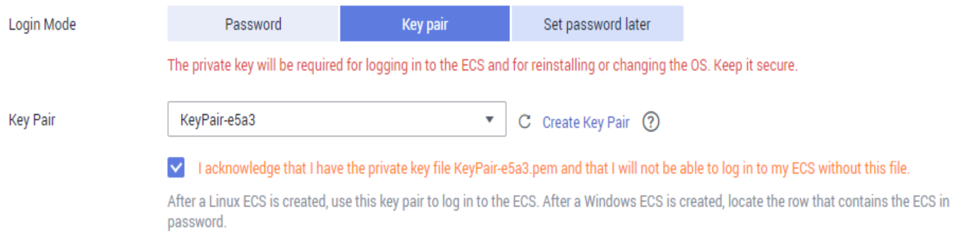
Figure 13-19 Downloading a key pair


Information

The key pair was successfully created. Save the private key to your local directory and keep it secure. The private key can be downloaded only once.

3. When purchasing an ECS, select the created or existing key pair in **Key pair**.

Figure 13-20 Selecting a key pair



The private key will be required for logging in to the ECS and for reinstalling or changing the OS. Keep it secure.

Key Pair: KeyPair-e5a3

☑ I acknowledge that I have the private key file KeyPair-e5a3.pem and that I will not be able to log in to my ECS without this file.

After a Linux ECS is created, use this key pair to log in to the ECS. After a Windows ECS is created, locate the row that contains the ECS in password.

13.16 Can I Download a Key Pair from My Phone?

No. This operation is not supported.

You can download the private key file only once when creating an ECS.

13.17 What Should I Do If a Key Pair Cannot Be Imported?

If you use Internet Explorer 9 to access the management console, the key pair may fail to import. In this case, perform the following steps to modify browser settings and then try again:

1. Click ⚙ in the upper right corner of the browser.
2. Select **Internet Options**.
3. Click the **Security** tab in the displayed dialog box.
4. Click **Internet**.
5. If the security level indicates **Custom**, click **Default Level** to restore to the default settings.
6. Move the scroll bar to set the security level to **Medium** and click **Apply**.
7. Click **Custom Level**.
8. Set **Initialize and script ActiveX controls not marked as safe for scripting** to **Prompt**.
9. Click **Yes**.

13.18 Why Does the Login to My Linux ECS Using a Key File Fail?

Symptom

When you use the key file created during your Linux ECS creation to log in to the ECS, the login fails.

Possible Causes

Possible causes vary depending on the image used to create the Linux ECS.

- Cause 1: The image that you used to create the Linux ECS is a private image, on which Cloud-Init is not installed.
- Cause 2: Cloud-Init is installed on the image, but you did not obtain the key pair when you created the ECS.

Solution

- If the issue is a result of cause 1, proceed as follows:

  If you created a private image without installing Cloud-Init, you cannot customize the ECS configuration. As a result, you can log in to the ECS only using the original image password or key pair.

  The original image password or key pair is the OS password or key pair you configured when you created the private image.

  If you have forgotten the original image password or the key pair is lost, reset the password on the ECS console.

  For details about Cloud-Init, see **(Optional) Installing and Configuring Cloud-Init**.
- If the issue is a result of cause 2, proceed as follows:
  a. Locate the row containing the target ECS, click **More** in the **Operation** column, and select **Restart**.
  b. Use the key file to log in to the ECS again and check whether the login is successful.
     - If the login is successful, no further action is required.
     - If it is not functional, contact customer service for technical support.

13.19 What Should I Do If I Cannot Download a Key Pair?

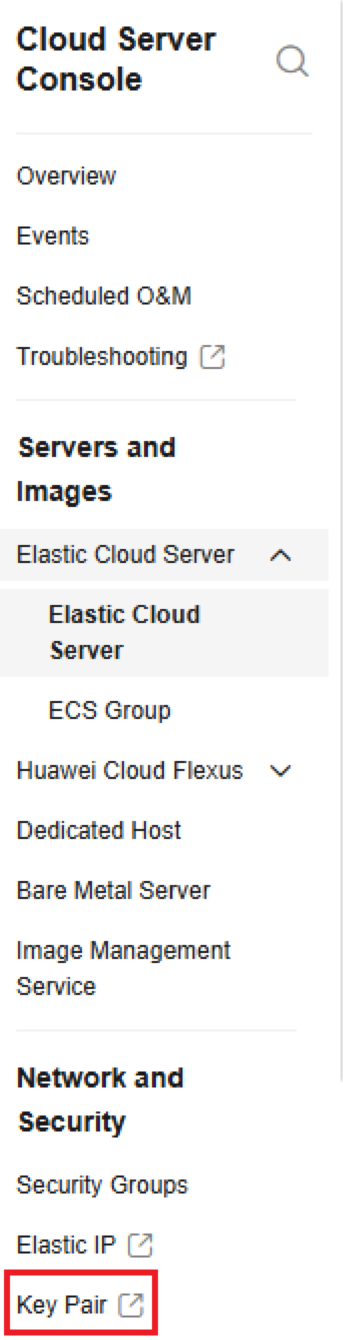
The private key file of a key pair can be downloaded only once.

If your private key file has been lost, create a key pair and download the private key file again.

Solution

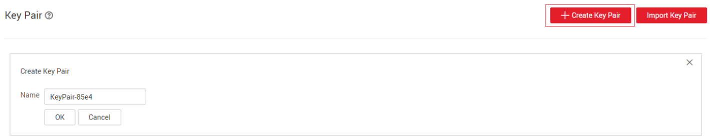
1. Log in to the **management console** and choose **Key Pair**.

Figure 13-21 Key Pair



2. Click **Create Key Pair**.

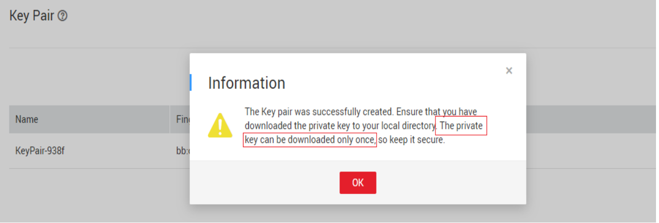
Figure 13-22 Creating a key pair



Name: KeyPair-85e4

3. Click **OK** to save the private key to your local directory.

Figure 13-23 Saving the private key



The Key pair was successfully created. Ensure that you have downloaded the private key to your local directory. The private key can be downloaded only once, so keep it secure.

13.20 Why Does a Key Pair Created Using puttygen.exe Fail to Be Imported on the Management Console?

Symptom

When you try to import a key pair that you created using **puttygen.exe** on the management console, the system displays a message indicating that the import failed.

Possible Causes

The format of the public key content does not meet system requirements.

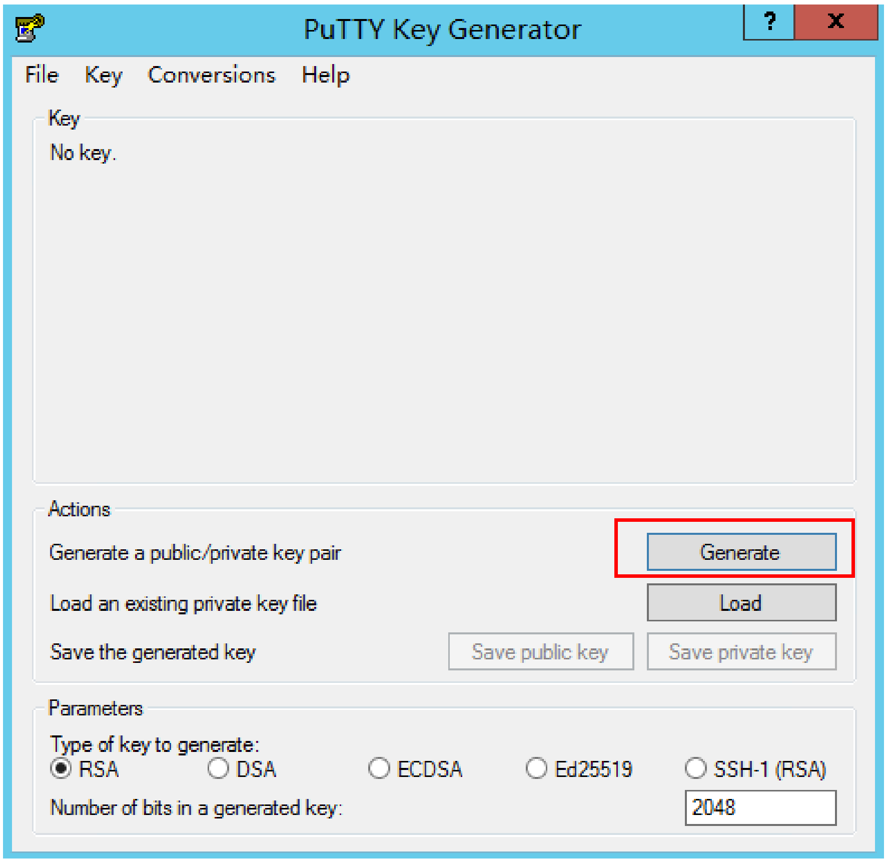
If you store a public key by clicking **Save public key** on PuTTY Key Generator, the format of the public key content will change. You cannot import the key on the management console.

Solution

Use the locally stored private key and **PuTTY Key Generator** to restore the format of the public key content. Then, import the public key to the management console.

1. Double-click **puttygen.exe** to open **PuTTY Key Generator**.

Figure 13-24 PuTTY Key Generator



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

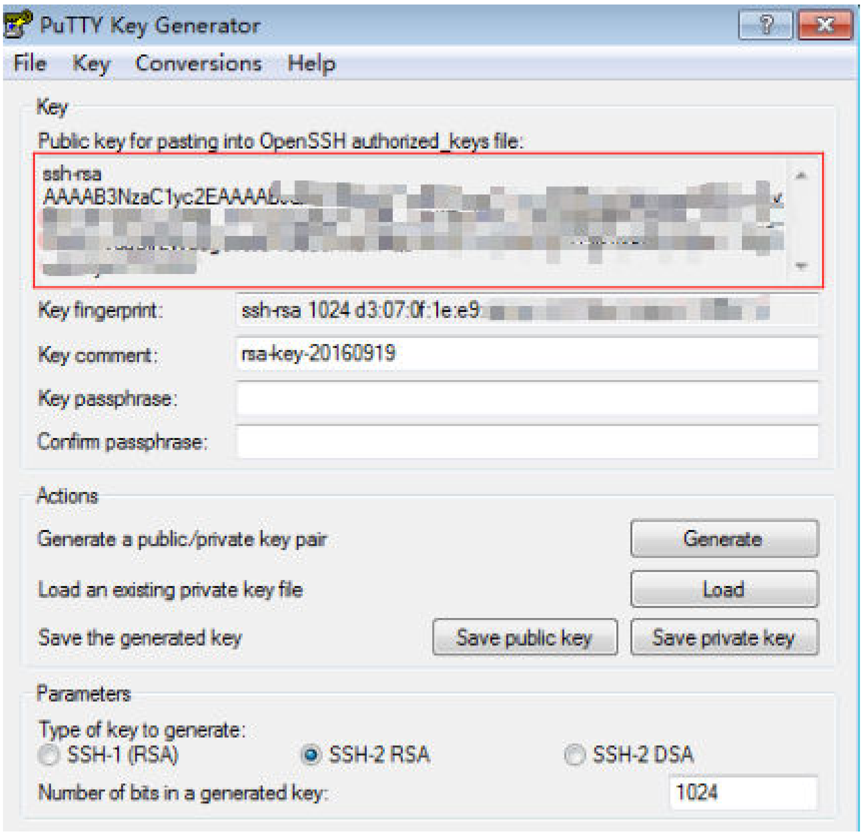
Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

2. Click **Load** and select the private key.

   The system automatically loads the private key and restores the format of the public key content in **PuTTY Key Generator**. The content in the red box in **Figure 13-25** is the public key whose format meets system requirements.

Figure 13-25 Restoring the format of the public key content



Key

Public key for pasting into OpenSSH authorized_keys file:

ssh-rsa
AAAAB3NzaC1yc2EAAAAB[redacted]

Key fingerprint: ssh-rsa 1024 d3:07:0f:1e:e9[redacted]

Key comment: rsa-key-20160919

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

3. Copy the public key content to a .txt file and save the file in a local directory.
4. Import the public key to the management console.
   a. Log in to the **management console**.
   b. Click in the upper left corner and select a region and project.
   c. Under **Compute**, click **Elastic Cloud Server**.
   d. In the navigation pane on the left, choose **Key Pair**.
   e. On the key pair page, click **Import Key Pair**.
   f. Copy the public key content in the .txt file to **Public Key Content** and click **OK**.

13.21 What Is the Cloudbase-Init Account in Windows ECSs Used for?

Description

In Windows ECSs, **cloudbase-init** is the default user of the Cloudbase-Init agent program. It is used to obtain the metadata and execute configurations when an ECS starts.

NOTE

This account is unavailable on Linux ECSs.

Do not modify or delete this account or uninstall the Cloudbase-Init agent program. Otherwise, you will be unable to inject data to initialize an ECS created using a Windows private image.

Security Hardening for Random cloudbase-init Passwords

In Cloudbase-Init 0.9.10, the security of random **cloudbase-init** passwords has been hardened to ensure that the hash values (LM-HASH and NTLM-HASH) of the passwords are different.

In Windows, the hash passwords are in the format of "Username:RID:LM-HASH value:NT-HASH value".

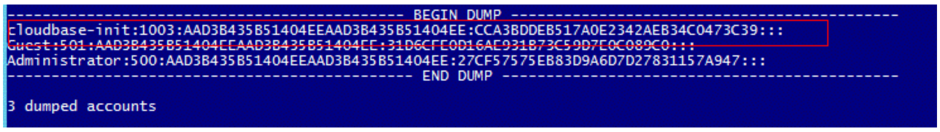
For example, in "Administrator:500:C8825DB10F2590EAAAD3B435B51404EE:683020925C5D8569C23AA724774CE9CC:::",

- Username: **Administrator**
- RID: **500**
- LM-HASH value: **C8825DB10F2590EAAAD3B435B51404EE**
- NT-HASH value: **683020925C5D8569C23AA724774CE9CC**

Use an image to create two ECSs, ecs01 and ecs02. Then, verify that the hash values of the **cloudbase-init** account for the two ECSs are different.

- LM-HASH and NTLM-HASH values of the **cloudbase-init** account for ecs01

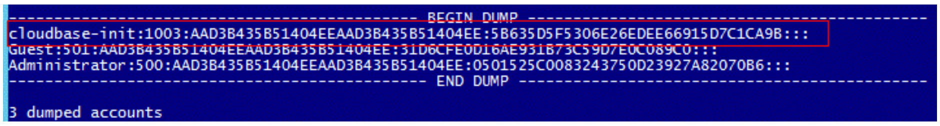
Figure 13-26 ecs01



```
--------------------------------------------- BEGIN DUMP ---------------------------------------------
cloudbase-init:1003:AAD3B435B51404EEAAD3B435B51404EE:CCA3BDDEB517A0E2342AEB34C0473C39:::
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::
Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:27CF57575EB83D9A6D7D27831157A947:::
---------------------------------------------- END DUMP ----------------------------------------------

3 dumped accounts
```

- LM-HASH and NTLM-HASH values of the **cloudbase-init** account for ecs02

Figure 13-27 ecs02



```
--------------------------------------------- BEGIN DUMP ---------------------------------------------
cloudbase-init:1003:AAD3B435B51404EEAAD3B435B51404EE:5B635D5F5306E26EDEE66915D7C1CA9B:::
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::
Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:0501525C0083243750D23927A82070B6:::
---------------------------------------------- END DUMP ----------------------------------------------

3 dumped accounts
```

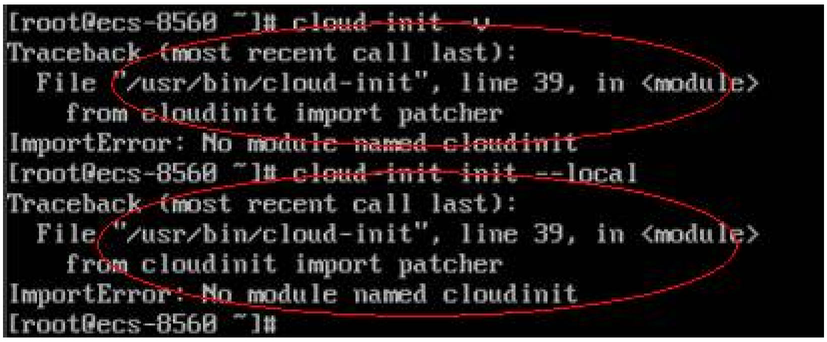
13.22 What Should I Do If Cloud-Init Does Not Work After Python Is Upgraded?

Symptom

Take an ECS running CentOS 6.8 as an example. After Python was upgraded from 2.6 to 2.7, Cloud-Init did not work. Data, such as the login password, key, and hostname could not be imported to the ECS using Cloud-Init.

After the **cloud-init -v** command was executed to view the Cloud-Init version, the system displayed errors, as shown in **Figure 13-28**.

Figure 13-28 Improper running of Cloud-Init



```
[root@ecs-8560 ~]# cloud-init -v
Traceback (most recent call last):
  File "/usr/bin/cloud-init", line 39, in <module>
    from cloudinit import patcher
ImportError: No module named cloudinit
[root@ecs-8560 ~]# cloud-init init --local
Traceback (most recent call last):
  File "/usr/bin/cloud-init", line 39, in <module>
    from cloudinit import patcher
ImportError: No module named cloudinit
[root@ecs-8560 ~]#
```

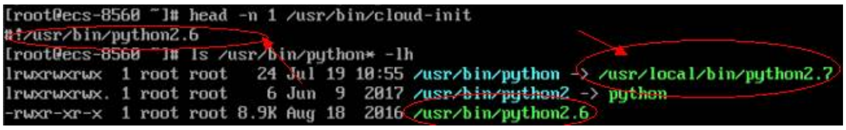
Possible Causes

The Python version used by Cloud-Init was incorrect.

Solution

Change the Python version used by Cloud-Init to the source version. To do so, change the environment variable value of **/usr/bin/cloud-init** from the default value **#!/usr/bin/python** to **#!/usr/bin/python2.6**.

Figure 13-29 Changing the Python version



```
[root@ecs-8560 ~]# head -n 1 /usr/bin/cloud-init
#!/usr/bin/python2.6
[root@ecs-8560 ~]# ls /usr/bin/python* -lh
lrwxrwxrwx  1 root root   24 Jul 19 10:55 /usr/bin/python -> /usr/local/bin/python2.7
lrwxrwxrwx. 1 root root    6 Jun  9  2017 /usr/bin/python2 -> python
-rwxr-xr-x  1 root root 8.9K Aug 18  2016 /usr/bin/python2.6
```

14 Application Deployment and Software Installation

14.1 Can a Database Be Deployed on an ECS?

Yes. You can deploy a database of any type on an ECS.

14.2 Does an ECS Support Oracle Databases?

Yes. You are advised to perform a performance test beforehand to ensure that the Oracle database can meet your requirements.

14.3 What Should I Do If a Msg 823 Error Occurs in Oracle, MySQL, or SQL Server System Logs After a Disk Initialization Script Is Executed?

Symptom

After a disk is added to an ECS and the disk initialization script is automatically executed upon ECS startup, the Msg 823 error occurs in the database system logs of the Oracle, MySQL, and SQL Server databases.

Possible Causes

During the execution of the disk initialization script **WinVMDataDiskAutoInitialize.ps1**, diskpart is invoked to enable the virtual disk service. After the execution is complete, diskpart exits and the virtual disk service is disabled. The automatic startup period of the built-in WinVMDataDiskAutoInitialize.ps1 overlaps the automatic startup period of the customer's database services, which may cause I/O operation errors.

The database uses Windows APIs (for example, ReadFile, WriteFile, ReadFileScatter, WriteFileGather) to perform file I/O operations. After performing these I/O operations, the database checks for any error conditions associated with these API calls. If the API calls fail with an operating system error, the database reports error 823. To obtain Microsoft official instructions, see **MSSQLSERVER error 823**.

The 823 error message contains the following information:

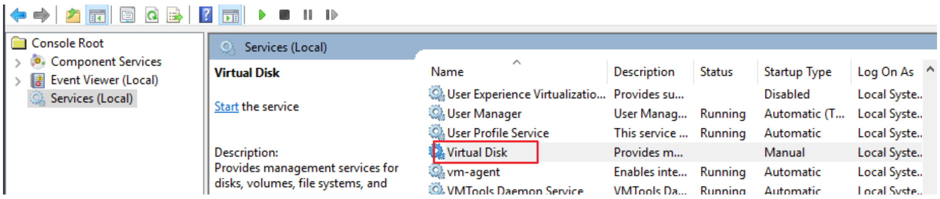
- Whether the I/O operation is a read or write request
- The offset within the file where the I/O operation was attempted
- The database file against which the I/O operation was performed
- The operating system error code and error description in parentheses

The 823 error message usually indicates that there is a problem with underlying storage system or the hardware or a driver that is in the path of the I/O request. You can encounter this error when there are inconsistencies in the file system or if the database file is damaged.

Solution

1. Log in to the ECS, open the **Run** dialog box, enter **services.msc**, and press **Enter**.
2. Search for the virtual disk service and ensure that it has been stopped.

   Figure 14-1 Checking the virtual disk status



Virtual Disk

Start the service

Description:
Provides management services for disks, volumes, file systems, and

Name	Description	Status	Startup Type	Log On As
User Experience Virtualizatio...	Provides su...		Disabled	Local Syste..
User Manager	User Manag...	Running	Automatic (T...	Local Syste..
User Profile Service	This service ...	Running	Automatic	Local Syste..
Virtual Disk	Provides m...		Manual	Local Syste..
vm-agent	Enables inte...	Running	Automatic	Local Syste..
VMTools Daemon Service	VMTools Da...	Running	Automatic	Local Syste..

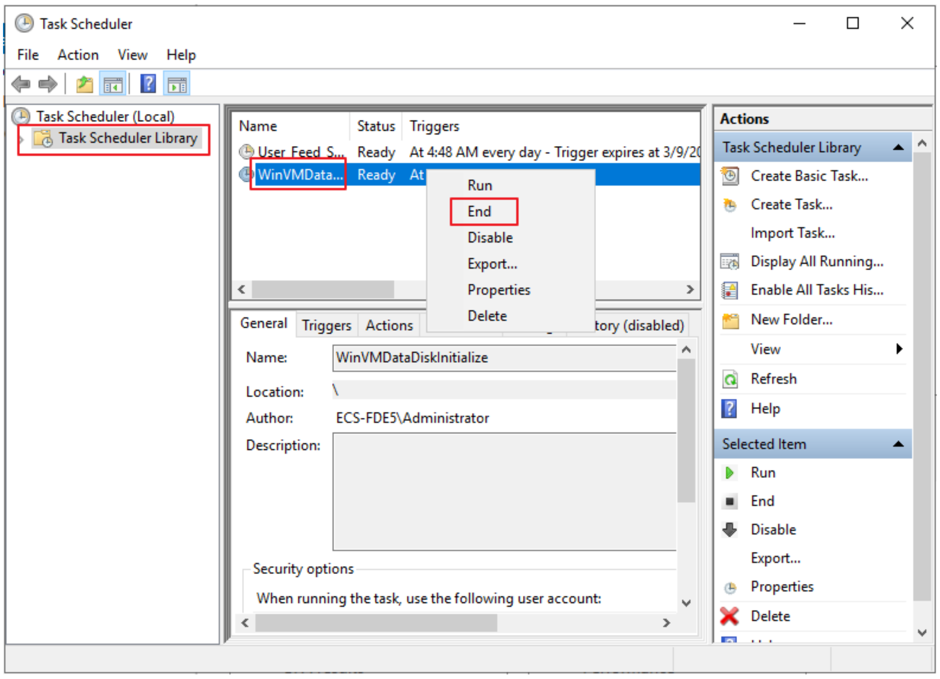
   If the virtual disk service is running, stop it in either of the following ways:

   - On the **Services** page of the Windows operating system, right-click **Virtual Disk** and choose **Stop**.
   - Open PowerShell and run the following command to stop the virtual disk service:

     Get-Service -Name "vds" | Where {$_.status -eq 'Running'} | Stop-Service -Force

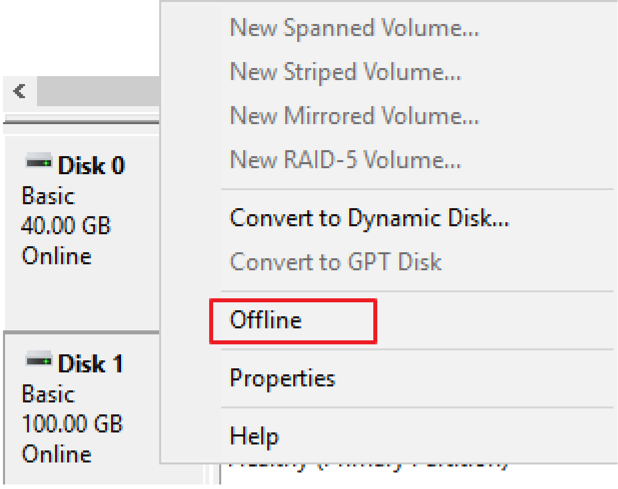
3. Disable the disk initialization script WinVMDataDiskAutoInitialize.ps1 from automatically initializing Windows data disks upon ECS startup.
   a. Open the **Run** dialog box, enter **taskschd.msc**, and press **Enter.** The **Task Scheduler** window is displayed.
   b. Open **Task Scheduler Library**, right-click **WinVMDataDiskInitialize** in the scheduled task list, and choose **End**.

Figure 14-2 Ending WinVMDataDiskInitialize



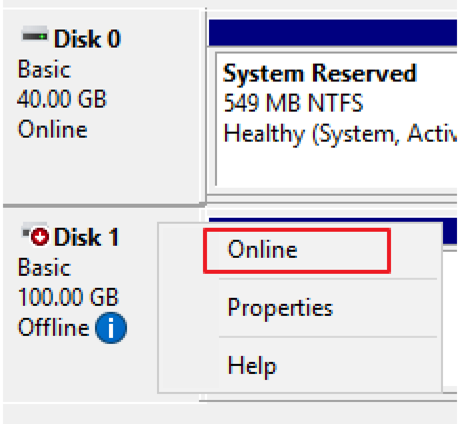
4. Restart the ECS or take the data disk offline and then online.
   a. Open the **Run** dialog box, enter **diskmgmt.msc**, and press **Enter**. The **Disk Management** window is displayed.
   b. Right-click the block to which the disk belongs and choose **Offline**.

Figure 14-3 Setting disk offline



   c. Right-click the block to which the disk belongs and choose **Online**.

Figure 14-4 Setting disk online



15 File Upload/Data Transfer

15.1 How Do I Upload Files to My ECS?

Windows

- File transfer tool

  Install a file transfer tool, such as FileZilla on both the local computer and the Windows ECS and use it to transfer files. For details, see **How Can I Use FTP to Transfer Files from a Local Windows Computer to a Windows or Linux ECS?**
- (Recommended) Local disk mapping

  Use MSTSC to transfer files. This method does not support resumable transmission. Do not use this method to transfer large files.

  For details, see **How Can I Transfer Files from a Local Windows Computer to a Windows ECS?**
- FTP site

  Transfer files through an FTP site. Before transferring files from a local computer to a Windows ECS, set up an FTP site on the ECS and install FileZilla on the local computer.

  For details, see **How Can I Use FTP to Transfer Files from a Local Windows Computer to a Windows or Linux ECS?**
- OBS

  You can use OBS to store any type of data. After storing data such as images and videos in OBS buckets, you can access OBS from the ECS and download data from the buckets. For details, see **How Can I Use OBS to Transfer Files from a Local Windows Computer to a Windows ECS?**
- From a local Mac

  If your local computer runs macOS, use Microsoft Remote Desktop for Mac to transfer files to the Windows ECS. For details, see **How Can I Transfer Files from a Local Mac to a Windows ECS?**

Linux

- From a local Windows computer

  Use WinSCP to transfer the files to the Linux ECS. For details, see **How Can I Use WinSCP to Transfer Files from a Local Windows Computer to a Linux ECS?**

  Before transferring files from a local computer to a Linux ECS, set up an FTP site on the ECS and install FileZilla on the local computer. For details, see **How Can I Use FTP to Transfer Files from a Local Windows Computer to a Windows or Linux ECS?**

- From a local Linux computer

  Use SCP to transfer the files to the Linux ECS. For details, see **How Can I Use SCP to Transfer Files Between a Local Linux Computer and a Linux ECS?**

  Use SFTP to transfer the files to the Linux ECS. For details, see **How Can I Use SFTP to Transfer Files Between a Local Linux Computer and a Linux ECS?**

  Use FTP to transfer the files to the Linux ECS. For details, see **How Can I Use FTP to Transfer Files Between a Local Linux Computer and a Linux ECS?**

Does an ECS Support FTP-based File Transferring by Default?

No. You need to install and configure FTP so that the ECS supports FTP-based file transfer.

15.2 How Can I Transfer Files from a Local Windows Computer to a Windows ECS?

Scenarios

You want to transfer files from a local Windows computer to a Windows ECS through an MSTSC-based remote desktop connection.

Prerequisites

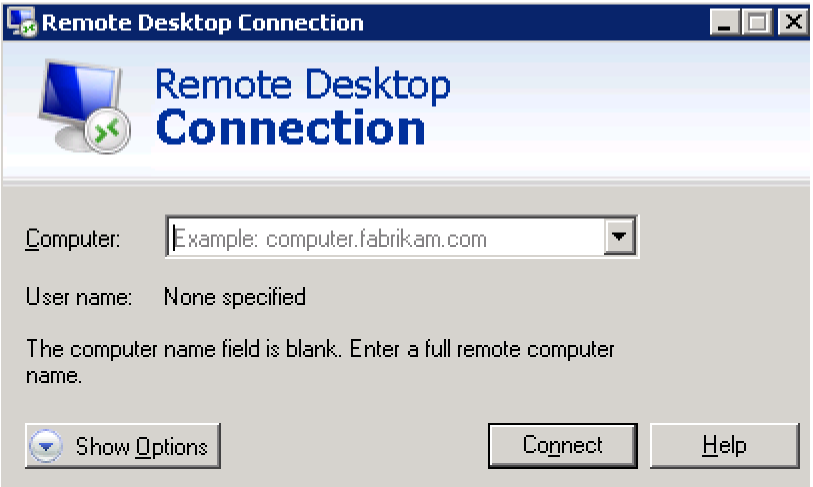
- The target ECS is running.
- An EIP has been bound to the ECS. For details, see **Binding an EIP**.
- Access to port 3389 is allowed in the inbound direction of the security group which the ECS belongs to. For details, see **Configuring Security Group Rules**.

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**.

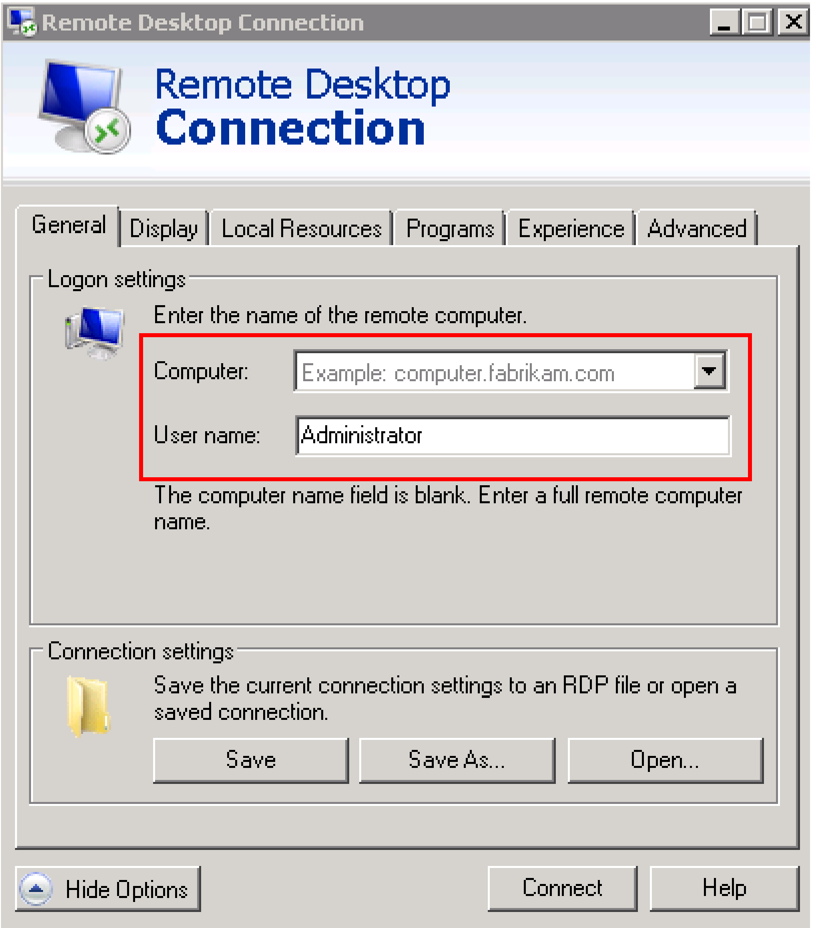


Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

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



Enter the name of the remote computer.

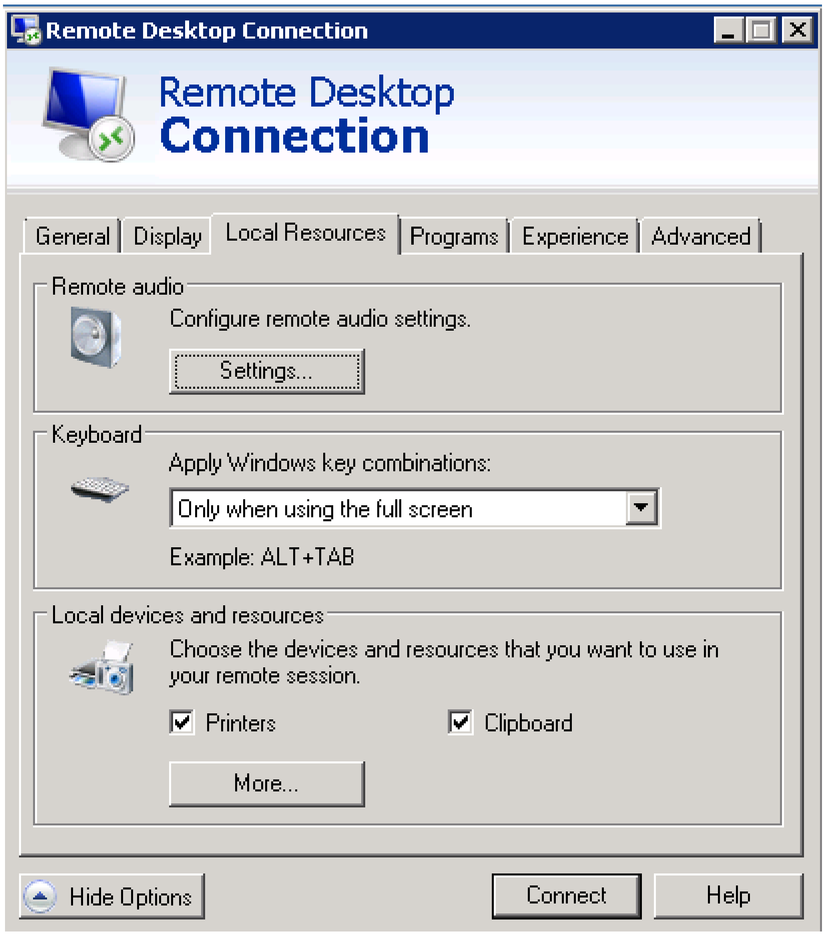
Computer: Example: computer.fabrikam.com

User name: Administrator

The computer name field is blank. Enter a full remote computer name.

Save the current connection settings to an RDP file or open a saved connection.

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



Configure remote audio settings.

Apply Windows key combinations:

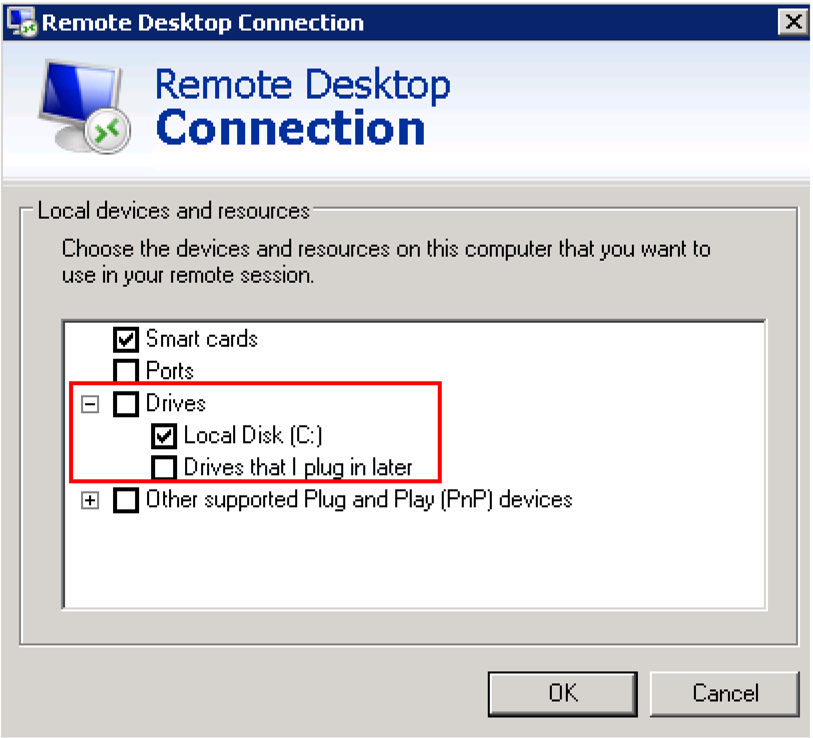
Only when using the full screen

Example: ALT+TAB

Choose the devices and resources that you want to use in your remote session.

☑ Printers ☑ Clipboard

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



Choose the devices and resources on this computer that you want to use in your remote session.

☑ Smart cards
☐ Ports
☐ Drives
  ☑ Local Disk (C:)
  ☐ Drives that I plug in later
☐ Other supported Plug and Play (PnP) devices

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

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

15.3 How Can I Use OBS to Transfer Files from a Local Windows Computer to a Windows ECS?

Scenarios

Through an intranet, an ECS can access OBS in which any type of data can be stored. After storing data such as images and videos in OBS, you can access OBS from the ECS and download data from OBS. The intranet access is free of charge and prevents data transmission interruptions caused by unstable networks. This maximizes transmission performance, reduces traffic costs, and minimizes data transmission failures.

NOTE

When you access OBS through an intranet, ensure that the target OBS resources are in the region where the ECS resides. If they are in different regions, you can access the OBS only through the Internet and traffic fees will be incurred.

Procedure

To transfer files to a Windows ECS using OBS Browser+, perform the following operations:

- **Step 1: Create a Bucket on the OBS Management Console**

  Before transferring files from a local computer to OBS, create a bucket.

  This section describes how to create a bucket on the OBS management console. For more details about how to create a bucket, see **Creating a Bucket**.

- **Step 2: Upload Local Files to the Bucket Using OBS Browser+**

  After creating a bucket, you can upload files to the bucket. OBS stores the files you upload to the bucket as objects.

  This section uses OBS Browser+ as an example to upload files.

  NOTE

  - Through the OBS management console, you can upload files with a total size lesser than 5 GB.
    - In batch upload mode, you can upload a maximum of 100 files at a time, and the total size of the files cannot exceed 5 GB.
    - In single upload mode, you can upload only one file at a time, and the file size cannot exceed 50 MB.
  - Using OBS Browser+ and obsutil, you can upload files with a total size lesser than 48.8 TB.
  - Using SDK/API PUT, POST, or append operations, you can upload files with a total size lesser than 5 GB.
  - Using SDK/API multipart upload or API resumable upload, you can upload files with a total size lesser than 48.8 TB.

  For details, see **Uploading an Object**.

- **Step 3: Use OBS Browser+ on the Windows ECS to Access the Bucket Through the Intranet**

  OBS Browser+ is a GUI-based Windows desktop application for OBS resource management. After configuring the private DNS server address of your ECS, you can use OBS Browser+ to access the bucket through the intranet and download data such as images and videos from the bucket.

Step 1: Create a Bucket on the OBS Management Console

1. In the navigation pane on the OBS management console, select **Object Storage**.
2. Click **Create Bucket** in the upper right corner of the page.
3. Choose a region and set the bucket name.
4. Set a storage class. In this example, **Standard** is the storage class.

   Standard storage is suitable for frequently accessed (multiple times per month) data such as small and essential files that require low latency.

   The storage class of a bucket is inherited by objects uploaded to the bucket by default. You can also change the storage class of an object when uploading it to the bucket.
5. Set other parameters, such as **Bucket Policy**, **Default Encryption**, and **Direct Reading**. For details, see **Creating a Bucket**. In this example, default settings are retained.
6. Click **Create Now**. The created bucket is displayed on the **Object Storage Service** page.

Step 2: Upload Local Files to the Bucket Using OBS Browser+

Step 1 Create access keys (AK and SK) on the management console.

When you access OBS using OBS Browser+, OBS requires the access keys (AK and SK) for authentication. Therefore, obtain the access keys (AK and SK) before you access OBS.

1. Log in to the **management console**. Hover over the username in the upper right corner and select **My Credentials** from the drop-down list.
2. In the navigation pane, select **Access Keys**.
3. Click **Create Access Key**.
4. In the **Create Access Key** dialog box, enter the login password.
5. Enter the verification code sent to your email or mobile phone.
6. Click **OK** to download the access key. Anyone who possesses your access keys can decrypt your login information. Therefore, keep your access keys secure.

Step 2 Install OBS Browser+ on the local computer.

1. Download the OBS Browser+ installation package.

   For details, see **Downloading OBS Browser+**.

   NOTE

   Currently, the OBS Browser+ package is stored in a bucket in the **CN North-Beijing1** region. Servers in the **CN North-Beijing1** region can download the package through the private network. Servers not in the **CN North-Beijing1** region can download the package using EIPs. Alternatively, you can upload the package to a bucket in the same region as your server and then download the package.
2. Decompress the downloaded software package and run **obs-browser-plus Setup *xxx*.exe** to install OBS Browser+.
3. Double-click **obs-browser-plus** on the **Start** menu or the desktop shortcut to run OBS Browser+.

Step 3 Log in to OBS Browser+.

For details, see **Logging In to OBS Browser+**.

Step 4 Use OBS Browser+ to upload files.

After logging in to OBS Browser+, search for the bucket created in **Step 1: Create a Bucket on the OBS Management Console** to access data.

For details, see **OBS Browser+ Best Practices**.

----End

Step 3: Use OBS Browser+ on the Windows ECS to Access the Bucket Through the Intranet

Step 1 Log in to the Windows ECS and check whether the private DNS server address has been configured.

In the cmd window, run the **ipconfig /all** command to check whether the **DNS Server** value is the private DNS server address in the region where the ECS resides.

NOTE

Huawei Cloud provides different private DNS server addresses for different regions. For details, see **What Are Huawei Cloud Private DNS Server Addresses?**

If the private DNS server address has not been configured, **configure the intranet DNS**.

Step 2 Install OBS Browser+ on the ECS.

1. Download the OBS Browser+ installation package.

   For details, see **Downloading OBS Browser+**.

2. Decompress the downloaded software package and run **obs-browser-plus Setup *xxx*.exe** to install OBS Browser+.
3. Double-click **obs-browser-plus** on the **Start** menu or the desktop shortcut to run OBS Browser+.

Step 3 Log in to OBS Browser+.

For details, see **Logging In to OBS Browser+**.

Step 4 Use OBS Browser+ to download files from the bucket.

After logging in to OBS Browser+, search for the bucket created in **Step 1: Create a Bucket on the OBS Management Console**. Then, you can access OBS through the Huawei Cloud intranet on the Windows ECS to perform basic data access operations and other advanced settings.

For details, see **OBS Browser+ Best Practices**.

Then, files are transferred from the local Windows computer to the Windows ECS using OBS Browser+.

----End

15.4 How Can I Use WinSCP to Transfer Files from a Local Windows Computer to a Linux ECS?

Scenarios

WinSCP can be used to securely copy-paste files across local and remote computers. Compared with FTP, WinSCP allows you to use a username and password to access the destination server without any additional configuration on the server.

To transfer a file from a local Windows computer to a Linux ECS, WinSCP is commonly used. This section describes how to transfer files from a local Windows computer to a Linux ECS using WinSCP. In this example, the ECS running CentOS 7.2 is used as an example.

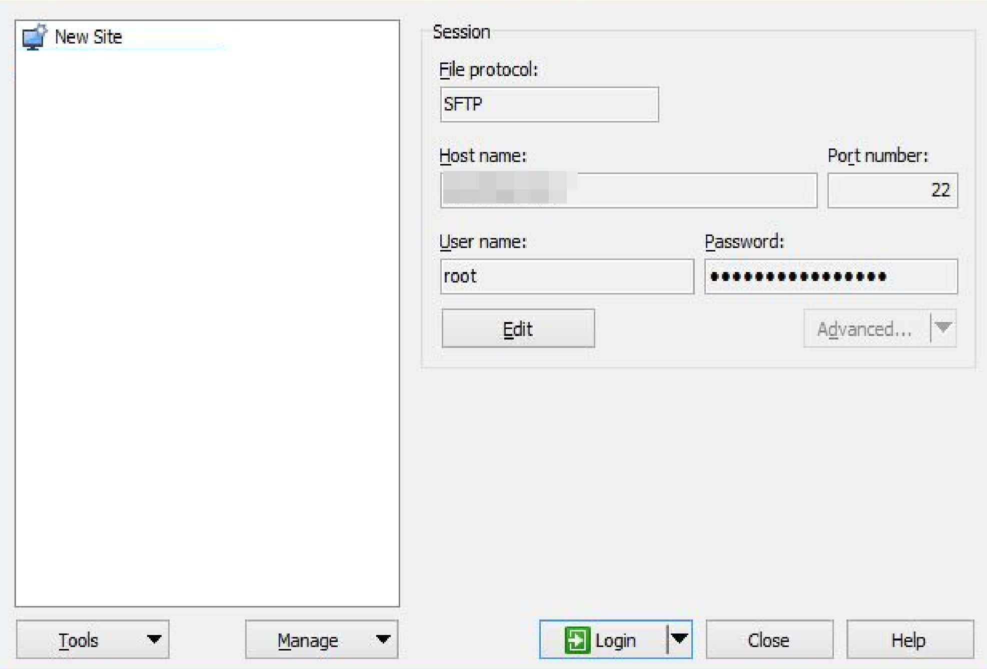
Prerequisites

- The target ECS is running.
- An EIP has been bound to the ECS. For details, see **Binding an EIP**.

- Access to port 22 is allowed in the inbound direction of the security group which the ECS belongs to. For details, see **Configuring Security Group Rules**.

Solution

1. **Download WinSCP**.
2. Install WinSCP.
3. Start WinSCP.



File protocol: SFTP
Host name: [redacted]
Port number: 22
User name: root
Password: ••••••••••••••••

Set parameters as follows:

   - **File protocol**: Set this to **SFTP** or **SCP**.
   - **Host name**: Enter the EIP bound to the ECS. 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 ECS.
     - If the ECS is logged in using an SSH key pair:
       - The username is **core** for a CoreOS public image.
       - The username is **root** for a non-CoreOS public image.
     - If the ECS is logged in using a password, the username is **root** for a public image (including CoreOS).
   - **Password**: the password set when you purchased the ECS or converted using a key.

4. Click **Login**.
5. Drag a file from the local computer on the left to the remotely logged in ECS on the right to transfer the file.

15.5 How Can I Transfer Files from a Local Mac to a Windows ECS?

Scenarios

This section describes how to use Microsoft Remote Desktop for Mac to transfer files from a local Mac to a Windows ECS.

Prerequisites

- The remote access tool supported by Mac has been installed on the local Mac. This section uses Microsoft Remote Desktop for Mac as an example. **Download Microsoft Remote Desktop for Mac**.
- The target Windows ECS has had an EIP bound.
- When you log in to the ECS for the first time, ensure that RDP has been enabled on it. To do so, use VNC to log in to the ECS, enable RDP, and access the ECS using MSTSC.

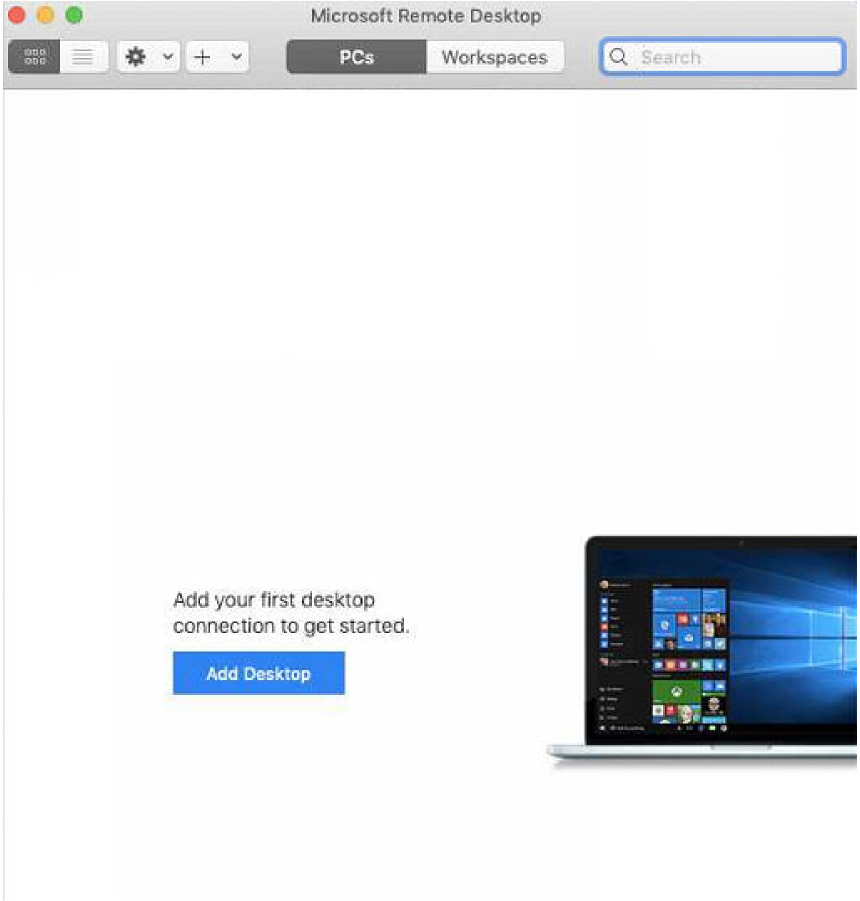
  NOTE

  By default, RDP has been enabled on the ECSs created using a public image.

Procedure

1. Start Microsoft Remote Desktop.
2. Click **Add Desktop**.

Figure 15-1 Add Desktop



3. Set login parameters.
   - **PC name**: Enter the EIP bound to the target Windows ECS.
   - **User account**: Select **Add User Account** from the drop-down list.

     The **Add a User Account** dialog box is displayed.

     i. Enter the username **administrator** and password for logging in to the Windows ECS and click **Add**.

Figure 15-2 Add user account

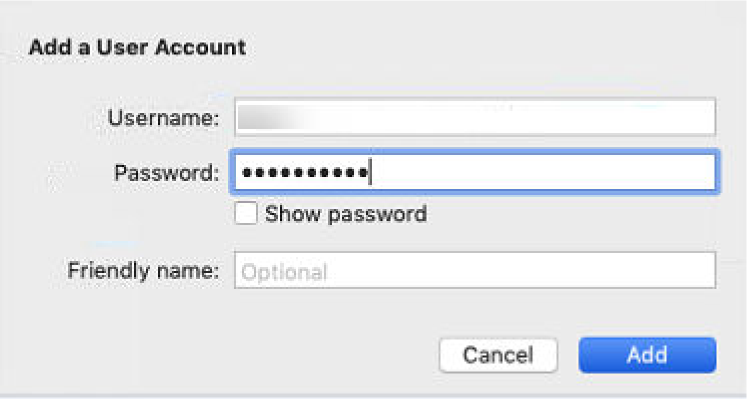
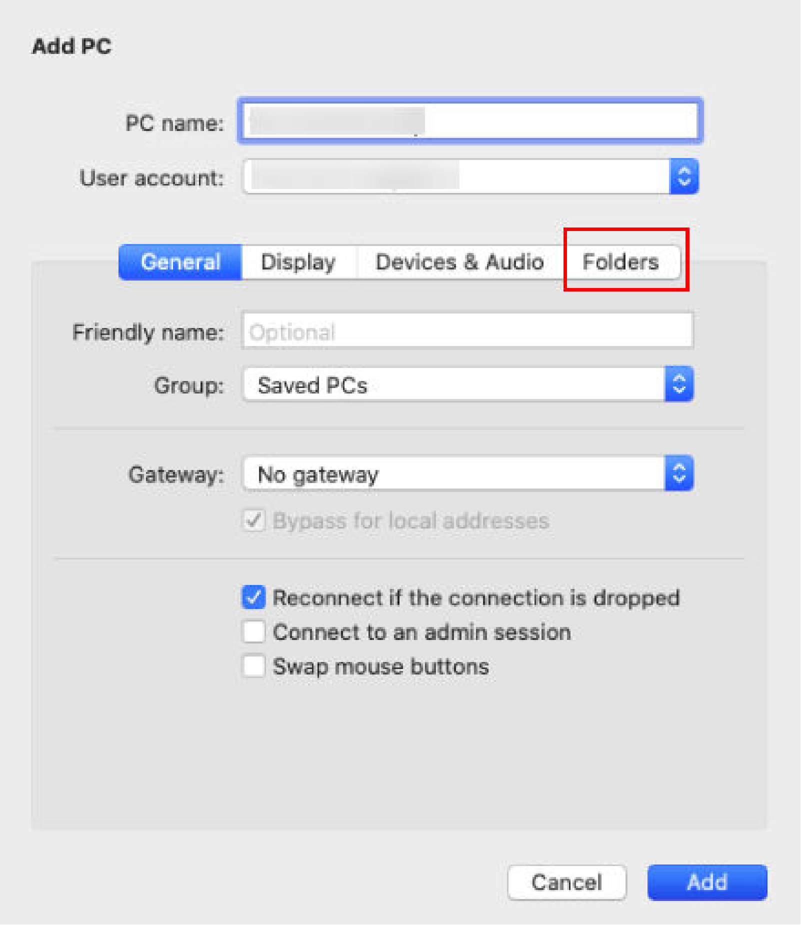
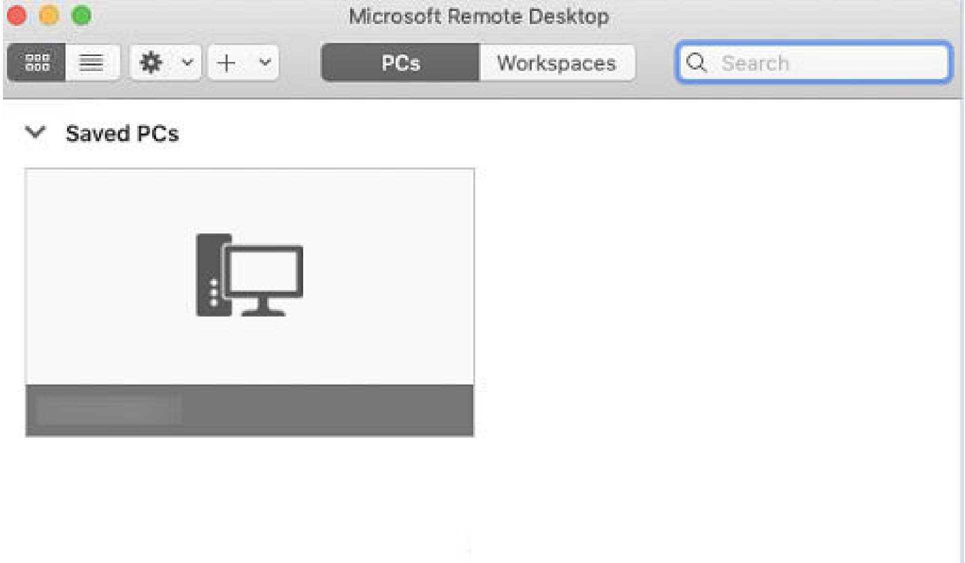


Figure 15-3 Add PC



4. Select the folder to be uploaded.
   a. Click **Folders** and switch to the folder list.
   b. Click + in the lower left corner, select the folder to be uploaded, and click **Add**.
5. On the **Remote Desktop** page, double-click the icon of the target Windows ECS.

Figure 15-4 Double-click for login



6. Confirm the information and click **Continue**.

   You have connected to the Windows ECS.

   View the shared folder on the ECS.

   Copy the files to be uploaded to the ECS. Alternatively, download the files from the ECS to your local Mac.

15.6 How Can I Use SCP to Transfer Files Between a Local Linux Computer and a Linux ECS?

Scenarios

You want to use SCP to transfer files between a local Linux computer and a Linux ECS.

Procedure

Log in to the management console. On the **Elastic Cloud Server** page, obtain the EIP bound to the target ECS in the **IP Address** column.

- **Uploading files**

  Run the following command on the local Linux computer to upload files to the Linux ECS:

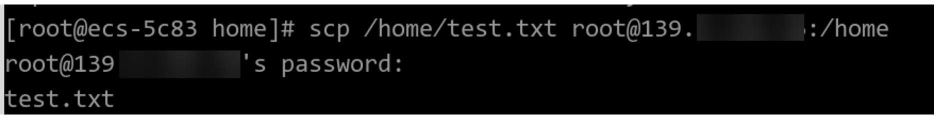
  scp *Path in which the files are stored on the local computer Username@EIP:Path in which the files are to be stored on the Linux ECS*

  For example, to transfer the **/home/test.txt** file on the local computer to the **/home** directory on the ECS whose EIP is 139.x.x.x, run the following command:

  scp /home/test.txt root@139.x.x.x:/home

  Enter the login password as prompted.

Figure 15-5 Setting file uploading



```
[root@ecs-5c83 home]# scp /home/test.txt root@139.[redacted]:/home
root@139[redacted]'s password:
test.txt
```

- **Downloading files**

  Run the following command on the local Linux computer to download files from the Linux ECS:

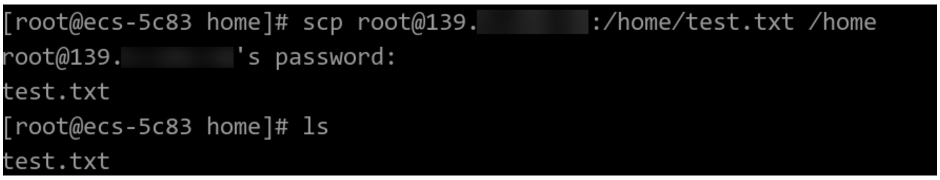
  scp *Username@EIP:Path in which the files are stored on the Linux ECS Path in which the files are to be stored on the local computer*

  For example, to download the **/home/test.txt** file on the ECS whose EIP is 139.x.x.x to the **/home** directory on the local computer, run the following command:

  scp root@139.x.x.x:/home/test.txt /home/

  Enter the login password as prompted.

Figure 15-6 Setting file downloading



```
[root@ecs-5c83 home]# scp root@139.[redacted]:/home/test.txt /home
root@139.[redacted]'s password:
test.txt
[root@ecs-5c83 home]# ls
test.txt
```

15.7 How Can I Use SFTP to Transfer Files Between a Local Linux Computer and a Linux ECS?

Scenarios

You want to use SFTP to transfer files between a local Linux computer and a Linux ECS. The following uses CentOS as an example.

Procedure

1. Log in to the ECS as user **root**.
2. Run the following command to check the OpenSSH version, which is expected to be 4.8p1 or later:

   ssh -V

   Information similar to the following is displayed:

   ```
   # OpenSSH_7.4p1, OpenSSL 1.0.2k-fips 26 Jan 2017
   ```

3. Create a user group and a user (for example, **user1**).

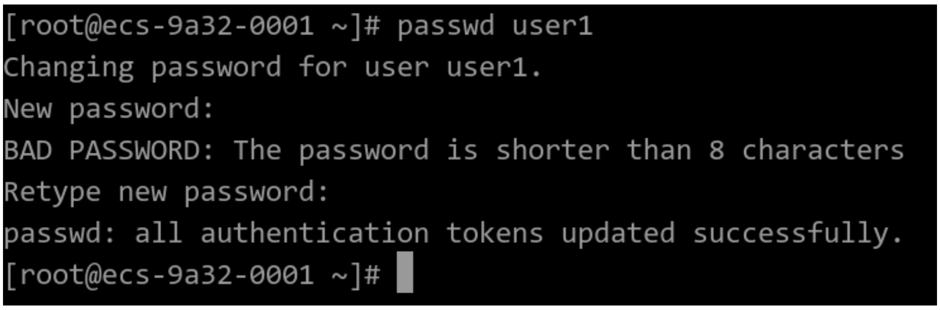
   groupadd sftp

   useradd -g sftp -s /sbin/nologin user1

4. Set a password for the user.

   passwd user1

Figure 15-7 Setting a password



```
[root@ecs-9a32-0001 ~]# passwd user1
Changing password for user user1.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ecs-9a32-0001 ~]#
```

5. Assign permissions to directories.

   chown root:sftp /home/user1

   chmod 755 -R /home/user1

   mkdir /home/user1/upload

   chown -R user1:sftp /home/user1/upload

   chmod -R 755 /home/user1/upload

6. Run the following command to edit the **sshd_config** configuration file:

   vim /etc/ssh/sshd_config

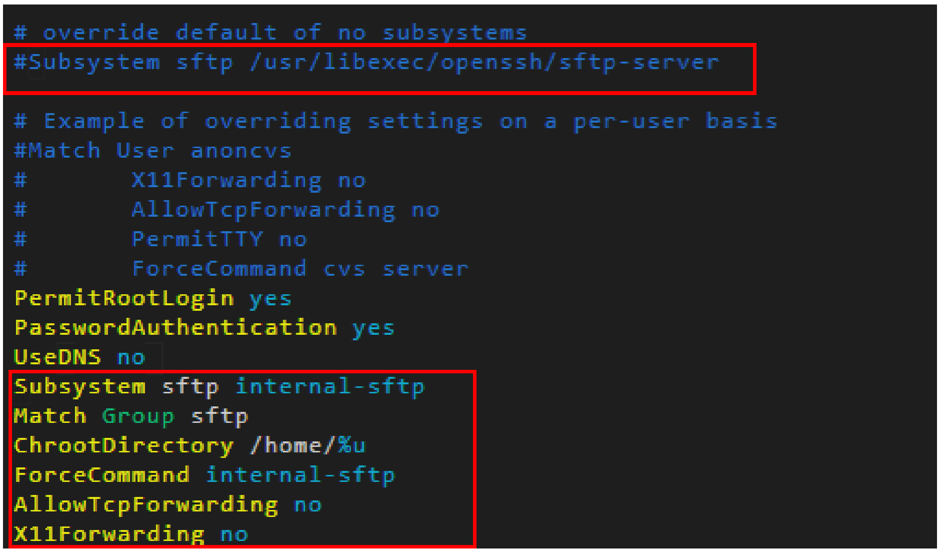
   Comment out the following information:

```
#Subsystem sftp /usr/libexec/openssh/sftp-server
```

   Add the following information:

```
Subsystem sftp internal-sftp
Match Group sftp
ChrootDirectory /home/%u
ForceCommand internal-sftp
AllowTcpForwarding no
X11Forwarding no
```

Figure 15-8 sshd_config file with the added information



```
# override default of no subsystems
#Subsystem sftp /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
PermitRootLogin yes
PasswordAuthentication yes
UseDNS no
Subsystem sftp internal-sftp
Match Group sftp
ChrootDirectory /home/%u
ForceCommand internal-sftp
AllowTcpForwarding no
X11Forwarding no
```

7. Run the following command to restart the ECS:

   service sshd restart

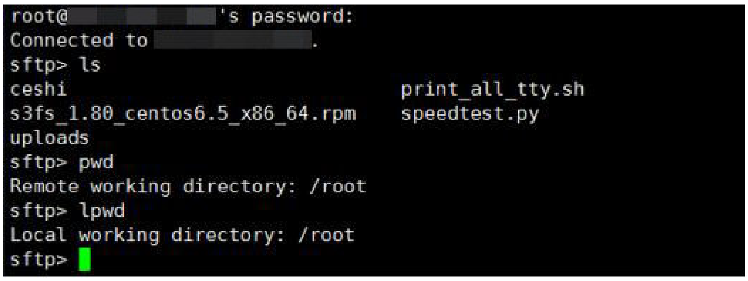
   Alternatively, run the following command to restart sshd:

   systemctl restart sshd

8. Run the following command on the local computer to set up the connection:

   sftp root@*IP address*

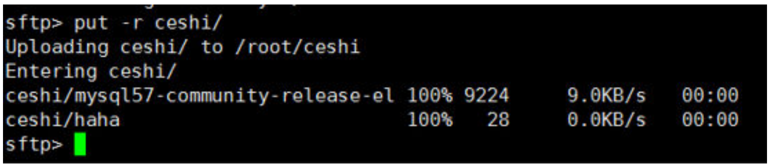
9. Run the **sftp** command to check the connection.

   ```
   root@[redacted]'s password:
   Connected to [redacted].
   sftp> ls
   ceshi                              print_all_tty.sh
   s3fs_1.80_centos6.5_x86_64.rpm     speedtest.py
   uploads
   sftp> pwd
   Remote working directory: /root
   sftp> lpwd
   Local working directory: /root
   sftp> 
   ```

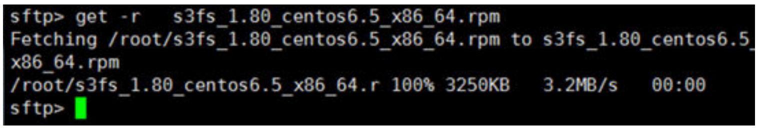
10. Transfer files or folders.

    To upload files or folders, run the **put -r** command.

    ```
    sftp> put -r ceshi/
    Uploading ceshi/ to /root/ceshi
    Entering ceshi/
    ceshi/mysql57-community-release-el 100% 9224     9.0KB/s   00:00
    ceshi/haha                         100%   28     0.0KB/s   00:00
    sftp> 
    ```

    To download files or folders, run the **get -r** command.

    ```
    sftp> get -r   s3fs_1.80_centos6.5_x86_64.rpm
    Fetching /root/s3fs_1.80_centos6.5_x86_64.rpm to s3fs_1.80_centos6.5_
    x86_64.rpm
    /root/s3fs_1.80_centos6.5_x86_64.r 100% 3250KB   3.2MB/s   00:00
    sftp> 
    ```

15.8 How Can I Use FTP to Transfer Files from a Local Windows Computer to a Windows or Linux ECS?

Scenarios

You want to use FTP to transfer files from a local Windows computer to an ECS.

Prerequisites

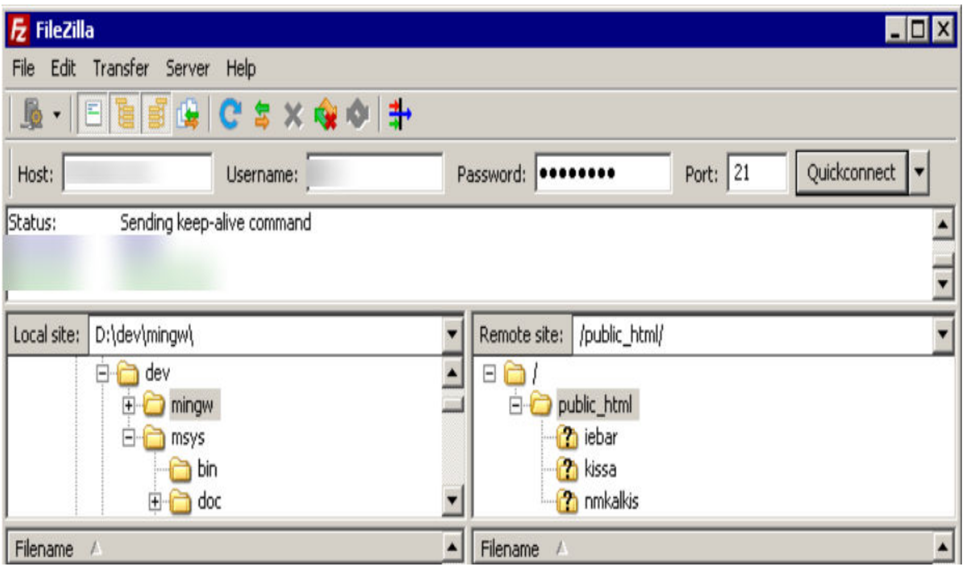
- An EIP has been bound to the ECS and access to TCP port 21 is allowed in the inbound direction of the security group to which the ECS belongs.
- You have enabled FTP on the target ECS. If you have not enabled FTP, check the following links to know how to set up an FTP site:
  - If the target ECS runs Windows, see **Setting Up an FTP Site (Windows)**.
  - If the target ECS runs Linux, see **Setting Up an FTP Site (Linux)**.

Procedure

1. **Download FileZilla** and install it on the local Windows computer.
2. On the local Windows computer, open FileZilla, enter the information about the target ECS, and click **Quickconnect**.
   - **Host**: EIP bound to an ECS

  - **Username**: username set when the FTP site was set up
  - **Password**: password of the username
  - **Port**: FTP access port, which is port 21 by default

Figure 15-9 Setting connection parameters



Status: Sending keep-alive command

3. Drag files from the local computer on the left to the target ECS on the right to transfer them.

15.9 How Can I Use FTP to Transfer Files Between a Local Linux Computer and a Linux ECS?

Scenarios

You want to use FTP on a local Linux computer to transfer files between the computer and a Linux ECS.

Prerequisites

You have enabled FTP on the target ECS. If you have not enabled FTP, check the following links to know how to set up an FTP site:

- An EIP has been bound to the ECS and access to TCP port 21 is allowed in the inbound direction of the security group to which the ECS belongs.
- You have enabled FTP on the target ECS. If you have not enabled FTP, check the following links to know how to set up an FTP site:
  - If the target ECS runs Windows, see **Setting Up an FTP Site (Windows)**.
  - If the target ECS runs Linux, see **Setting Up an FTP Site (Linux)**.

Procedure

1. Install FTP on the local Linux computer.

   Take CentOS 7.6 as an example. Run the following command to install FTP:

yum -y install ftp

2. Run the following command to access the ECS:

   ftp *EIP bound to the ECS*

   Enter the username and password as prompted for login.

   - **Uploading files**

     Run the following command to upload local files to the ECS:

     put *Path in which files are stored on the local computer*

     For example, to upload the **/home/test.txt** file on the local Linux computer to the ECS, run the following command:

     put /home/test.txt

   - **Downloading files**

     Run the following command to download files on the ECS to the local computer:

     get *Path in which the files are stored on the ECS Path in which the files are to be stored on the local computer*

     For example, to download the **test.txt** file on the ECS to the local Linux computer, run the following command:

     get /home/test.txt

15.10 How Can I Transfer Data Between a Local Computer and a Windows ECS?

Method 1: Install a Data Transfer Tool

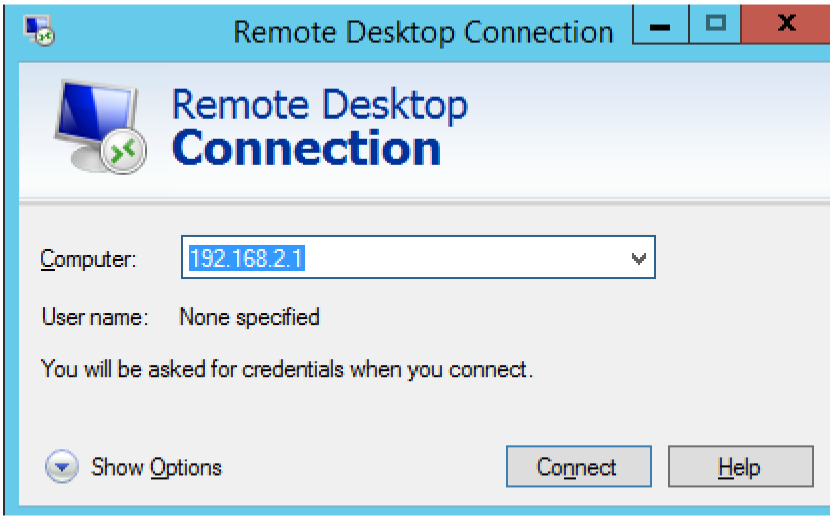
Install a data transfer tool, such as FileZilla on both the local computer and the Windows ECS to transmit data.

Method 2: Configure Local Disk Mapping

Use MSTSC to transfer data. This method does not support resumable transmission. Do not use this method to transfer large files. If you want to transfer a large file, use FTP.

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

Figure 15-10 Remote Desktop Connection



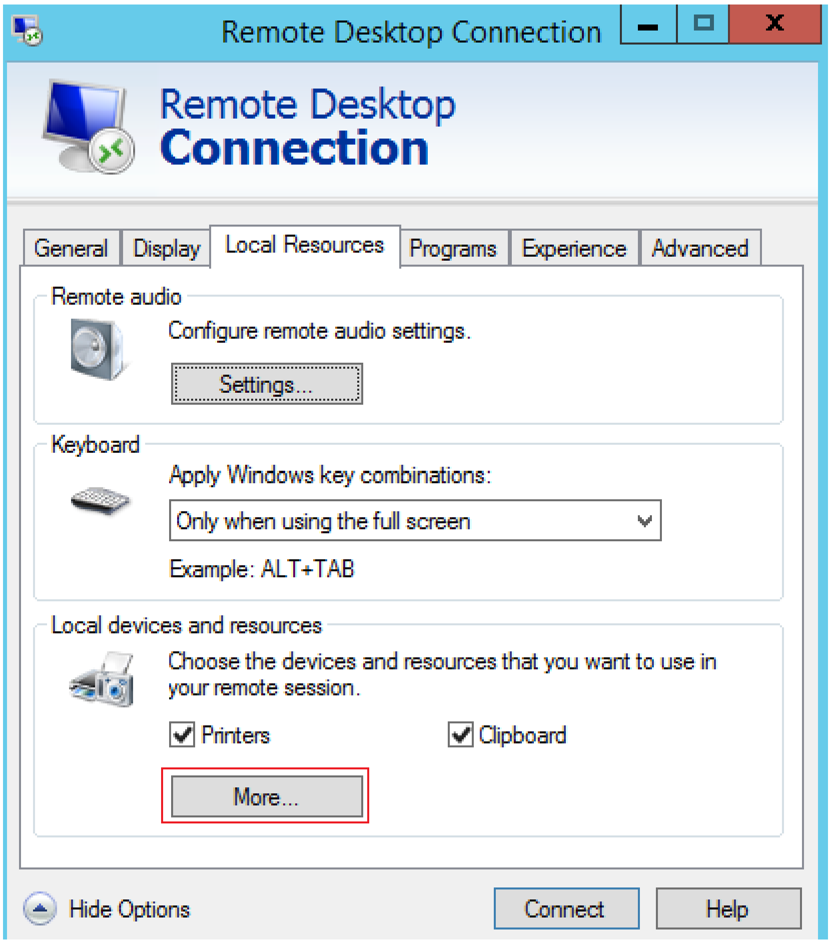
Computer: 192.168.2.1

User name: None specified

You will be asked for credentials when you connect.

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

Figure 15-11 Local Resources



Configure remote audio settings.

Apply Windows key combinations: Only when using the full screen

Example: ALT+TAB

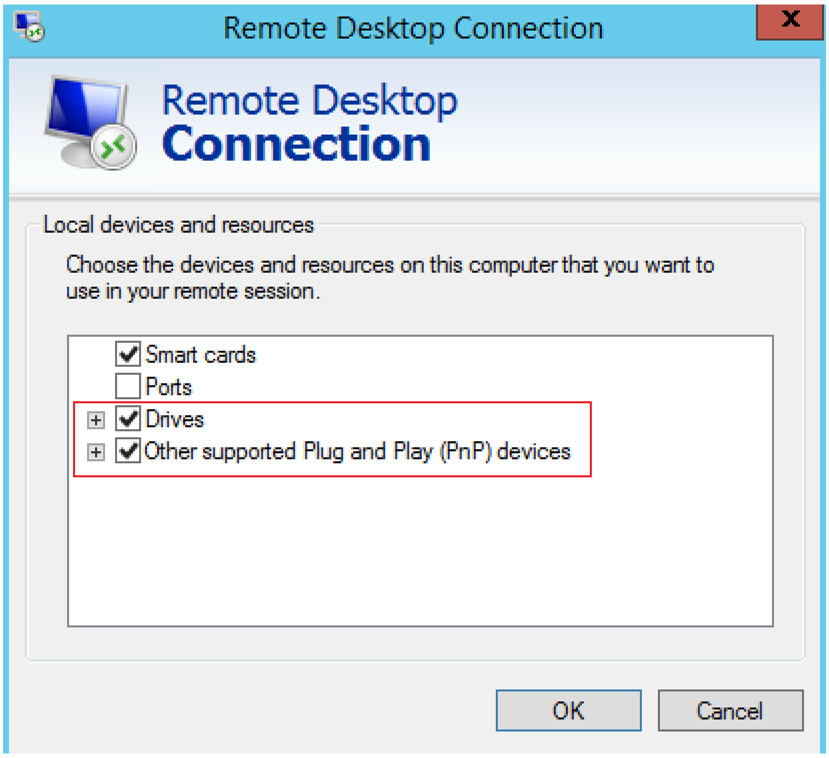
Choose the devices and resources that you want to use in your remote session.

☑ Printers ☑ Clipboard

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

   If you want to map only certain disks on the local computer to the Windows ECS, expand **Drives** and select the desired ones.

   Figure 15-12 Local devices and resources

   Remote Desktop Connection

   Remote Desktop Connection

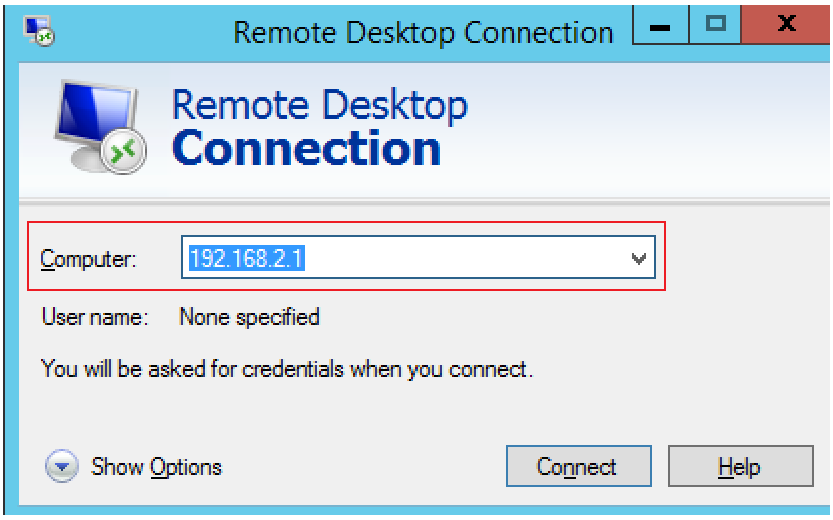
   Local devices and resources

   Choose the devices and resources on this computer that you want to use in your remote session.

   ☑ Smart cards
   ☐ Ports
   ☑ Drives
   ☑ Other supported Plug and Play (PnP) devices

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

   Figure 15-13 Connecting a remote desktop to the Windows ECS

   Remote Desktop Connection

   Remote Desktop Connection

   Computer: 192.168.2.1

   User name: None specified

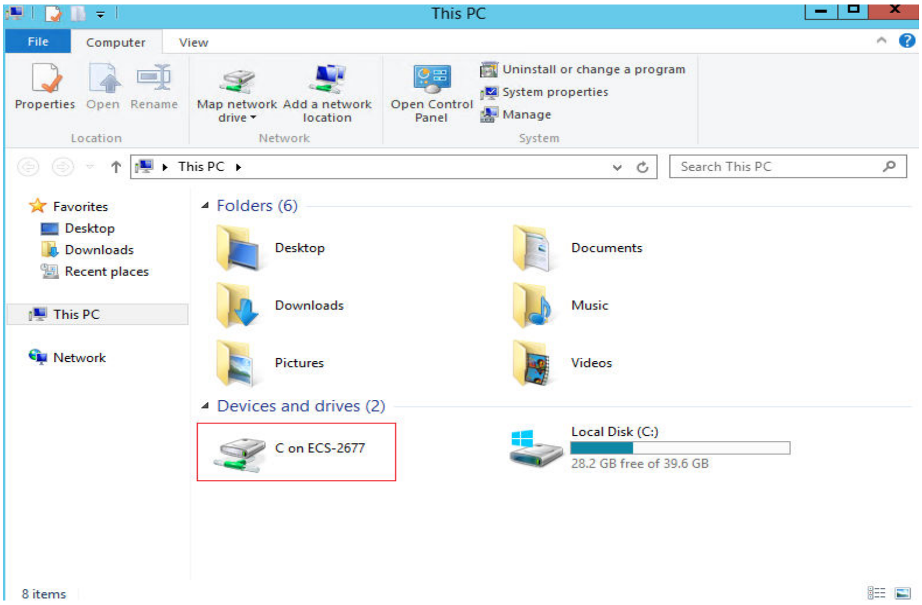
   You will be asked for credentials when you connect.

8. Click **Connect**.

   Log in to the Windows ECS.

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

Figure 15-14 Viewing disks



Method 3: Set Up an FTP Site

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

15.11 What Should I Do If the Connection Between the Client and the Server Times Out When I Upload a File Using FTP?

Symptom

When I attempted to access the server from the client to upload a file using FTP, the connection timed out.

Constraints

The operations described in this section apply to FTP on local Windows only.

Possible Causes

Data is intercepted by the firewall or security group on the server.

Solution

1. Check the firewall settings on the server.
2. Disable the firewall or add desired rules to the security group.

15.12 What Should I Do If Writing Data Failed When I Upload a File Using FTP?

Symptom

When I attempted to upload a file using FTP, writing data failed. As a result, the file transfer failed.

Constraints

The operations described in this section apply to FTP on Windows ECSs only.

Possible Causes

When NAT is enabled on the FTP server, the FTP client must connect to the FTP server in passive mode. In such a case, the public IP address (EIP) of the server cannot be accessed from the router. You need to add the EIP to the public IP address list on the server. Additionally, set the port range to limit the number of ports with data forwarded by the router.

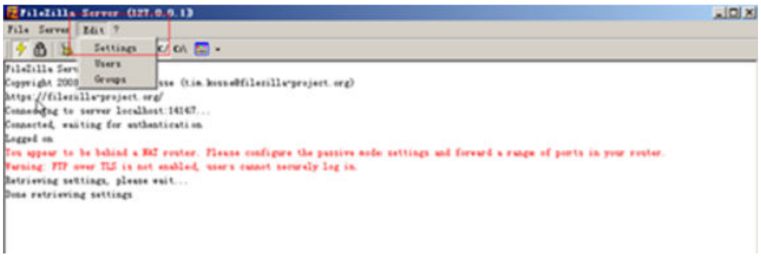
Solution

The EIP must be associated with the private IP address using NAT, so the server must be configured accordingly.

1. Set the public IP address of the server.

   Choose **Edit** > **Settings**.

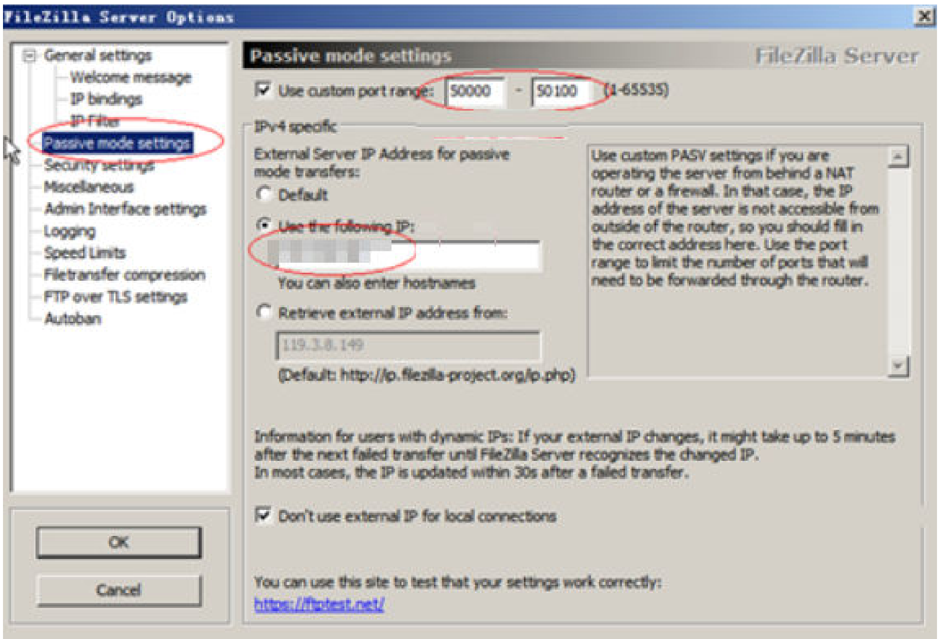
   Figure 15-15 Setting the public IP address

```
FileZilla Serv
Copyright 200                  se (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
You appear to be behind a NAT router. Please configure the passive mode settings and forward a range of ports in your router.
Warning: FTP over TLS is not enabled, users cannot securely log in.
Retrieving settings, please wait...
Done retrieving settings
```

2. Choose **Passive mode settings**, set the port range (for example, 50000-50100) for transmitting data, and enter the target EIP.

Figure 15-16 Setting the range of ports for data transmission



☑ Use custom port range: 50000 - 50100 (1-65535)

IPv4 specific

External Server IP Address for passive mode transfers:

○ Default

● Use the following IP:

[redacted]

You can also enter hostnames

○ Retrieve external IP address from:

119.3.8.149

(Default: http://ip.filezilla-project.org/ip.php)

Use custom PASV settings if you are operating the server from behind a NAT router or a firewall. In that case, the IP address of the server is not accessible from outside of the router, so you should fill in the correct address here. Use the port range to limit the number of ports that will need to be forwarded through the router.

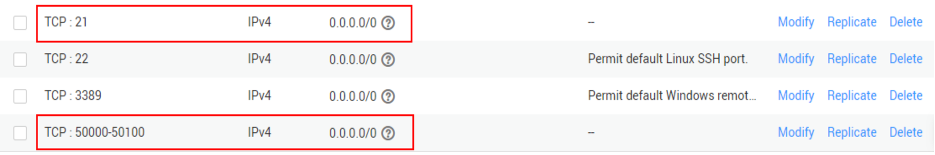
Information for users with dynamic IPs: If your external IP changes, it might take up to 5 minutes after the next failed transfer until FileZilla Server recognizes the changed IP.
In most cases, the IP is updated within 30s after a failed transfer.

☑ Don't use external IP for local connections

You can use this site to test that your settings work correctly:
https://ftptest.net/

3. Click **OK**.
4. Allow traffic on TCP ports 50000-50100 and 21 in the security group in the inbound direction.

Figure 15-17 Enabling ports 50000-50100 and 21



☐	TCP : 21	IPv4	0.0.0.0/0 ⓘ	--	Modify Replicate Delete
☐	TCP : 22	IPv4	0.0.0.0/0 ⓘ	Permit default Linux SSH port.	Modify Replicate Delete
☐	TCP : 3389	IPv4	0.0.0.0/0 ⓘ	Permit default Windows remot...	Modify Replicate Delete
☐	TCP : 50000-50100	IPv4	0.0.0.0/0 ⓘ	--	Modify Replicate Delete

5. Test the connection on the client.

15.13 Why Does Internet Access to an ECS Deployed with FTP Fail?

Symptom

- You cannot access a Windows ECS with FTP deployed by using an EIP.
- The FTP client cannot access the FTP server, and the connection times out.
- It takes a lot of time to upload files.

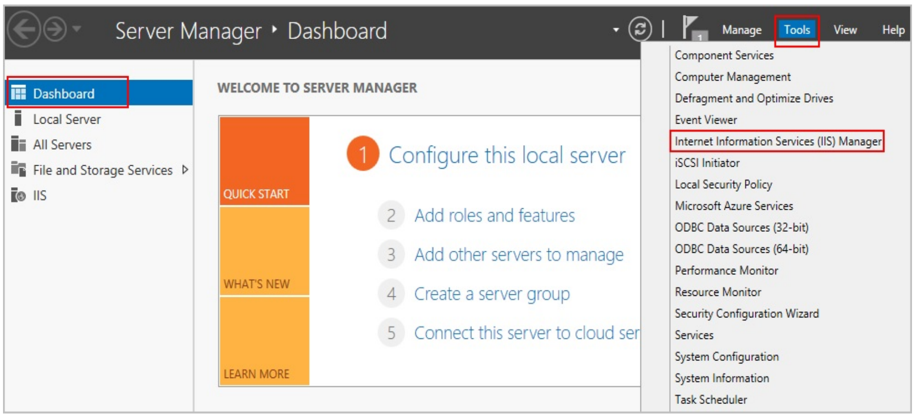
Possible Causes

- The security group associated with the target ECS denies inbound traffic from the Internet.
- The firewall of the ECS blocks the FTP process.

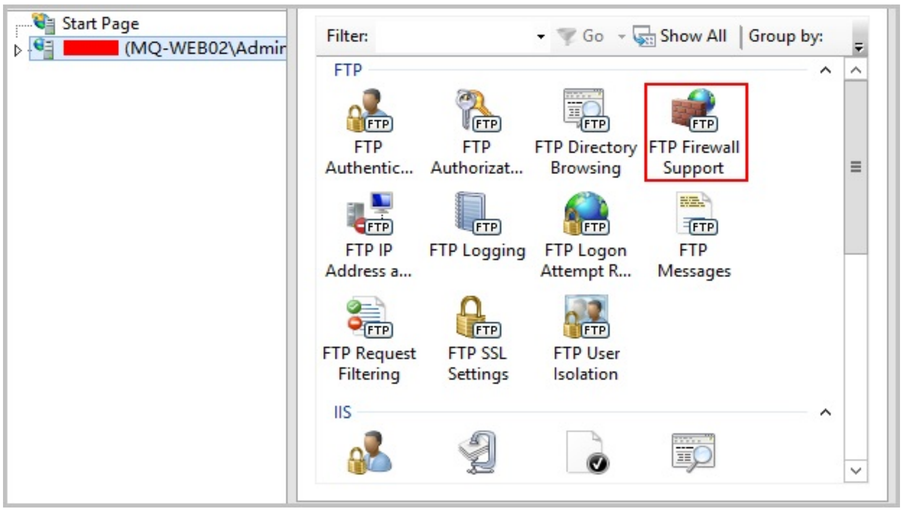
Enabling FTP Firewall Support

To allow a Huawei Cloud server to access an FTP server deployed on an ECS using an EIP, the FTP server must work in passive mode. In this case, enable FTP firewall support.

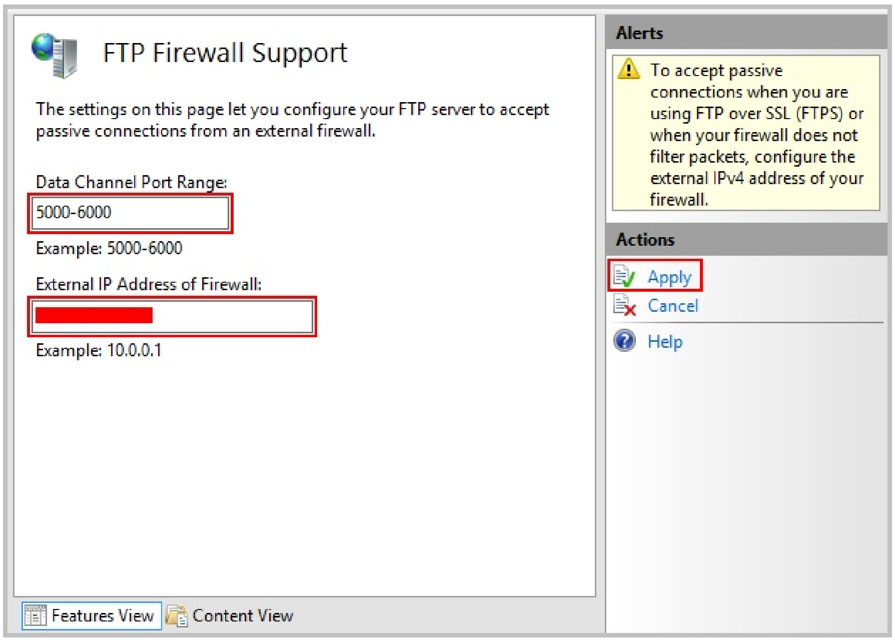
1. Log in to the **management console** and then log in to the ECS using **VNC**.
2. Choose **Start** > **Server Manager**.
3. In **Server Manager**, choose **Dashboard** > **Tools** > **Internet Information Services (IIS) Manager**.



4. Double-click **FTP Firewall Support**.



5. Set parameters and click **Apply**.
   - **Data Channel Port Range**: specifies the range of ports used for passive connections. The port range is 1025-65535. Configure this parameter based on site requirements.
   - **External IP Address of Firewall**: specifies the public IP address of the ECS.



FTP Firewall Support

The settings on this page let you configure your FTP server to accept passive connections from an external firewall.

Data Channel Port Range: 5000-6000

Example: 5000-6000

External IP Address of Firewall: [redacted]

Example: 10.0.0.1

To accept passive connections when you are using FTP over SSL (FTPS) or when your firewall does not filter packets, configure the external IPv4 address of your firewall.

6. Restart the ECS for the firewall configuration to take effect.

Setting the Security Group and Firewall

After deploying FTP, add a rule to the target security group to allow access to the FTP port in the inbound direction.

After **enabling FTP firewall support**, allow access to the ports used by the FTP site and the data channel ports used by the FTP firewall in the security group.

By default, the firewall allows access to TCP port 21 for FTP. If another port is used, add an inbound rule that allows access to that port on the firewall.

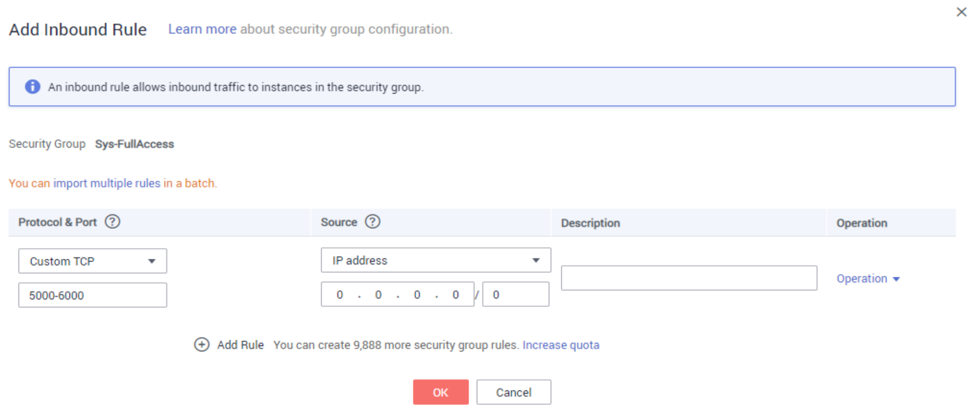
1. Log in to the **management console**.
2. Click in the upper left corner and select a region and project.
3. Under **Compute**, click **Elastic Cloud Server**.
4. On the **Elastic Cloud Server** page, click the name of the target ECS.

   The page providing details about the ECS is displayed.
5. Click the **Security Groups** tab and view security group rules.
6. Click the security group ID.

   The system automatically switches to the **Security Group** page.
7. On the **Inbound Rules** tab, click **Add Rule** and configure the access rule for the inbound direction.

   Set **Source** to the IP address segment containing the IP addresses allowed to access the ECS over the Internet.

   The valid port range that can be specified in **Enabling FTP Firewall Support** is 1025-65535. For example, the configured data port range is 5000-6000.



An inbound rule allows inbound traffic to instances in the security group.

Security Group Sys-FullAccess

You can import multiple rules in a batch.

Protocol & Port	Source	Description	Operation
Custom TCP 5000-6000	IP address 0 . 0 . 0 . 0 / 0		Operation

You can create 9,888 more security group rules.

NOTE

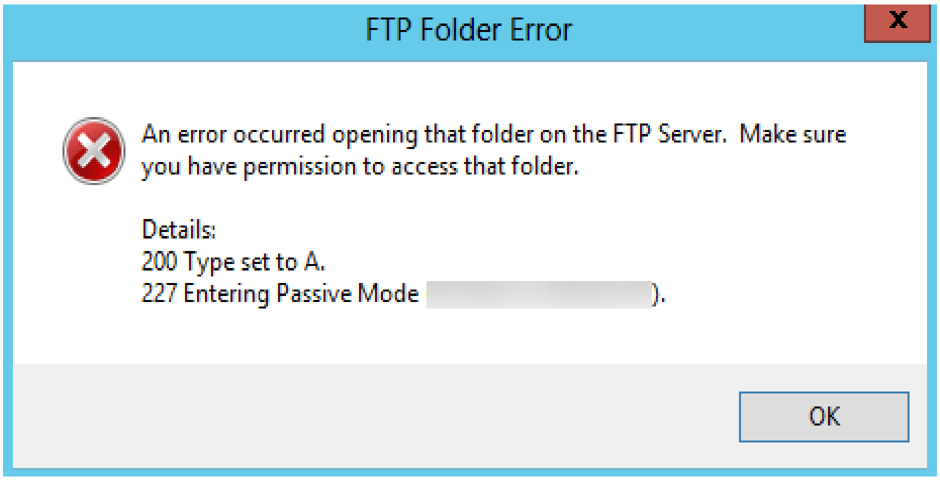
The default source IP address **0.0.0.0/0** indicates that all IP addresses can access ECSs in the security group.

15.14 Why Am I Seeing an FTP Folder Error When I Open a Folder on an FTP Server?

Symptom

An error occurs when you open a folder on an FTP server. The system displays a message asking you to check permissions.

Figure 15-18 FTP Folder Error



An error occurred opening that folder on the FTP Server. Make sure you have permission to access that folder.

Details:
200 Type set to A.
227 Entering Passive Mode [redacted]).

Possible Causes

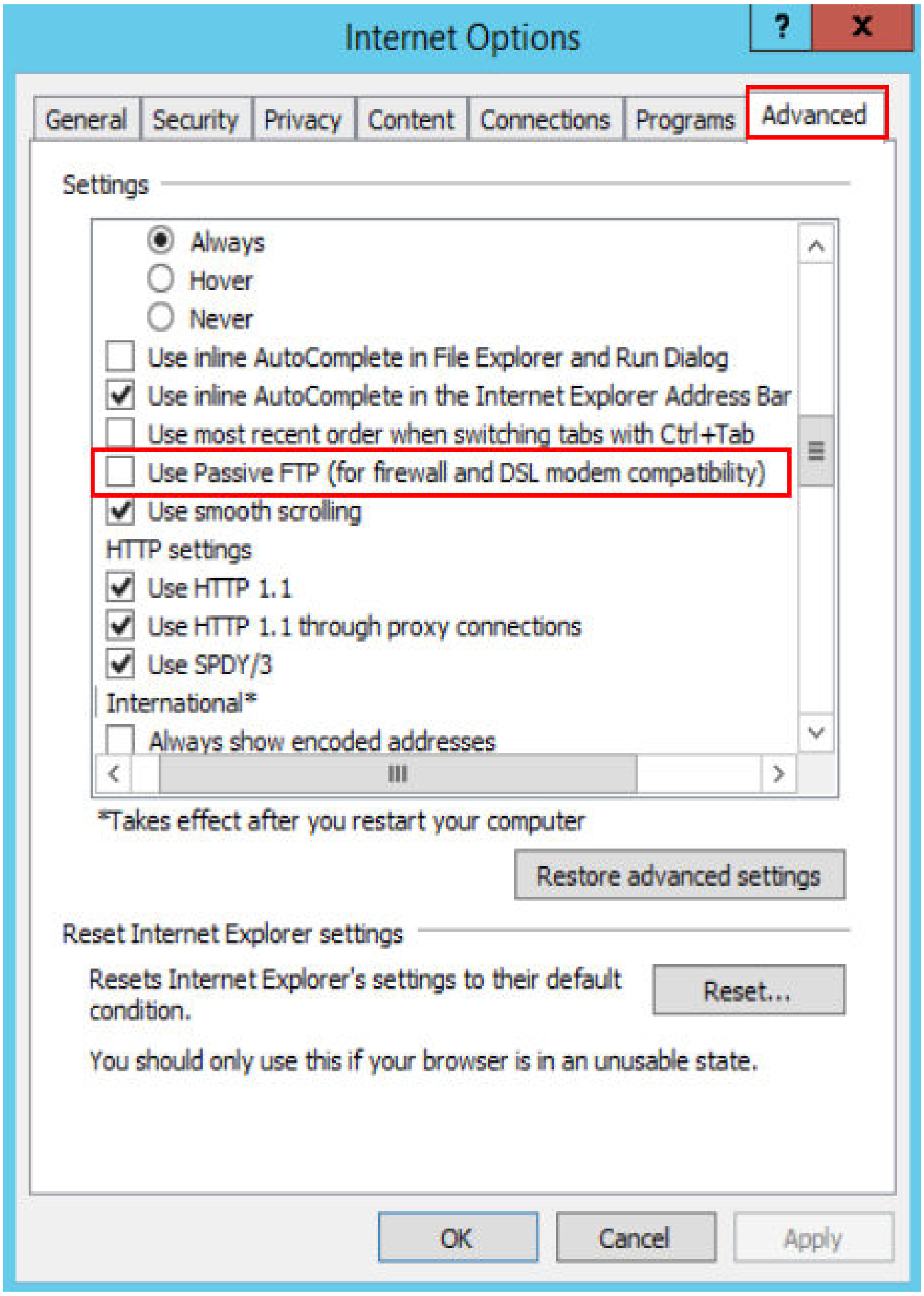
The FTP firewall configured for the browser does not allow you to open the folder.

Solution

The following uses Internet Explorer as an example.

1. Open the Internet Explorer and choose **Tools** > **Internet options**.
2. Click the **Advanced** tab.
3. Deselect **Use Passive FTP (for firewall and DSL modem compatibility)**.

Figure 15-19 Internet Options



Settings

● Always
○ Hover
○ Never
☐ Use inline AutoComplete in File Explorer and Run Dialog
☑ Use inline AutoComplete in the Internet Explorer Address Bar
☐ Use most recent order when switching tabs with Ctrl+Tab
☐ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP settings
☑ Use HTTP 1.1
☑ Use HTTP 1.1 through proxy connections
☑ Use SPDY/3
International*
☐ Always show encoded addresses

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

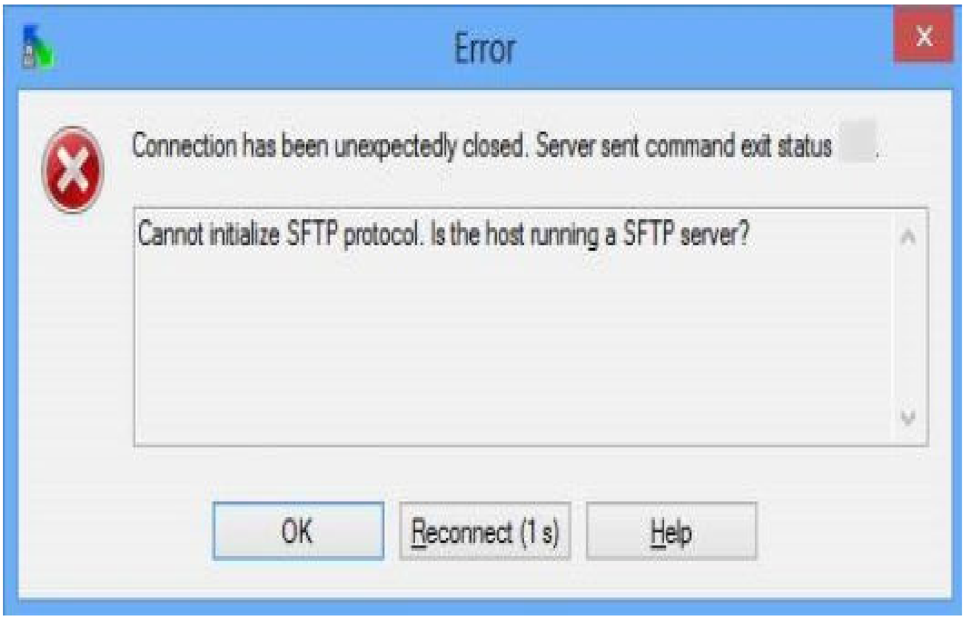
4. Click **OK**, restart Internet Explorer, and open the folder on the FTP server again.

15.15 Why Do I Fail to Connect to a Linux ECS Using WinSCP?

Symptom

Connecting to a Linux ECS using WinSCP fails, while using SSH tools like Xshell succeeds.

Figure 15-20 Connection error using WinSCP



Connection has been unexpectedly closed. Server sent command exit status [redacted].

Cannot initialize SFTP protocol. Is the host running a SFTP server?

Root Cause

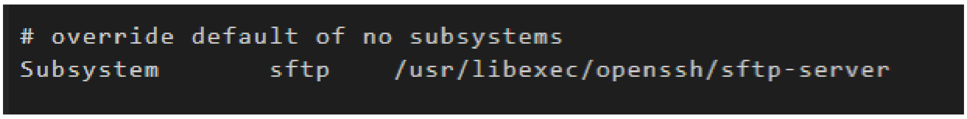
If you can connect to a Linux ECS using SSH tools, the SSH tools run properly. Check the SFTP configuration file because WinSCP allows you to connect your Linux ECS via SFTP protocol.

Run the following command to view the **/etc/ssh/sshd_config** file:

vi /etc/ssh/sshd_config

Check the SFTP configuration and the configuration file is **/usr/libexec/openssh/sftp-server**.

Figure 15-21 SFTP configuration file



```
# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server
```

If the SFTP configuration file does not exist or the file permission is not 755, connecting to a Linux ECS using WinSCP will fail.

Solution

- If the SFTP configuration file does not exist, you can transfer the file from an ECS that runs properly to your Linux ECS using SCP or other file transfer tools.
- If the file permission is not 755, you can run the following command to change the file permission to 755:

  ```
  chmod 755 -R /usr/libexec/openssh/sftp-server
  ```

16 ECS Failure

16.1 How Do I Handle Error Messages Displayed on the Management Console?

Symptom

This section helps you resolve the following issues:

- An error message was displayed on the management console after you performed ECS-related operations.
- An error code was displayed after you used an ECS API (see *Elastic Cloud Server API Reference*).

Background

After you perform ECS-related operations on the management console, the system displays the request status on the **Elastic Cloud Server** page. You can determine the request execution status based on the information displayed in the request status.

- If the operation request is executed, the system automatically clears the task prompt.
- If an error occurs during the request execution, the system displays an error code and its description in the taskbar.

Solution

If an error occurs, check the error code and perform the corresponding operations listed in **Table 16-1**.

Table 16-1 Error codes and solution suggestions

Error Code	Message Displayed on the Management Console	Solution Suggestion for Pay-per-Use ECSs	Solution Suggestion for Yearly/Monthly ECSs
Ecs.0000	Request error. Try again later or contact customer service.	Adjust the request structure as directed in *Elastic Cloud Server API Reference*.	Adjust the request structure as directed in *Elastic Cloud Server API Reference*.
Ecs.0001	The maximum number of ECSs or EVS disks has been reached. Contact customer service and request a quota increase.	Contact customer service to apply for an increased ECS quota. **NOTE** When applying for increasing your ECS quota, first determine the number of target ECSs, CPU cores (vCPUs), and memory capacity (RAM) required.	Submit a service ticket to apply for an increased ECS quota. After the submission, contact customer service for troubleshooting. **NOTE** When applying for increasing your ECS quota, first determine the number of target ECSs, CPU cores (vCPUs), and memory capacity (RAM) required.
Ecs.0005	System error. Try again later or contact customer service.	Adjust the request structure as directed in *Elastic Cloud Server API Reference*.	Adjust the request structure as directed in *Elastic Cloud Server API Reference*.
Ecs.0006	Invalid parameters.	If your selected ECS configuration has not been released, change the configuration and create the ECS again.	If your selected ECS configuration has not been released, change the configuration and create the ECS again.
Ecs.0010	The private IP address is in use. Select an available IP address and create the ECS again.	Use idle IP addresses to purchase your ECSs.	Contact customer service to cancel the order and use an idle IP address to purchase your ECS.

Error Code	Message Displayed on the Management Console	Solution Suggestion for Pay-per-Use ECSs	Solution Suggestion for Yearly/Monthly ECSs
Ecs.0011	Invalid password. Change the password to make it meet the password complexity requirements, and perform the required operation again.	Input a password that meets password complexity requirements.	Contact customer service to cancel the order, input a password that meets password complexity requirements, and perform the request again.
Ecs.0012	The number of IP addresses in the subnet is insufficient. Release IP addresses in the subnet or select another subnet, and create the ECS again.	Obtain more idle IP addresses on the target subnet or use a new subnet for purchasing ECSs.	Obtain more idle IP addresses on the target subnet and contact customer service for troubleshooting. Alternatively, contact customer service to cancel the order and use a new subnet for purchasing ECSs.
Ecs.0013	Insufficient EIP quota. Contact customer service and request an EIP quota increase.	Contact customer service to apply for an increased EIP quota.	Submit a service ticket to apply for an increased EIP quota and contact customer service for troubleshooting.
Ecs.0015	This disk type is not supported by the ECS.	Select a supported EVS disk and attach it to the ECS.	Select a supported EVS disk and attach it to the ECS.
Ecs.0100	The ECS status does not meet requirements. Change the ECS status to the desired one and try again.	Change to the desired ECS status and try again.	Change the ECS status to the required status and contact customer service for troubleshooting.
Ecs.0104	Insufficient number of ECS slots for attaching disks.	Detach an EVS disk from the ECS before attaching a new EVS disk.	Detach an EVS disk from the ECS before attaching a new EVS disk.

Error Code	Message Displayed on the Management Console	Solution Suggestion for Pay-per-Use ECSs	Solution Suggestion for Yearly/Monthly ECSs
Ecs.0105	No system disk found.	Reattach the EVS system disk to the ECS and perform the desired operation again.	Reattach the EVS system disk to the ECS and contact customer service for troubleshooting.
Ecs.0107	The number of shared disks to be attached to an ECS exceeds the maximum limit.	Detach an EVS disk from the ECS before attaching a new EVS disk.	Detach an EVS disk from the ECS before attaching a new EVS disk.
Ecs.0509	This operation is not allowed on a yearly/monthly system disk. Select a pay-per-use system disk and perform the required operation again.	N/A	Change the ECS billing mode to pay-per-use and perform the desired operation again.
Ecs.0510	Yearly/Monthly ECSs do not support OS changing.	N/A	Change the ECS billing mode to pay-per-use and perform the desired operation again.

16.2 How Can I Recover a Windows ECS with an Abnormal Virtualization Driver?

Background

An error occurs in the virtualization driver on a Windows ECS because of improper running of Tools. To ensure proper ECS running, handle this issue by following the instructions provided in this section.

Symptom

The virtualization driver of an ECS became abnormal and this affected the data security, availability, and performance of the ECS.

The impact of this issue is as follows:

1. The file system may be damaged.

   When you stop or restart such an ECS on the management console, the ECS will be forcibly stopped or restarted due to the lack of the virtualization driver Tools.

2. Services on the ECS may become unavailable

   The affected ECS cannot be hot migrated between physical servers. If the host accommodating such an ECS becomes faulty or the hardware of the host is maintained, the ECS cannot be migrated to another host, affecting service high availability.

3. The network and storage performance of the ECS deteriorates.

   The virtualization driver can improve the ECS network and storage performance. When the virtualization driver becomes abnormal, the network and storage performance will deteriorate.

Scenarios

- Scenario 1

  Tools is not installed on the Windows ECS.

- Scenario 2

  Tools has been uninstalled from the ECS.

Procedure

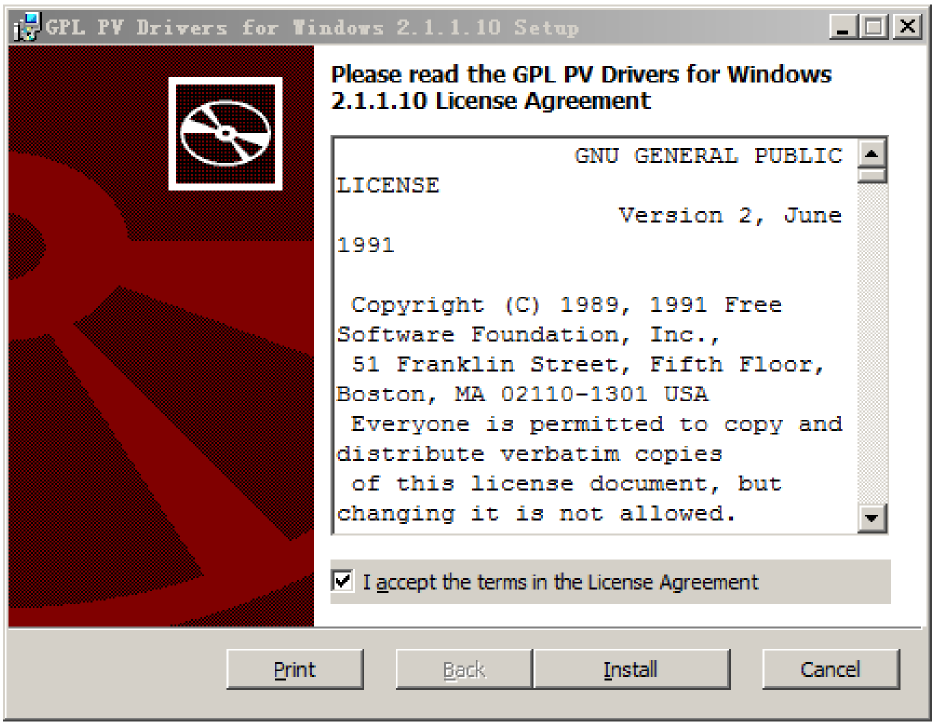
To install Tools on the Windows ECS, do as follows:

1. Obtain the Tools installation package **pvdriver-windows.zip**.

   To download the installation package, log in at **https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-windows.zip**.

2. Decompress the software package and double-click **setup.exe** to start the installation.

Figure 16-1 Installing the virtualization driver



Please read the GPL PV Drivers for Windows 2.1.1.10 License Agreement

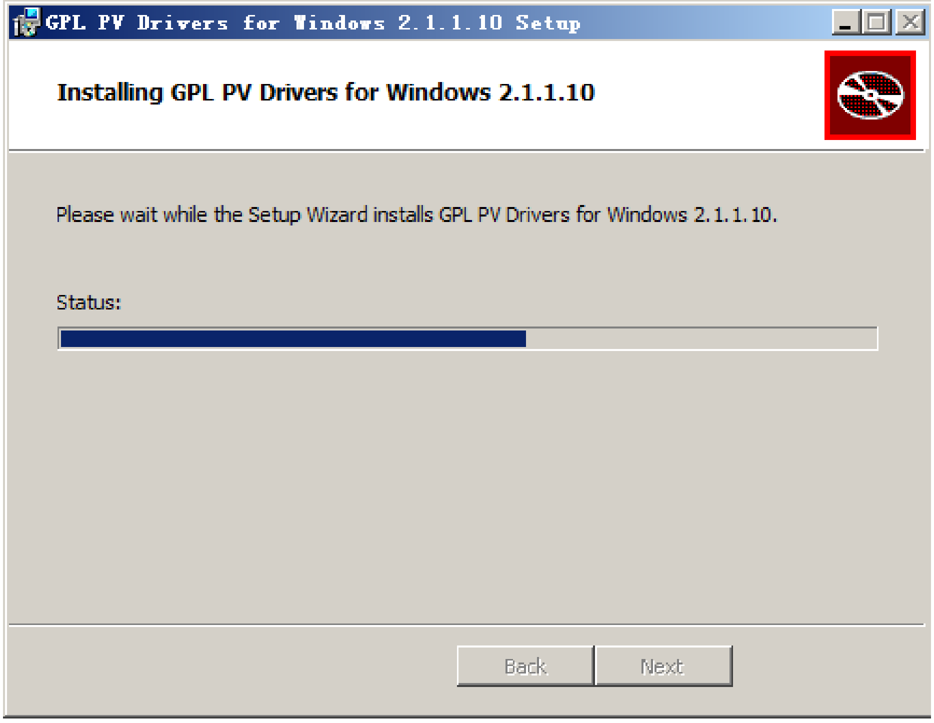
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

☑ I accept the terms in the License Agreement

3. Click **Next** and select "I accept the terms in the License Agreement".
4. Click **Install** to start the installation.

Figure 16-2 Installation progress



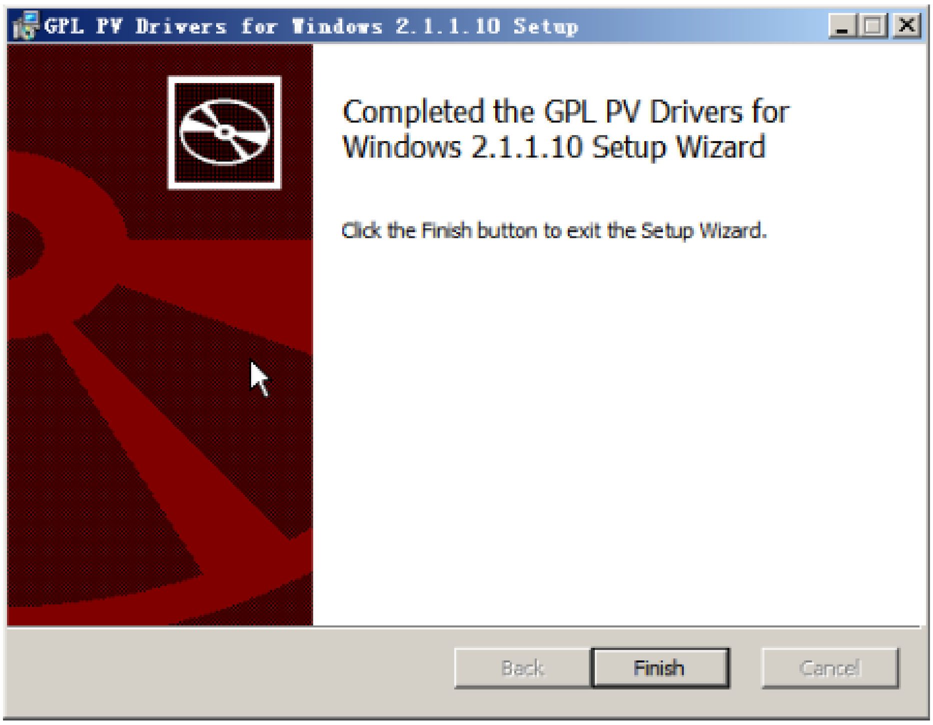
Installing GPL PV Drivers for Windows 2.1.1.10

Please wait while the Setup Wizard installs GPL PV Drivers for Windows 2.1.1.10.

Status:

5. Click **Finish** to complete the installation.

Figure 16-3 Installation completed

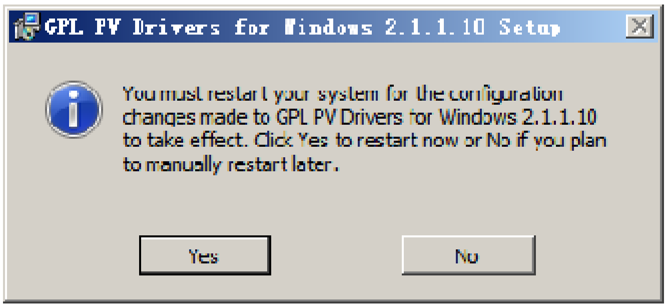

GPL PV Drivers for Windows 2.1.1.10 Setup

Completed the GPL PV Drivers for Windows 2.1.1.10 Setup Wizard

Click the Finish button to exit the Setup Wizard.

6. Restart the ECS, as shown in **Figure 16-4**.

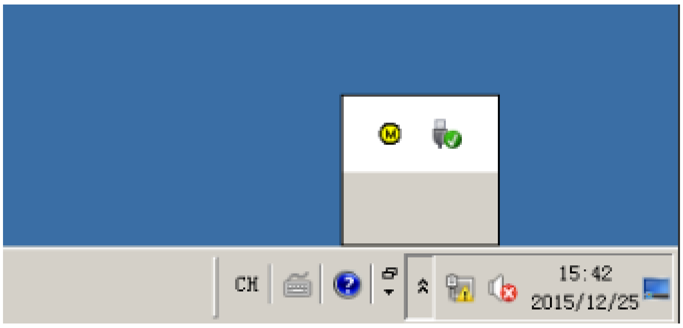
Figure 16-4 Determining whether to restart the ECS


GPL PV Drivers for Windows 2.1.1.10 Setup

You must restart your system for the configuration changes made to GPL PV Drivers for Windows 2.1.1.10 to take effect. Click Yes to restart now or No if you plan to manually restart later.

7. View the virtualization driver status in the bottom right corner of the ECS desktop. The yellow icon indicates that the virtualization driver is running properly.

Figure 16-5 Proper running status of the virtualization driver



16.3 What Should I Do If Emails Configured on an ECS Cannot Be Sent?

Solution

- For the emails sent using the browser:

  When you use a browser to log in to your mailbox, HTTP is used, and the default port number is 80. However, SMTP is used between email servers.

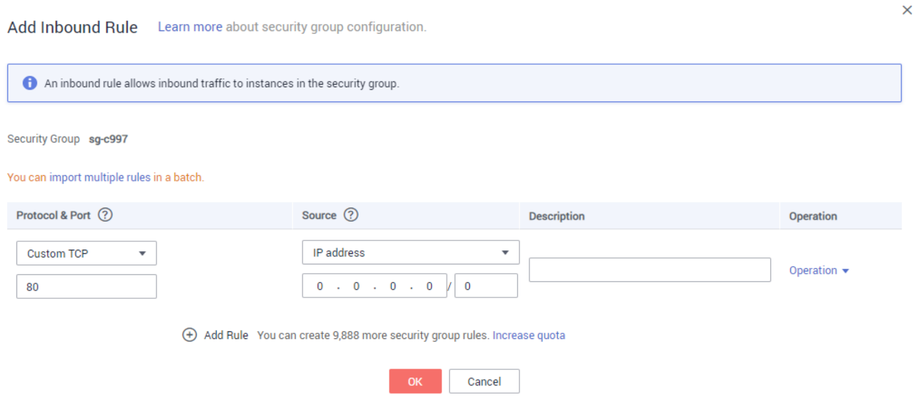
  If you use a browser to send emails, enable port 80 for TCP in the outbound direction.

  a. On the ECS details page, locate the security group and click the security group ID.

  b. On the **Security Group** page, click the **Outbound** tab and then **Add Rule**.

  c. In the dialog box that is displayed, set **Protocol/Application** to **TCP** and **Port** to **80**. Then, click **OK**.

  Figure 16-6 Adding port 80



Add Inbound Rule Learn more about security group configuration.

An inbound rule allows inbound traffic to instances in the security group.

Security Group sg-c997

You can import multiple rules in a batch.

Protocol & Port	Source	Description	Operation
Custom TCP 80	IP address 0 . 0 . 0 . 0 / 0		Operation

You can create 9,888 more security group rules. Increase quota

- For the emails sent and received through an email client:

  The protocols used on the receiving and transmitting ends are different.

  Protocol used on the transmitting end:

  SMTPS is used, and the port number is 465. Alternatively, SMTP is used, and the port number is 25.

  Port 465 is recommended. If port 25 is required, enable it. For details, see **Why Is Outbound Access on TCP Port 25 Blocked?**

  Protocol used on the receiving end: POP3 is used, and the port number is 110.

  For details, see steps **a** to **c**.

  NOTE

  Add an inbound rule with **Protocol** set to **TCP** and **Port** to **110**. Add an outbound rule with **Protocol** set to **TCP** and **Port** to **465** or **25**.

16.4 Why Is My Windows ECS Muted?

Symptom

You cannot play audio files on a Windows ECS that is remotely accessed using MSTSC.

Constraints

This section applies only to ECSs running Windows Server 2008 R2 or Windows Server 2016.

Possible Causes

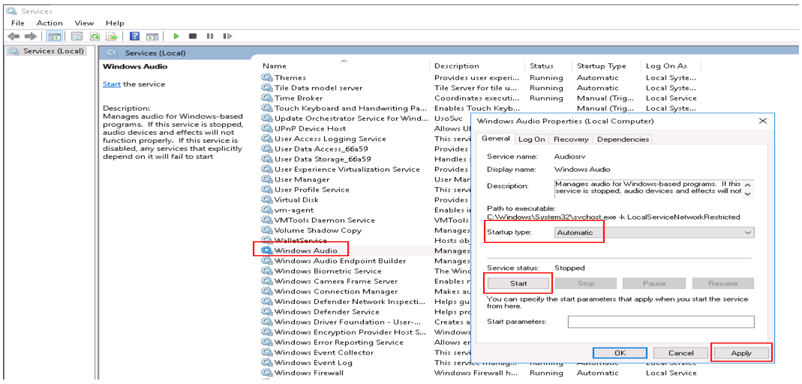
The audio function is disabled on Windows ECSs by default. As a result, audio files cannot be played on them. To enable the audio function, perform the operations described in this section.

Step 1: Enable Windows Audio

Enable Windows audio and set it to run automatically.

1. Start the **Run** dialog box.
2. Enter **services.msc** to access the service management console.
3. Find **Windows Audio** and set it as follows:
    - **Startup type**: **Automatic**
    - **Service status**: **Start**

    The following figure uses Windows Server 2012 as an example.



Windows Audio

Start the service

Description:
Manages audio for Windows-based programs. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start

Name	Description	Status	Startup Type	Log On As
Themes	Provides user experi...	Running	Automatic	Local Syste...
Tile Data model server	Tile Server for tile u...	Running	Automatic	Local Syste...
Time Broker	Coordinates executi...	Running	Manual (Trig...	Local Service
Touch Keyboard and Handwriting Pa...	Enables Touch Keyb...		Manual (Trig...	Local Syste...
Update Orchestrator Service for Wind...	UsoSvc			
UPnP Device Host	Allows UI			
User Access Logging Service	This servi			
User Data Access_66a59	Provides			
User Data Storage_66a59	Handles			
User Experience Virtualization Service	Provides			
User Manager	User Man			
User Profile Service	This servi			
Virtual Disk	Provides			
vm-agent	Enables i			
VMTools Daemon Service	VMTools			
Volume Shadow Copy	Manages			
WalletService	Hosts ob			
Windows Audio	Manages			
Windows Audio Endpoint Builder	Manages			
Windows Biometric Service	The Wind			
Windows Camera Frame Server	Enables r			
Windows Connection Manager	Makes au			
Windows Defender Network Inspecti...	Helps gu			
Windows Defender Service	Helps pro			
Windows Driver Foundation - User-...	Creates a			
Windows Encryption Provider Host S...	Windows			
Windows Error Reporting Service	Allows er			
Windows Event Collector	This servi			
Windows Event Log	This service manag...			
Windows Firewall	Windows Firewall h...	Running	Automatic	Local Service

Windows Audio Properties (Local Computer)

Service name: Audiosrv
Display name: Windows Audio
Description: Manages audio for Windows-based programs. If this service is stopped, audio devices and effects will not
Path to executable:
C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Startup type: Automatic
Service status: Stopped

You can specify the start parameters that apply when you start the service from here.
Start parameters:

4. Disable the remote connection.

Step 2: Enable Audio and Video Playback

The method of enabling audio and video playback varies depending on the ECS OS.

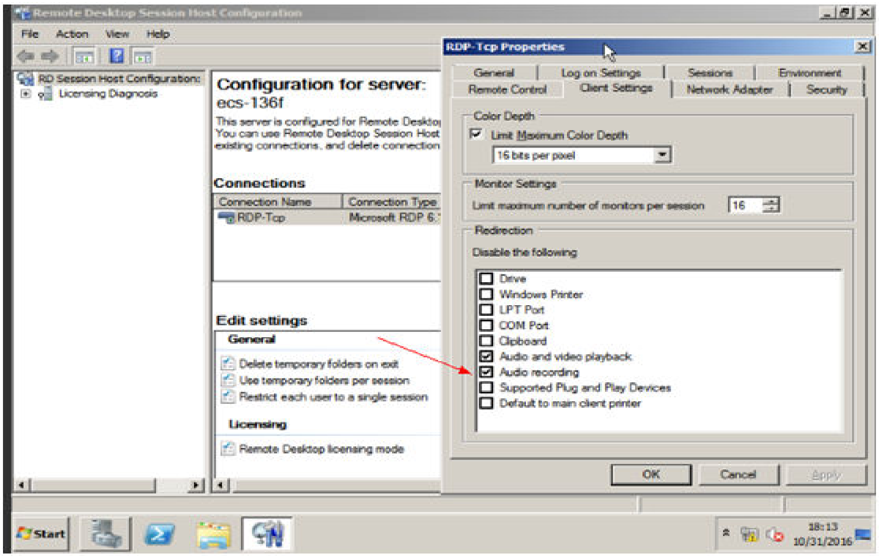
Windows Server 2008

Step 1 Enable RDP-TCP **Audio and video playback** and **Audio recording**.

1. Log in to the **Remote Desktop Session Host Configuration** management console.
    a. Choose **Start** > **Control Panel**.
    b. In the upper right corner of the page, choose **Category** for **View by**.
    c. Choose **System and Security** > **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**.
2. Deselect **Audio and video playback** and **Audio recording**.

    In the **Connections** pane, double-click **RDP-Tcp**. In the **RDP-Tcp Properties** dialog box, click the **Client Settings** tab and deselect **Audio and video playback** and **Audio recording**.

    Figure 16-7 Remote Desktop Session Host Configuration


Remote Desktop Session Host Configuration
File
Action
View
Help
RD Session Host Configuration:
Licensing Diagnosis
Configuration for server:
ecs-136f
This server is configured for Remote Deskto
You can use Remote Desktop Session Host
existing connections, and delete connection
Connections
Connection Name
Connection Type
RDP-Tcp
Microsoft RDP 6.
Edit settings
General
Delete temporary folders on exit
Use temporary folders per session
Restrict each user to a single session
Licensing
Remote Desktop licensing mode
RDP-Tcp Properties
General
Log on Settings
Sessions
Environment
Remote Control
Client Settings
Network Adapter
Security
Color Depth
Monitor Settings
Redirection
Disable the following
OK
Cancel
Apply
Start
18:13
10/31/2016

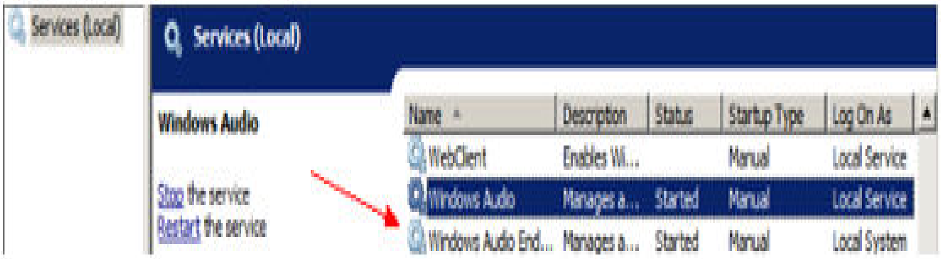
☑ Limit Maximum Color Depth
16 bits per pixel
Limit maximum number of monitors per session 16
☐ Drive
☐ Windows Printer
☐ LPT Port
☐ COM Port
☐ Clipboard
☑ Audio and video playback
☑ Audio recording
☐ Supported Plug and Play Devices
☐ Default to main client printer

3. Click **OK** to enable the audio function.

Step 2 Click **Send CtrlAltDel** to restart the ECS and log in to it.

Step 3 Enable the audio service.

Figure 16-8 Enabling the audio service



Name	Description	Status	Startup Type	Log On As
WebClient	Enables Wi...		Manual	Local Service
Windows Audio	Manages a...	Started	Manual	Local Service
Windows Audio End...	Manages a...	Started	Manual	Local System

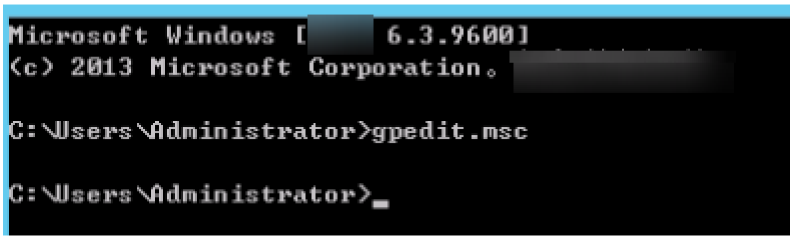
Step 4 Play an audio file to verify the service.

----End

Windows Server 2012

Step 1 Start the **Run** dialog box.

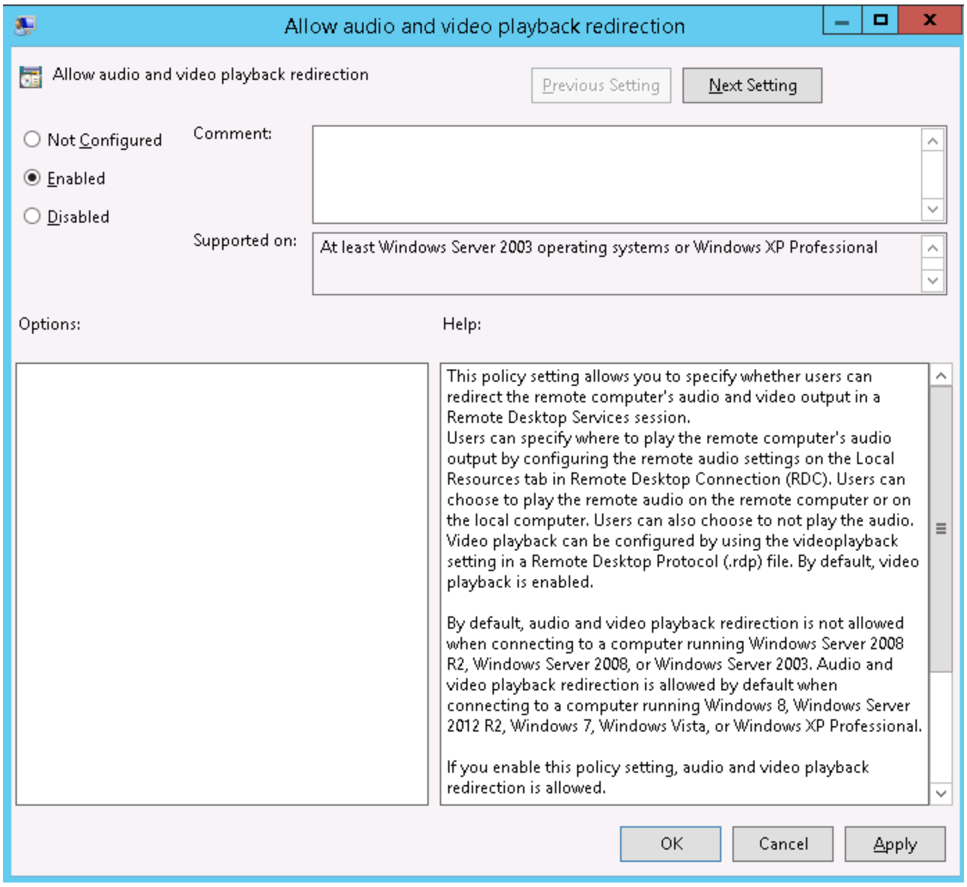
Step 2 Run the **gpedit.msc** command to start **Local Group Policy Editor**.



```
Microsoft Windows [[redacted] 6.3.9600]
(c) 2013 Microsoft Corporation。[redacted]

C:\Users\Administrator>gpedit.msc

C:\Users\Administrator>_
```

Step 3 Choose **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Device and Resource Redirection**. Then, enable **Allow audio and video playback redirection**.

Step 4 Select **Enabled** and click **Apply**.



Allow audio and video playback redirection
Allow audio and video playback redirection
Previous Setting
Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Help:

This policy setting allows you to specify whether users can redirect the remote computer's audio and video output in a Remote Desktop Services session.
Users can specify where to play the remote computer's audio output by configuring the remote audio settings on the Local Resources tab in Remote Desktop Connection (RDC). Users can choose to play the remote audio on the remote computer or on the local computer. Users can also choose to not play the audio. Video playback can be configured by using the videoplayback setting in a Remote Desktop Protocol (.rdp) file. By default, video playback is enabled.

By default, audio and video playback redirection is not allowed when connecting to a computer running Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003. Audio and video playback redirection is allowed by default when connecting to a computer running Windows 8, Windows Server 2012 R2, Windows 7, Windows Vista, or Windows XP Professional.

If you enable this policy setting, audio and video playback redirection is allowed.

Retain the default settings of MSTSC.

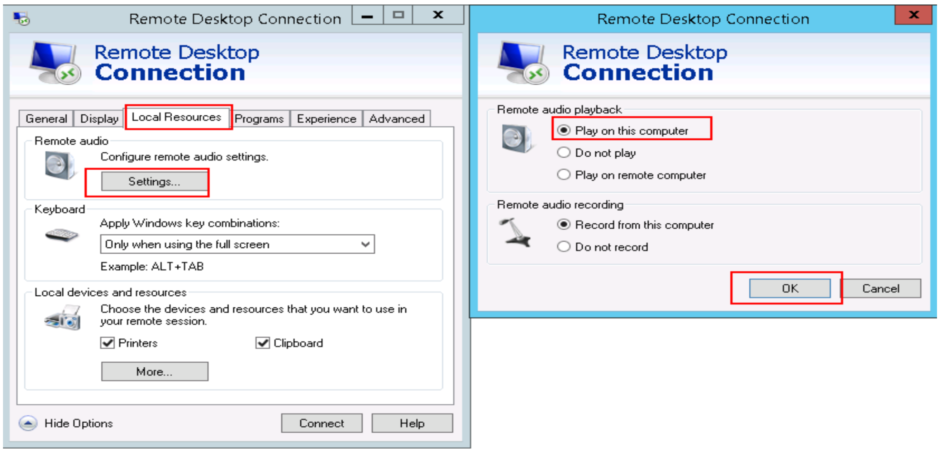
Step 5 Run the following command to update the group policy:

gpupdate

----End

Step 3: Configure Remote Audio Settings

Start the local remote desktop software MSTSC, choose **Options** > **Local Resources**, and click **Settings** in **Remote audio**. Then, select **Play on this computer** in **Remote audio playback** and click **OK**.


Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Programs
Experience
Advanced
Remote audio
Configure remote audio settings.
Settings...
Keyboard
Apply Windows key combinations:
Only when using the full screen
Example: ALT+TAB
Local devices and resources
Choose the devices and resources that you want to use in your remote session.
☑ Printers
☑ Clipboard
More...
Hide Options
Connect
Help
Remote Desktop Connection
Remote Desktop Connection
Remote audio playback
● Play on this computer
○ Do not play
○ Play on remote computer
Remote audio recording
● Record from this computer
○ Do not record
OK
Cancel

Log in to the ECS using MSTSC and check whether audio files can be played properly.

16.5 How Do I Change an ECS SID?

Microsoft identifies computers and users by security identifier (SID). The ECSs created using an image have the same SID. If such ECSs are required to join in a Windows domain, they must use different SIDs.

This section describes how to use SIDCHG to change an ECS SID.

To change SIDs in a batch, use a private image and follow the operations provided in **Running Sysprep**.

NOTE

Changing an ECS SID may lead to data loss or system damage, so back up ECS data before changing the SID.

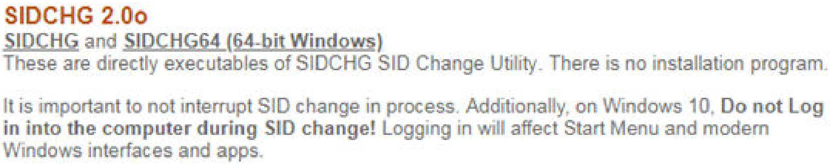
Procedure

1. Click **SIDCHG** to download it.

   NOTE

   For the server edition, download the 64-bit version.

   Figure 16-9 Downloading SIDCHG

   SIDCHG 2.0o
   SIDCHG and SIDCHG64 (64-bit Windows)
   These are directly executables of SIDCHG SID Change Utility. There is no installation program.

   It is important to not interrupt SID change in process. Additionally, on Windows 10, **Do not Log in into the computer during SID change!** Logging in will affect Start Menu and modern Windows interfaces and apps.

2. Run the following command to change the ECS SID:

sidchg64-2.0n.exe /R

NOTE

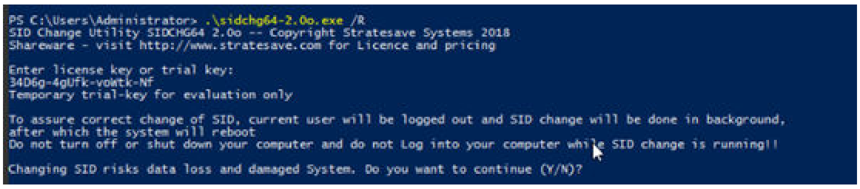
In the preceding command, **/R** indicates that the ECS will automatically restart after its SID is changed, and **/S** indicates that the ECS will not automatically restart.

3. Enter the trial key or license and press **Enter**.

   Obtain the latest trial key and learn how to use SIDCHG.

4. When the system displays a message asking you whether to continue, press **y**.

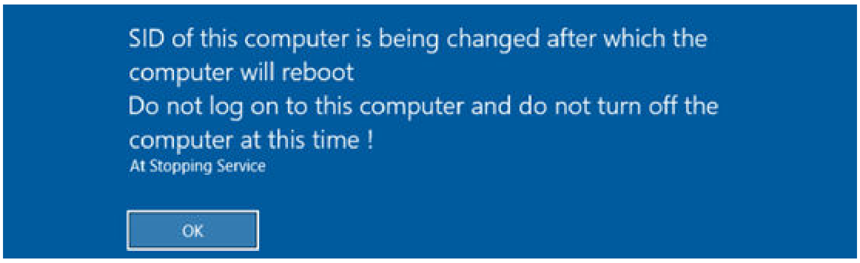
   Figure 16-10 Risk prompt

```
PS C:\Users\Administrator> .\sidchg64-2.0o.exe /R
SID Change Utility SIDCHG64 2.0o -- Copyright Stratesave Systems 2018
Shareware - visit http://www.stratesave.com for Licence and pricing

Enter license key or trial key:
34D6g-4gUfk-voWtk-Nf
Temporary trial-key for evaluation only

To assure correct change of SID, current user will be logged out and SID change will be done in background,
after which the system will reboot
Do not turn off or shut down your computer and do not Log into your computer while SID change is running!!

Changing SID risks data loss and damaged System. Do you want to continue (Y/N)?
```

5. Log in to the ECS again.

   Figure 16-11 Re-login

   SID of this computer is being changed after which the computer will reboot
   Do not log on to this computer and do not turn off the computer at this time !
   At Stopping Service

6. After the ECS is restarted, run the **cmd** command to open the CLI and run **whoami /user** to verify that the SID has been changed.

16.6 Why Does a Pay-per-Use ECS Fail to Be Started?

After a pay-per-use ECS is stopped, its resources such as vCPUs and memory are released. When it is being started the next time, the startup may fail due to insufficient resources.

If the ECS startup failed, try again later or modify the specifications.

For details about how to modify specifications, see **Modifying Individual ECS Specifications**.

16.7 Why Is the Memory of an ECS Obtained by Running the free Command Inconsistent with the Actual Memory?

Symptom

After you create an ECS, you run the **free -m** command to view the ECS memory. The ECS memory is less than the memory configured during ECS creation.

For example:

When you are creating an ECS, the configured memory size is 4,194,304 KB (4,096 MB). After the ECS is created, you run the **free -m** command to view its memory. The command output is as follows:

```
[root@localhost ~]# free -m
total used free shared buff/cache available
Mem: 3790 167 3474 8 147 3414
Swap: 1022 0 1022
```

The memory in the command output is 3,790 MB, which is less than the configured 4,096 MB.

Run the **dmidecode -t memory** command to check the actual memory configured for the ECS. The command output is as follows:

```
[root@localhost ~]# dmidecode -t memory
# dmidecode 3.0
Getting SMBIOS data from sysfs.
SMBIOS 2.8 present.

Handle 0x1000, DMI type 16, 23 bytes
Physical Memory Array
Location: Other
Use: System Memory
Error Correction Type: Multi-bit ECC
Maximum Capacity: 4 GB
Error Information Handle: Not Provided
Number Of Devices: 1

Handle 0x1100, DMI type 17, 40 bytes
Memory Device
Array Handle: 0x1000
Error Information Handle: Not Provided
Total Width: Unknown
Data Width: Unknown
Size: 4,096 MB
Form Factor: DIMM
Set: None
Locator: DIMM 0
Bank Locator: Not Specified
Type: RAM
Type Detail: Other
Speed: Unknown
Manufacturer: QEMU
Serial Number: Not Specified
Asset Tag: Not Specified
Part Number: Not Specified
Rank: Unknown
Configured Clock Speed: Unknown
Minimum Voltage: Unknown
Maximum Voltage: Unknown
Configured Voltage: Unknown
```

The memory in the command output is the same as that configured during ECS creation.

Possible Causes

When the OS is started, related devices are initialized, which occupies memory. In addition, when the kernel is started, it also occupies memory. The memory occupied by kdump can be set. Unless otherwise specified, do not change the memory size occupied by kdump.

The command output of **free -m** shows the available memory of the ECS, and that of **dmidecode -t memory** shows the hardware memory.

The memory obtained by running the **free -m** command is less than the memory configured for the ECS. This is a normal phenomenon.

NOTE

This is a normal phenomenon even for physical servers.

16.8 Why Is the Hostname of My ECS Restored to the Original Name After the ECS Is Restarted?

The following uses an ECS running CentOS 7 as an example:

1. Log in to the Linux ECS and view the Cloud-Init configuration file.
2. In the **/etc/cloud/cloud.cfg** file, comment out or delete **update_hostname**.

   NOTE

   - **update_hostname** indicates that the hostname is changed in Cloud-Init each time the ECS is restarted.
   - For an ECS created from a public image, Cloud-Init has been installed on it by default. You do not need to manually install Cloud-Init for it. For details about how to modify a private image, see **Installing Cloud-Init**.

16.9 Is an ECS Hostname with Suffix .novalocal Normal?

Symptom

Hostnames of ECSs created based on some types of images have the suffix **.novalocal**, whereas others do not.

For example, the hostname is set to **abc** during ECS creation. **Table 16-2** lists the hostnames (obtained by running the **hostname** command) of ECSs created using different images and those displayed after the ECSs are restarted.

Table 16-2 Hostnames of ECSs created from different images

Image	Hostname Before ECS Restart	Hostname After ECS Restart
CentOS 6.8	abc	abc.novalocal
CentOS 7.3	abc.novalocal	abc.novalocal
Ubuntu 16	abc	abc

Troubleshooting

This is a normal phenomenon.

The static hostname of a Linux ECS is user defined and injected using Cloud-Init during the ECS creation. According to the test results, Cloud-Init adapts to OSs differently. As a result, hostnames of some ECSs have suffix **.novalocal**, whereas others do not.

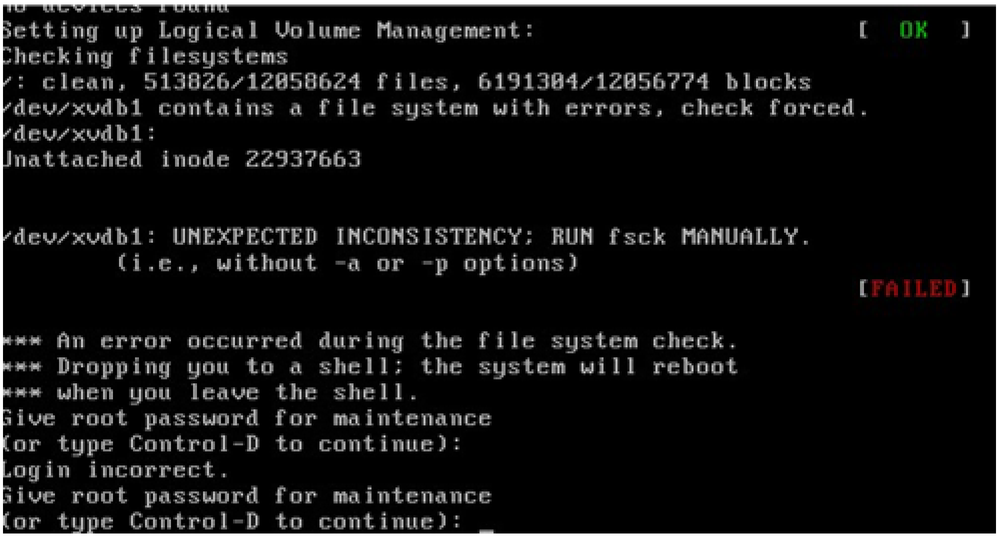
If you do not want to have the obtained hostnames contain suffix **.novalocal**, change the hostnames by referring to **How Can a Changed Static Hostname Take Effect Permanently?**

16.10 Why Does a Forcibly-Stopped Linux ECS Fail to Be Restarted?

Symptom

When you try to restart a forcibly-stopped Linux ECS, the ECS failed to be restarted, as shown in **Figure 16-12**.

Figure 16-12 Restart failure



```
Setting up Logical Volume Management:                          [  OK  ]
Checking filesystems
/: clean, 513826/12058624 files, 6191304/12056774 blocks
/dev/xvdb1 contains a file system with errors, check forced.
/dev/xvdb1:
Unattached inode 22937663


/dev/xvdb1: UNEXPECTED INCONSISTENCY: RUN fsck MANUALLY.
        (i.e., without -a or -p options)
                                                               [FAILED]

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

Possible Causes

As shown in **Figure 16-12**, the ECS cannot be restarted because the file system was damaged. Forcibly stopping or restarting an ECS is highly risky because this operation may cause inconsistent metadata in the file system, leading to the file system damage.

Solution

Use the disk repair tool (fsck) delivered with the Linux OS to rectify the fault.

The following procedure considers the affected disk partition as **/dev/xvdb1**, which is the partition shown in **Figure 16-12**.

1. Enter the password of user **root** as prompted.
2. Run the following command to check whether the affected disk partition has been mounted:

   mount | grep xvdb1

   - If yes, go to step 3.
   - If no, go to step 4.
3. Run the following command to unmount the affected disk partition:

   umount /dev/xvdb1
4. Run the following command to rectify the file system of the affected disk partition:

   fsck -y /dev/xvdb1
5. Run the following command to restart the ECS:

   reboot

   NOTE

   If the fault persists, contact customer service for technical support.

16.11 How Can a Changed Static Hostname Take Effect Permanently?

Symptom

The static hostname of a Linux ECS is user defined and injected using Cloud-Init during the ECS creation. Although the hostname can be changed by running the **hostname** command, the changed hostname is restored after the ECS is restarted.

Changing the Hostname on the ECS

To make the changed hostname still take effect even after the ECS is stopped or restarted, save the changed hostname into configuration files.

The changed hostname is assumed to be **new_hostname**.

1. Modify the **/etc/hostname** configuration file.
   1. Run the following command to edit the configuration file:

      sudo vim /etc/hostname
   2. Change the hostname to the new one.
   3. Run the following command to save and exit the configuration file:

      :wq
2. Modify the **/etc/sysconfig/network** configuration file.
   1. Run the following command to edit the configuration file:

      sudo vim /etc/sysconfig/network
   2. Change the **HOSTNAME** value to the new hostname.

      HOSTNAME=*Changed hostname*

NOTE

If there is no **HOSTNAME** in the configuration file, manually add this parameter and set it to the changed hostname.

For example:

```
HOSTNAME=new_hostname
```

   c. Run the following command to save and exit the configuration file:

      :wq

3. Modify the **/etc/cloud/cloud.cfg** configuration file.
   a. Run the following command to edit the configuration file:

      sudo vim /etc/cloud/cloud.cfg

   b. Use either of the following methods to modify the configuration file:
      - Method 1: Change the **preserve_hostname** parameter value or add the **preserve_hostname** parameter to the configuration file.

        If **preserve_hostname: false** is already available in the **/etc/cloud/cloud.cfg** configuration file, change it to **preserve_hostname: true**. If **preserve_hostname** is unavailable in the **/etc/cloud/cloud.cfg** configuration file, add **preserve_hostname: true** before **cloud_init_modules**.

        If you use method 1, the changed hostname still takes effect after the ECS is stopped or restarted. However, if the ECS is used to create a private image and the image is used to create a new ECS, the hostname of the new ECS is the hostname (**new_hostname**) used by the private image, and user-defined hostnames cannot be injected using Cloud-Init.

      - Method 2 (recommended): Delete or comment out **- update_hostname**.

        If you use method 2, the changed hostname still takes effect after the ECS is stopped or restarted. If the ECS is used to create a private image and the image is used to create a new ECS, the changed hostname permanently takes effect, and user-defined hostnames (such as **new_new_hostname**) can be injected using Cloud-Init.

        NOTE

        After a user-defined name of ECS using some OS versions is injected using Cloud-init, the host name obtained by running the **hostname** command may contain the **.novalocal** suffix. For details, see **Is an ECS Hostname with Suffix .novalocal Normal?**

        In this case, you can modify the configuration by referring to **Installing Cloud-Init** so that the host name created using a private image does not contain the **.novalocal** suffix.

4. Run the following command to restart the ECS:

   sudo reboot

5. Run the following command to check whether the hostname has been changed:

   sudo hostname

   If the changed hostname is displayed in the command output, the hostname has been changed and the new name permanently takes effect.

Modifying the Mapping Between the ECS Hostname and IP Address (Modifying the hosts File)

If you want to use the changed hostname as the preferred localhost and localhost.localdomain, update the mapping between the hostname and IP address after the hostname is changed and then save the configuration to the corresponding Cloud-Init configuration file so that the new hostname takes effect permanently.

The changed hostname is assumed to be **new_hostname**.

1. Modify the **/etc/hostname** configuration file.
    a. Run the following command to edit the configuration file:
       sudo vim /etc/hostname
    b. Change the hostname to the new one.
    c. Run the following command to save and exit the configuration file:
       :wq
2. Modify the **/etc/sysconfig/network** configuration file.
    a. Run the following command to edit the configuration file:
       sudo vim /etc/sysconfig/network
    b. Change the **HOSTNAME** value to the new hostname.
       HOSTNAME=*Changed hostname*

       NOTE

       If there is no **HOSTNAME** in the configuration file, manually add this parameter and set it to the changed hostname.

       For example:

       ```
       HOSTNAME=new_hostname
       ```
    c. Run the following command to save and exit the configuration file:
       :wq
3. Modify the **/etc/cloud/cloud.cfg** configuration file.
    a. Run the following command to edit the configuration file:
       sudo vim /etc/cloud/cloud.cfg
    b. Use either of the following methods to modify the configuration file:
        - Method 1: Change the **preserve_hostname** parameter value or add the **preserve_hostname** parameter to the configuration file.

          If **preserve_hostname: false** is already available in the **/etc/cloud/cloud.cfg** configuration file, change it to **preserve_hostname: true**. If **preserve_hostname** is unavailable in the **/etc/cloud/cloud.cfg** configuration file, add **preserve_hostname: true** before **cloud_init_modules**.

          If you use method 1, the changed hostname still takes effect after the ECS is stopped or restarted. However, if the ECS is used to create a private image and the image is used to create a new ECS, the hostname of the new ECS is the hostname (**new_hostname**) used by the private image, and user-defined hostnames cannot be injected using Cloud-Init.

- Method 2 (recommended): Delete or comment out **-update_hostname**.

  If you use method 2, the changed hostname still takes effect after the ECS is stopped or restarted. If the ECS is used to create a private image and the image is used to create a new ECS, the changed hostname permanently takes effect, and user-defined hostnames (such as **new_new_hostname**) can be injected using Cloud-Init.

4. Update the mapping between the hostname and IP address in **/etc/hosts** to an entry starting with 127.0.0.1. Use **new_hostname** as your preferred **localhost** and **localhost.localdomain**.
   1. Run the following command to edit **/etc/hosts**:

      sudo vim /etc/hosts
   2. Modify the entry starting with 127.0.0.1 and replace **localhost** and **localhost.localdomain** with **new_hostname**.
      ```
      ::1     localhost       localhost.localdomain   localhost6      localhost6.localdomain6
      127.0.0.1       localhost       localhost.localdomain   localhost4      localhost4.localdomain4
      127.0.0.1       new_hostname    new_hostname
      ```
   3. Run the following command to save and exit the configuration file:

      :wq
5. Modify the **/etc/cloud/cloud.cfg** configuration file.
   1. Run the following command to edit the configuration file:

      sudo vim /etc/cloud/cloud.cfg
   2. Set **manage_etc_hosts** to **manage_etc_hosts: false**.
      ```
      manage_etc_hosts: false
      ```
   3. Run the following command to save and exit the configuration file:

      :wq
6. Run the following command to restart the ECS:

   sudo reboot
7. Run the following commands to check whether the changes to **hostname** and **hosts** take effect permanently:

   sudo hostname

   sudo cat /etc/hosts

   If the changed hostname (**new_hostname**) and **hosts** are displayed in the command output, the changes take effect permanently.

16.12 Why Can't My Linux ECS Obtain Metadata?

Symptom

The security group of the Linux ECS has been configured based on the prerequisites in **Obtaining Metadata** in the outbound direction, but the ECS still cannot obtain the metadata through the route with the destination of 169.254.169.254.

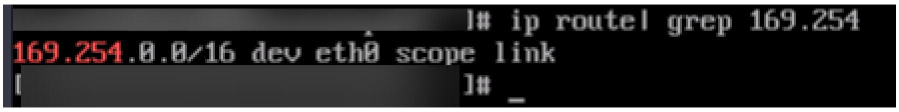
Root Cause

Run the following command on the Linux ECS configured with a static IP address:

# ip route| grep 169.254

The route with the destination of 169.254.169.254 does not exist, but the route with the destination of 169.254.0.0/16 exists.

Figure 16-13 Route information



```
[redacted]]# ip route| grep 169.254
169.254.0.0/16 dev eth0 scope link
[[redacted]]# _
```

After the network is restarted, the original route with the destination of 169.254.169.254 is changed to the route with the destination of 169.254.0.0/16 without a next hop, as shown in **Figure 16-13**. As a result, the Linux ECS cannot obtain metadata.

Solution

1. Add the route with the destination of 169.254.169.254, and specify the next hop (gateway) and the output device (primary NIC of the Linux ECS). The following is an example:

   # ip route add 169.254.169.254 via *192.168.1.1* dev *eth0*

   192.168.1.1 is the gateway address of the subnet that the primary NIC resides, and eth0 is the primary NIC.

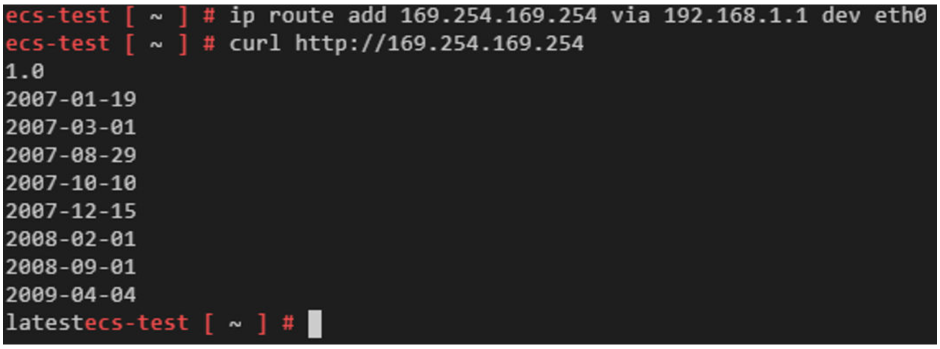
   How Do I View the Primary NIC?

   How Do I View the Gateway Address?

2. Run the following command to verify that the metadata can be obtained:

   # curl http://169.254.169.254

   Figure 16-14 Obtaining metadata

```
ecs-test [ ~ ] # ip route add 169.254.169.254 via 192.168.1.1 dev eth0
ecs-test [ ~ ] # curl http://169.254.169.254
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
latestecs-test [ ~ ] # 
```

3. Run the following command to create or modify the **/etc/sysconfig/network-scripts/route-eth0** file to prevent the static route from being changed after network restart:

   # vi /etc/sysconfig/network-scripts/route-eth0

   Add the following content to the file:

In this example, the primary NIC is eth0 and gateway address is 192.168.1.1. Replace them based on site requirements.

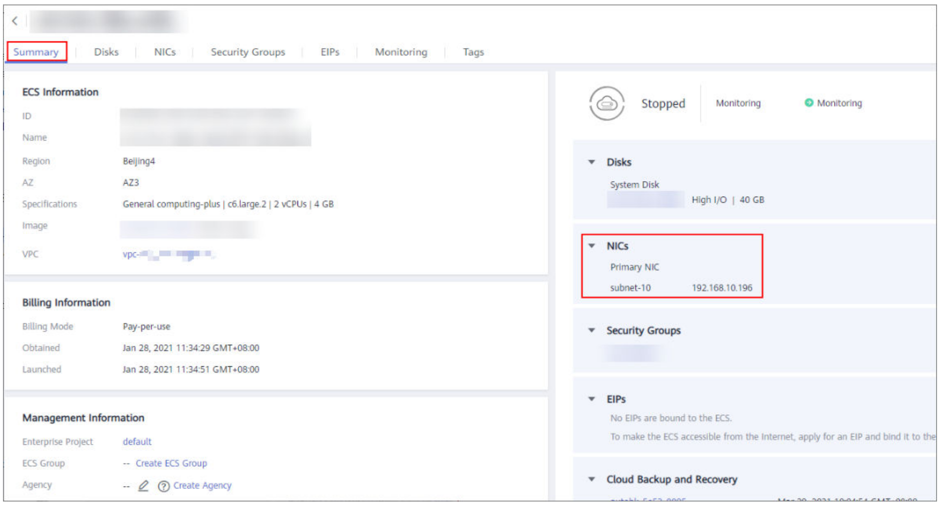
```
# 169.254.169.254 via 192.168.1.1
```

How Do I View the Primary NIC?

1. Log in to the **management console**.
2. Click in the upper left corner and select a region and project.
3. Under **Compute**, click **Elastic Cloud Server**.
4. Click the name of the target ECS.

   The page providing details about the ECS is displayed.
5. Click the **Summary** tab to view details about the primary NIC.

Figure 16-15 Primary NIC details



ECS Information

ID [redacted]

Name

Region Beijing4

AZ AZ3

Specifications General computing-plus | c6.large.2 | 2 vCPUs | 4 GB

Image [redacted]

VPC vpc-[redacted]

Billing Information

Billing Mode Pay-per-use

Obtained Jan 28, 2021 11:34:29 GMT+08:00

Launched Jan 28, 2021 11:34:51 GMT+08:00

Management Information

Enterprise Project default

ECS Group -- Create ECS Group

Agency -- Create Agency

Disks

System Disk

[redacted] High I/O | 40 GB

NICs

Primary NIC

subnet-10 192.168.10.196

Security Groups

[redacted]

EIPs

No EIPs are bound to the ECS.

To make the ECS accessible from the Internet, apply for an EIP and bind it to the

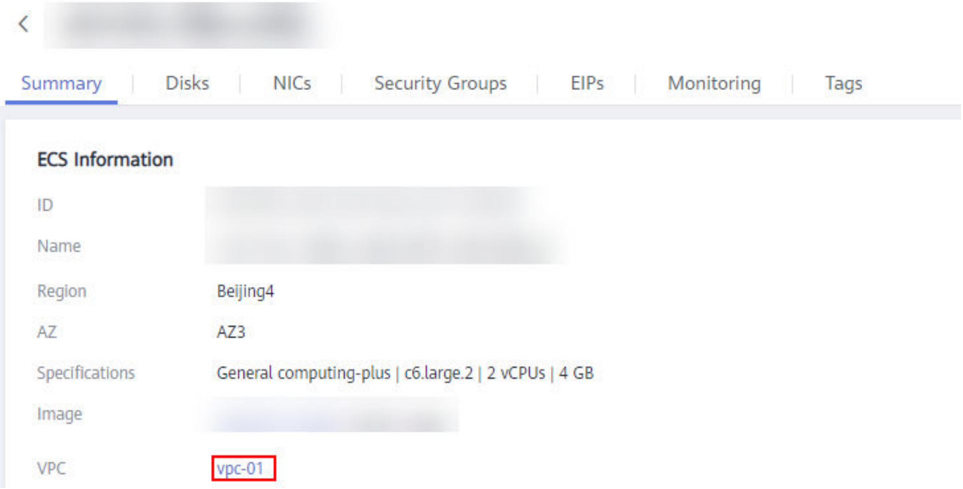
Cloud Backup and Recovery

How Do I View the Gateway Address?

1. Log in to the **management console**.
2. Click in the upper left corner and select a region and project.
3. Under **Compute**, click **Elastic Cloud Server**.
4. Click the name of the target ECS.

   The page providing details about the ECS is displayed.
5. Click the VPC name to go to the VPC list page.

Figure 16-16 VPC name



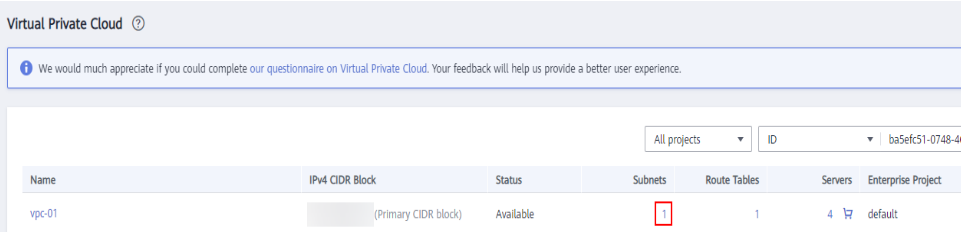
[redacted]

ECS Information

ID [redacted]
Name [redacted]
Region Beijing4
AZ AZ3
Specifications General computing-plus | c6.large.2 | 2 vCPUs | 4 GB
Image [redacted]
VPC vpc-01

6. Locate the row that contains the target VPC and click the number in the **Subnets** column to go to the subnet list page.

Figure 16-17 Number in the **Subnets** column



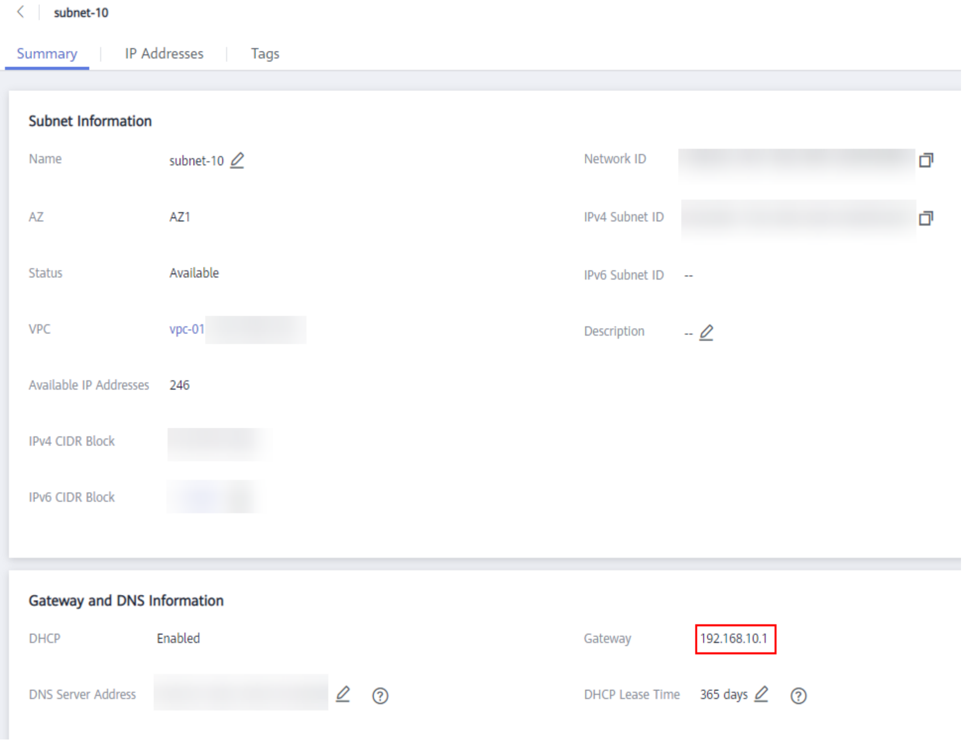
Virtual Private Cloud

We would much appreciate if you could complete our questionnaire on Virtual Private Cloud. Your feedback will help us provide a better user experience.

Name	IPv4 CIDR Block	Status	Subnets	Route Tables	Servers	Enterprise Project
vpc-01	[redacted] (Primary CIDR block)	Available	1	1	4	default

7. Click the target subnet name to go to the subnet details page and view the gateway address.

Figure 16-18 Gateway address



Subnet Information

Name subnet-10

AZ AZ1

Status Available

VPC vpc-01 [redacted]

Available IP Addresses 246

IPv4 CIDR Block [redacted]

IPv6 CIDR Block [redacted]

Network ID [redacted]

IPv4 Subnet ID [redacted]

IPv6 Subnet ID --

Description --

Gateway and DNS Information

DHCP Enabled

DNS Server Address [redacted]

Gateway 192.168.10.1

DHCP Lease Time 365 days

17 ECS Lag (Windows)

17.1 Why Is My Windows ECS Running Slowly?

If your ECS runs slowly or is disconnected suddenly, the possible causes are as follows:

- Your ECS is a shared ECS.

  Multiple ECSs share CPU resources. When resources are insufficient, ECSs may contend for CPU resources, causing slow responses.

- The bandwidth or CPU usage of the ECS may be excessively high.

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

If your ECS is a shared ECS, perform the following steps:

1. Fault locating: Check the instance type. For details about dedicated and shared ECSs, see **ECS Types**.
2. Troubleshooting: If you have high requirements on service stability, you are advised to change a shared ECS to a dedicated ECS by referring to **Modifying Individual ECS Specifications**.

To handle this issue, perform the following operations:

1. Fault locating:

   Identify the drivers from unknown sources and processes leading to high bandwidth or CPU 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 full memory dump.

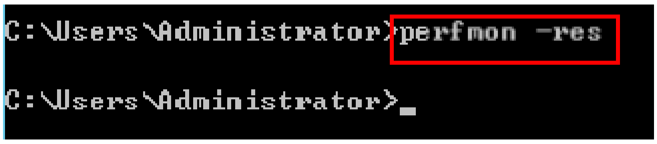
2. Check whether the processes and drivers are malicious and handle the issue accordingly.
   - If the processes are not malicious, optimize their programs or **modify ECS specifications**.
   - If the processes are abnormal, stop these processes manually or use a third-party tool to stop them automatically.

- If the drivers are from official sources, there is no need to deal with system built-in drivers. Determine whether to uninstall the third-party software based on your requirements.
- If the drivers are from unknown sources, you are advised to uninstall them by using commercial antivirus software or third-party security management tools.

Fault Locating

1. Log in to the ECS using VNC available on the management console.
2. Start the **Run** dialog box, and then enter **perfmon -res**.

Figure 17-1 Starting the Resource Monitor



```
C:\Users\Administrator>perfmon -res

C:\Users\Administrator>_
```

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

Figure 17-2 Resource Monitor

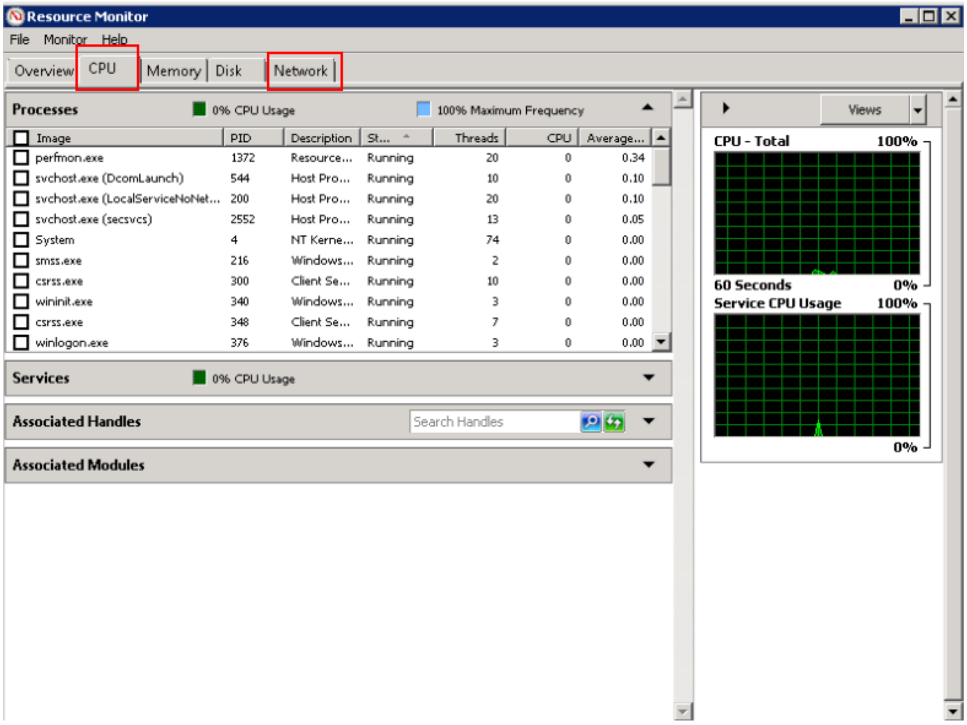


Image	PID	Description	St...	Threads	CPU	Average...
☐ perfmon.exe	1372	Resource...	Running	20	0	0.34
☐ svchost.exe (DcomLaunch)	544	Host Pro...	Running	10	0	0.10
☐ svchost.exe (LocalServiceNoNet...	200	Host Pro...	Running	20	0	0.10
☐ svchost.exe (secsvcs)	2552	Host Pro...	Running	13	0	0.05
☐ System	4	NT Kerne...	Running	74	0	0.00
☐ smss.exe	216	Windows...	Running	2	0	0.00
☐ csrss.exe	300	Client Se...	Running	10	0	0.00
☐ wininit.exe	340	Windows...	Running	3	0	0.00
☐ csrss.exe	348	Client Se...	Running	7	0	0.00
☐ winlogon.exe	376	Windows...	Running	3	0	0.00

4. Obtain the IDs and names of the processes with high CPU or bandwidth usage.
5. On the VNC remote login page, click **Ctrl+Alt+Del** to start the **Windows Task Manager**.

   Alternatively, start the **Run** dialog box and enter **taskmgr** to start the **Windows Task Manager**.

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

a. Click the **Processes** tab.

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

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

d. Check whether the process is malicious.

Figure 17-3 Checking the process

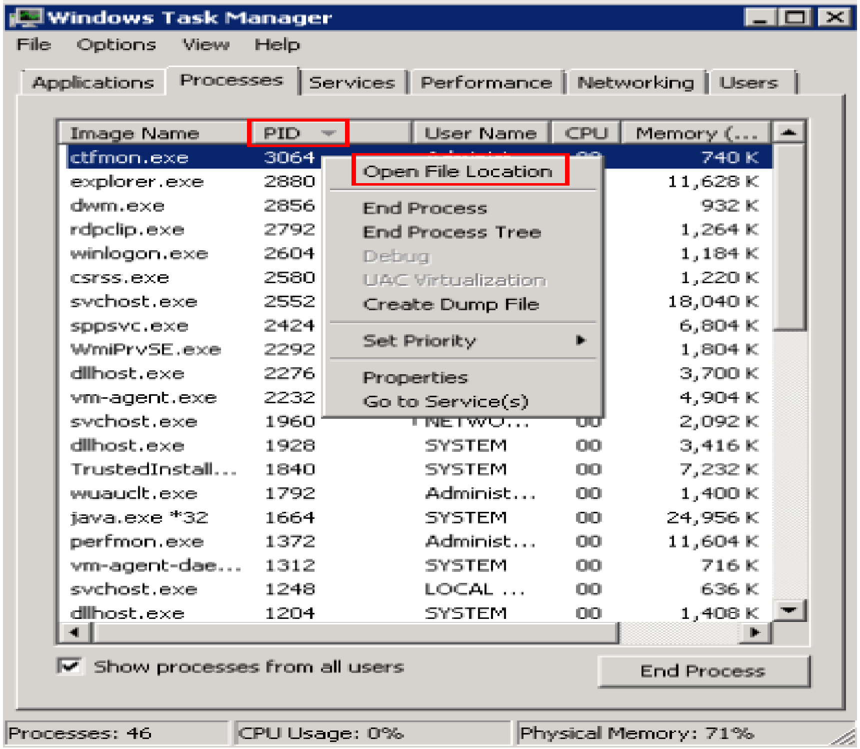


Image Name	PID	User Name	CPU	Memory (...
ctfmon.exe	3064			740 K
explorer.exe	2880			11,628 K
dwm.exe	2856			932 K
rdpclip.exe	2792			1,264 K
winlogon.exe	2604			1,184 K
csrss.exe	2580			1,220 K
svchost.exe	2552			18,040 K
sppsvc.exe	2424			6,804 K
WmiPrvSE.exe	2292			1,804 K
dllhost.exe	2276			3,700 K
vm-agent.exe	2232			4,904 K
svchost.exe	1960	NETWO...	00	2,092 K
dllhost.exe	1928	SYSTEM	00	3,416 K
TrustedInstall...	1840	SYSTEM	00	7,232 K
wuauclt.exe	1792	Administ...	00	1,400 K
java.exe *32	1664	SYSTEM	00	24,956 K
perfmon.exe	1372	Administ...	00	11,604 K
vm-agent-dae...	1312	SYSTEM	00	716 K
svchost.exe	1248	LOCAL ...	00	636 K
dllhost.exe	1204	SYSTEM	00	1,408 K

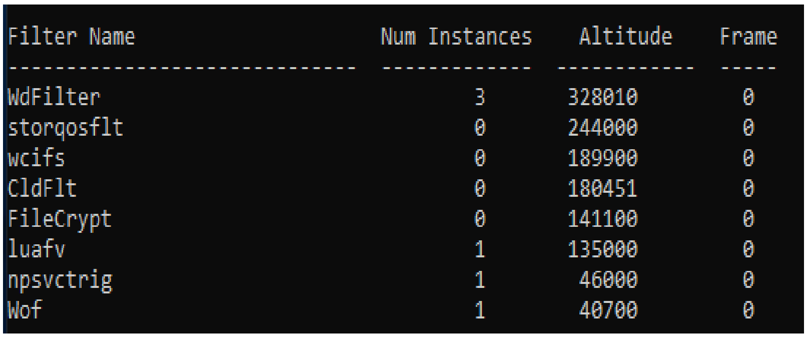
☑ Show processes from all users

Processes: 46 CPU Usage: 0% Physical Memory: 71%

6. Open the **Run** dialog box and enter **fltmc** to view the filter drivers of the system.

   The following figure uses Windows 10 as an example. Different OSs have different built-in drivers. For details, see their official websites. If a third-party driver is installed, it is also displayed in this figure.

Figure 17-4 Viewing the system drivers

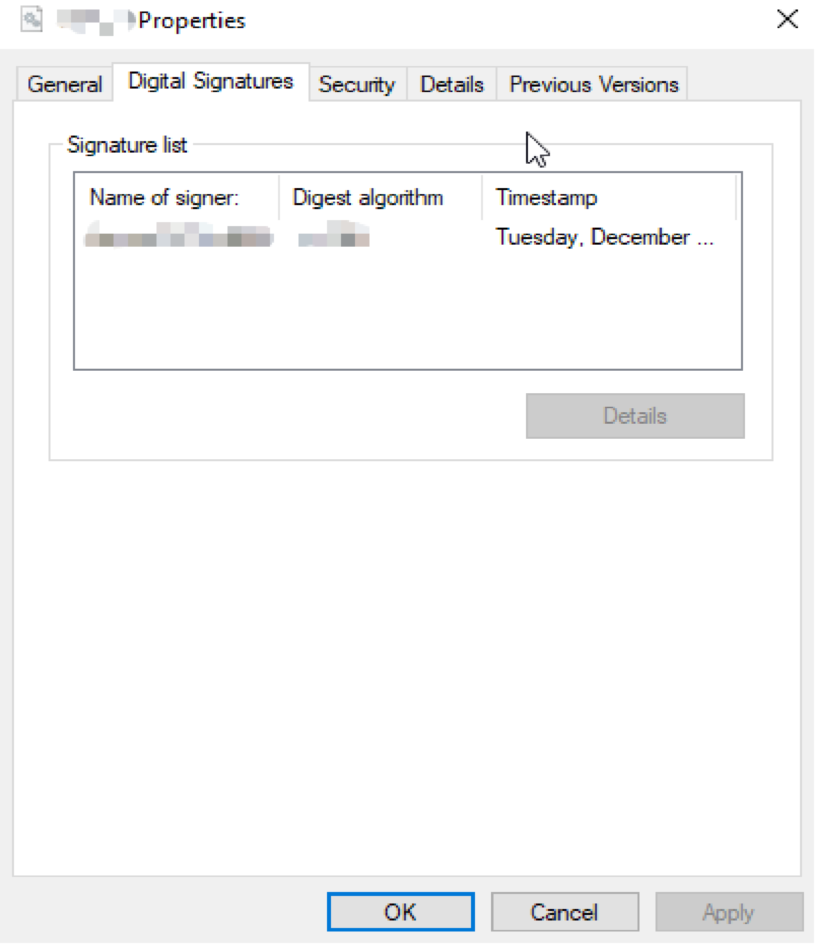


```
Filter Name                     Num Instances    Altitude    Frame
------------------------------  -------------  ------------  -----
WdFilter                                3        328010         0
storqosflt                              0        244000         0
wcifs                                   0        189900         0
CldFlt                                  0        180451         0
FileCrypt                               0        141100         0
luafv                                   1        135000         0
npsvctrig                               1         46000         0
Wof                                     1         40700         0
```

The following describes how to view a driver source and check whether the source is unknown.

a. Go to the **C:\Windows\System32\drivers** directory on the local PC.
b. Click the name of the unknown driver and choose **Properties** to view its details.
c. Click the **Digital Signatures** tab to view the driver source.

Figure 17-5 Viewing the driver source



Troubleshooting

Before the troubleshooting, check whether the processes or drivers leading to the high CPU or bandwidth usage are normal, and handle the issue accordingly.

Suggestions for non-malicious processes

1. If your ECS runs Windows Server 2008 or 2012, ensure that the available memory is 2 GiB or larger.
2. Check whether Windows Update is running.
3. Check whether the antivirus software is scanning files and programs on the backend.
4. Check whether any applications requiring high CPU or bandwidth resources are running on the ECS. If yes, **modify ECS specifications** or **increase bandwidth**.

5. If the ECS configuration meets the 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 caused by viruses or Trojan horses, manually stop the affected processes. You are advised to troubleshoot the issue as follows:

1. Use the 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 the official Microsoft document *How to perform a clean boot in Windows*.
4. If the ECS or site encounters a DDoS or CC attack, and a large number of access requests are generated within a short period, log in to the management console and perform the following operations:
   - Check whether Anti-DDoS has been enabled and whether the protection rules are proper. To configure a protection rule, see **Setting a Traffic Scrubbing Threshold to Intercept Attack Traffic**.
   - Check whether CC attack protection has been enabled and whether the protection rules are appropriate. To configure a protection rule, see **Configuring a CC Attack Protection Rule**.

Suggestions for drivers from unknown sources

Some viruses and Trojan horses are loaded through the filter drivers of the system. If you find a driver from an unknown source, you are advised to uninstall it. You can also use commercial antivirus software or third-party security management tools to delete it.

If an unknown driver cannot be deleted, or will appear again after being deleted, it is usually a virus or Trojan horse driver. If the driver cannot be completely deleted using commercial antivirus software or third-party security management tools, you are advised to reinstall the OS and back up data before the reinstallation.

18 ECS Lag (Linux)

18.1 Why Is My Linux ECS Running Slowly?

If your ECS runs slowly or is disconnected suddenly, the possible causes are as follows:

- Your ECS is a shared ECS.

  Multiple ECSs share CPU resources. When resources are insufficient, ECSs may contend for CPU resources, causing slow responses.

- The bandwidth or CPU usage of the ECS may be excessively high.

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

If your ECS is a shared ECS, perform the following steps:

1. Fault locating: Check the instance type. For details about dedicated and shared ECSs, see **ECS Types**.
2. Troubleshooting: If you have high requirements on service stability, you are advised to change a shared ECS to a dedicated ECS by referring to **Modifying Individual ECS Specifications**.

To handle this issue, perform the following operations:

1. Fault locating:

   Identify the processes leading to high bandwidth or CPU usage.

2. Troubleshooting: Check whether the processes are malicious and handle the issue accordingly.
   - If the processes are normal, optimize them or **modify ECS specifications**.
   - If the processes are malicious, stop these processes manually or use a third-party tool to stop them automatically.

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 ECS performance metrics, such as the CPU usage, are as follows:

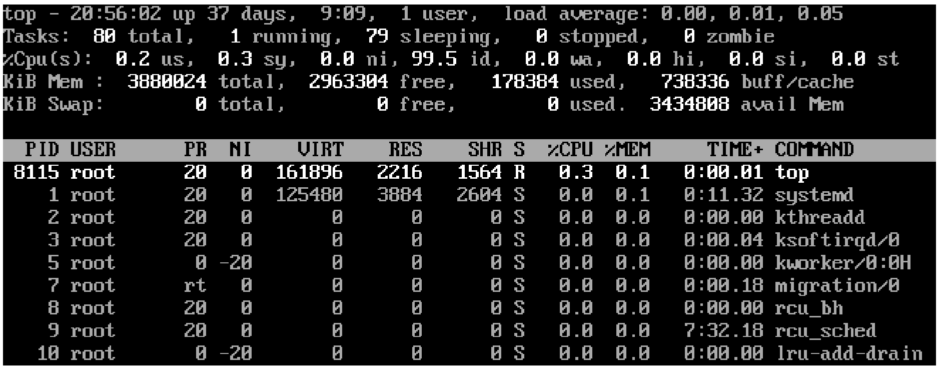
- **ps -aux**
- **ps -ef**
- **top**

Locating High CPU Usage

1. Log in to the ECS using VNC.
2. Run the following command to check the OS running status:

   top

   Information similar to the following is displayed.

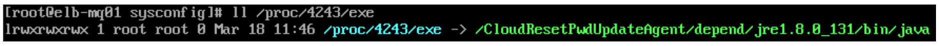
```
top - 20:56:02 up 37 days,  9:09,  1 user,  load average: 0.00, 0.01, 0.05
Tasks:  80 total,   1 running,  79 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.2 us,  0.3 sy,  0.0 ni, 99.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3880024 total,  2963304 free,   178384 used,   738336 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  3434808 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 8115 root      20   0  161896   2216   1564 R   0.3  0.1   0:00.01 top
    1 root      20   0  125480   3884   2604 S   0.0  0.1   0:11.32 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S   0.0  0.0   0:00.04 ksoftirqd/0
    5 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0H
    7 root      rt   0       0      0      0 S   0.0  0.0   0:00.18 migration/0
    8 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcu_bh
    9 root      20   0       0      0      0 S   0.0  0.0   7:32.18 rcu_sched
   10 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 lru-add-drain
```

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 ECS 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 PID.



```
[root@elb-mq01 sysconfig]# ll /proc/4243/exe
lrwxrwxrwx 1 root root 0 Mar 18 11:46 /proc/4243/exe -> /CloudResetPwdUpdateAgent/depend/jre1.8.0_131/bin/java
```

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 ECS 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.

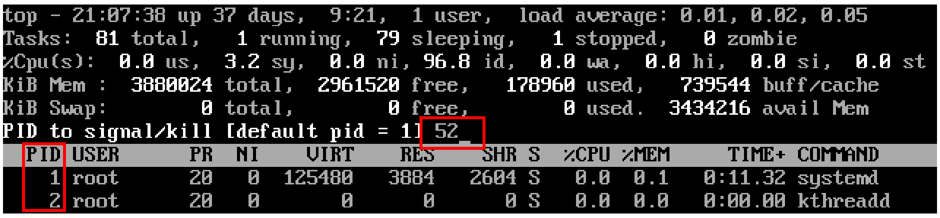
- For the detected malicious processes

  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.

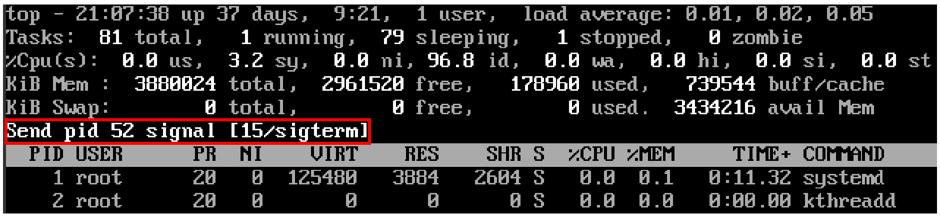
  b. Enter the PID of the process to be stopped.

     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**.



```
top - 21:07:38 up 37 days,  9:21,  1 user,  load average: 0.01, 0.02, 0.05
Tasks:  81 total,   1 running,  79 sleeping,   1 stopped,   0 zombie
%Cpu(s):  0.0 us,  3.2 sy,  0.0 ni, 96.8 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3880024 total,  2961520 free,   178960 used,   739544 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  3434216 avail Mem
PID to signal/kill [default pid = 1] 52_
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
    1 root      20   0  125480   3884   2604 S   0.0  0.1   0:11.32 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kthreadd
```

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



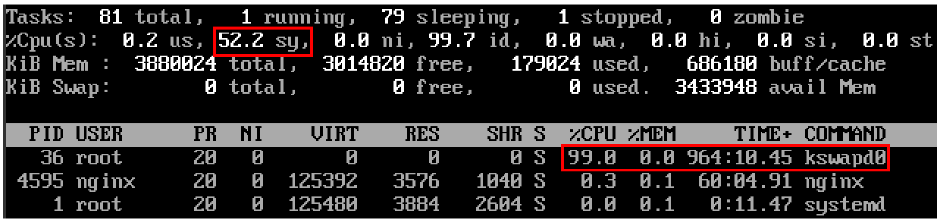
```
top - 21:07:38 up 37 days,  9:21,  1 user,  load average: 0.01, 0.02, 0.05
Tasks:  81 total,   1 running,  79 sleeping,   1 stopped,   0 zombie
%Cpu(s):  0.0 us,  3.2 sy,  0.0 ni, 96.8 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3880024 total,  2961520 free,   178960 used,   739544 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  3434216 avail Mem
Send pid 52 signal [15/sigterm]
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
    1 root      20   0  125480   3884   2604 S   0.0  0.1   0:11.32 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kthreadd
```

- 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, you can preliminarily determine that the system is consistently paging. In such a case, the high CPU usage is caused by insufficient memory.



```
Tasks:  81 total,   1 running,  79 sleeping,   1 stopped,   0 zombie
%Cpu(s):  0.2 us, 52.2 sy,  0.0 ni, 99.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3880024 total,  3014820 free,   179024 used,   686180 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  3433948 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
   36 root      20   0       0      0      0 S  99.0  0.0 964:10.45 kswapd0
 4595 nginx     20   0  125392   3576   1040 S   0.3  0.1  60:04.91 nginx
    1 root      20   0  125480   3884   2604 S   0.0  0.1   0:11.47 systemd
```

  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 by running 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.

  To handle this issue, expand the ECS 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 ECS, 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 **nethogs** command to check bandwidth usage.

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

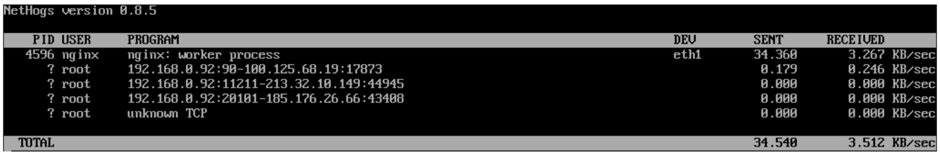
   - **-d**: Set the update interval in the unit of second. The default value is 1s.
   - **-t**: Enable tracing.
   - **-c**: Set the number of updates.
   - **device**: Set the NIC to be monitored. The default value is **eth0**.

   The following parameters are involved in command execution:

   - **q**: Exit **nethogs**.
   - **s**: Sort processes in the process list by TX traffic in ascending or descending order.
   - **r**: Sort processes in the process list by RX traffic in ascending or descending order.
   - **m**: Switch 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*



```
NetHogs version 0.8.5

  PID USER     PROGRAM                                      DEV        SENT      RECEIVED
 4596 nginx    nginx: worker process                        eth1      34.360      3.267 KB/sec
    ? root     192.168.0.92:90-100.125.68.19:17873                     0.179      0.246 KB/sec
    ? root     192.168.0.92:11211-213.32.10.149:44945                  0.000      0.000 KB/sec
    ? root     192.168.0.92:20101-185.176.26.66:43408                  0.000      0.000 KB/sec
    ? root     unknown TCP                                             0.000      0.000 KB/sec

 TOTAL                                                                34.540      3.512 KB/sec
```

   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 ECS against CC attacks

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

19 Specification Modification

19.1 How Do I Upgrade or Downgrade the Specifications of an ECS and Do I Need to Stop the ECS?

If the specifications of an existing ECS cannot meet service requirements, modify the ECS specifications as needed, for example, upgrading the vCPUs and memory.

To do so, switch to the list view on the **Elastic Cloud Server** page, locate the row containing the target ECS and choose **More** > **Modify Specifications** in the **Operation** column.

NOTICE

The ECS needs to be stopped during the specification modification, so you are advised to perform this operation during off-peak hours.

Specification modifications include specification upgrade and downgrade.

- For pay-per-use ECSs, the specifications upgrade and downgrade take effect immediately. You are billed based on the new specifications.
- For yearly/monthly ECSs:
  - Specifications upgrade: The price of the new specifications is higher than that of the current one. You need to pay for the price difference for the upgrade to take effect.
  - Specifications downgrade: The price of the new specifications is lower than that of the current one. You'll get a refund from Huawei Cloud.

  For details, see **Pricing of a Changed Specification**.

19.2 What Should I Do If My Specifications Modification Request Failed to Submit?

Symptom

When you tried to modify specifications of a stopped ECS, the system displayed a message indicating that the system was busy, and the request failed to be submitted.

Solution

Check the ECS order and resources.

- If the resources specified in the order have entered the retention period, the ECS specifications cannot be modified. In such a case, renew the order and then modify the specifications.
- If your ECS is billed on a yearly/monthly basis, and the order has been renewed but the new order has not taken effect, the ECS specifications cannot be modified. In such a case, unsubscribe from the new order that has not taken effect and then modify the specifications.

19.3 What Should I Do If Executing a Driver Installation Script Failed on an ECS Running CentOS 5?

Scenarios

After executing the script for installing the Virtio driver on an ECS running CentOS 5, users cannot determine whether the driver has been successfully installed. This section describes how to check driver installation.

Procedure

1. Log in to the ECS and create a temporary directory **check**.

   ```
   mkdir /check
   ```

2. Copy the image file to the current directory.

   ```
   cp /boot/initrd-2.6.18-308.el5.img /check/
   ```

3. Run the following commands to convert the file format to .gz:

   ```
   cd /check
   ```

   ```
   mv initrd-2.6.18-308.el5.img initrd-2.6.18-308.el5.img.gz
   ```

4. Decompress the package.

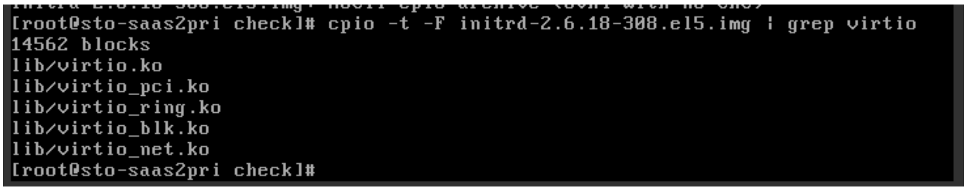
   ```
   gzip -d initrd-2.6.18-308.el5.img.gz
   ```

5. Check whether the driver has been successfully installed.

   ```
   cpio -t -F initrd-2.6.18-308.el5.img | grep virtio
   ```

   The check process is shown in the following figure.

Figure 19-1 Checking driver installation



```
[root@sto-saas2pri check]# cpio -t -F initrd-2.6.18-308.el5.img | grep virtio
14562 blocks
lib/virtio.ko
lib/virtio_pci.ko
lib/virtio_ring.ko
lib/virtio_blk.ko
lib/virtio_net.ko
[root@sto-saas2pri check]#
```

If the command output contains **virtio**, **virtio_blk**, **virtio_net**, and **virtio_pci**, the driver has been successfully installed.

In the preceding figure, the image is of an early version and has no virtio_scsi driver installed. As a result, SCSI disks cannot be attached to such an ECS.

19.4 What Should I Do If Executing a Driver Installation Script Failed When I Attempted to Modify the Specifications of a Linux ECS?

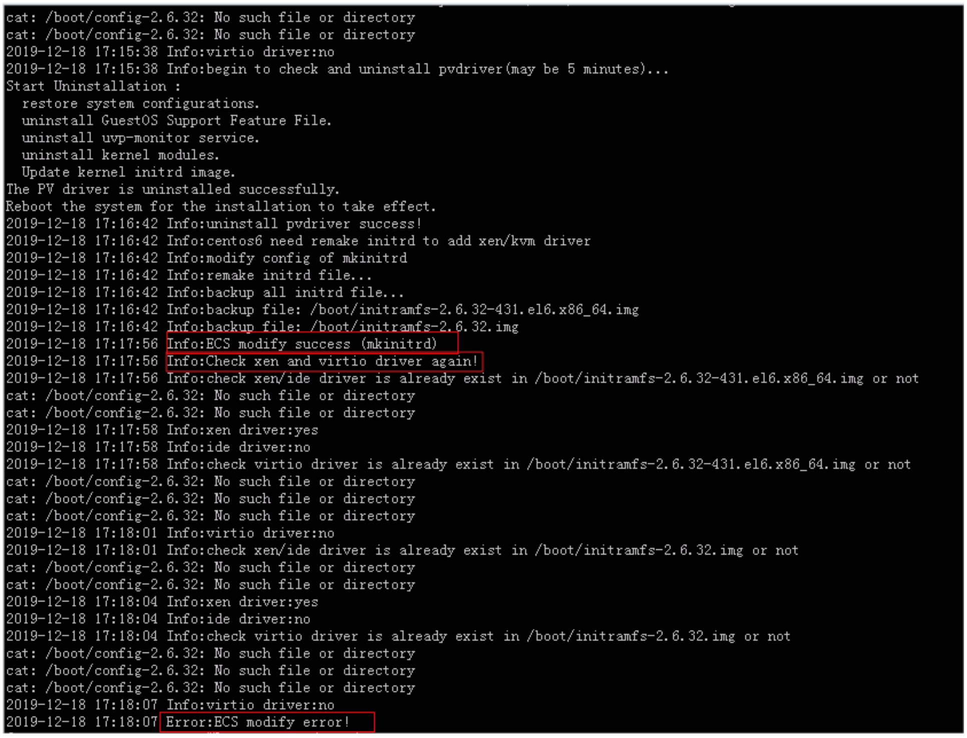
Symptom

During ECS specifications modification, a script was used to automatically install drivers on a Linux ECS.

During the installation, the following information is displayed, indicating that the script has been executed. However, the installation check failed. The possible cause is that certain drivers were not installed on the ECS.

```
...
Info:ECS modify success (mkinitrd)
Info:Check xen and virtio driver again!
...
Error:ECS modify error!
```

Figure 19-2 Successful driver installation with a failed installation check



```
cat: /boot/config-2.6.32: No such file or directory
cat: /boot/config-2.6.32: No such file or directory
2019-12-18 17:15:38 Info:virtio driver:no
2019-12-18 17:15:38 Info:begin to check and uninstall pvdriver(may be 5 minutes)...
Start Uninstallation :
  restore system configurations.
  uninstall GuestOS Support Feature File.
  uninstall uvp-monitor service.
  uninstall kernel modules.
  Update kernel initrd image.
The PV driver is uninstalled successfully.
Reboot the system for the installation to take effect.
2019-12-18 17:16:42 Info:uninstall pvdriver success!
2019-12-18 17:16:42 Info:centos6 need remake initrd to add xen/kvm driver
2019-12-18 17:16:42 Info:modify config of mkinitrd
2019-12-18 17:16:42 Info:remake initrd file...
2019-12-18 17:16:42 Info:backup all initrd file...
2019-12-18 17:16:42 Info:backup file: /boot/initramfs-2.6.32-431.el6.x86_64.img
2019-12-18 17:16:42 Info:backup file: /boot/initramfs-2.6.32.img
2019-12-18 17:17:56 Info:ECS modify success (mkinitrd)
2019-12-18 17:17:56 Info:Check xen and virtio driver again!
2019-12-18 17:17:56 Info:check xen/ide driver is already exist in /boot/initramfs-2.6.32-431.el6.x86_64.img or not
cat: /boot/config-2.6.32: No such file or directory
cat: /boot/config-2.6.32: No such file or directory
2019-12-18 17:17:58 Info:xen driver:yes
2019-12-18 17:17:58 Info:ide driver:no
2019-12-18 17:17:58 Info:check virtio driver is already exist in /boot/initramfs-2.6.32-431.el6.x86_64.img or not
cat: /boot/config-2.6.32: No such file or directory
cat: /boot/config-2.6.32: No such file or directory
cat: /boot/config-2.6.32: No such file or directory
2019-12-18 17:18:01 Info:virtio driver:no
2019-12-18 17:18:01 Info:check xen/ide driver is already exist in /boot/initramfs-2.6.32.img or not
cat: /boot/config-2.6.32: No such file or directory
cat: /boot/config-2.6.32: No such file or directory
2019-12-18 17:18:04 Info:xen driver:yes
2019-12-18 17:18:04 Info:ide driver:no
2019-12-18 17:18:04 Info:check virtio driver is already exist in /boot/initramfs-2.6.32.img or not
cat: /boot/config-2.6.32: No such file or directory
cat: /boot/config-2.6.32: No such file or directory
cat: /boot/config-2.6.32: No such file or directory
2019-12-18 17:18:07 Info:virtio driver:no
2019-12-18 17:18:07 Error:ECS modify error!
```

Solution

Check whether the desired drivers have been successfully installed by following the instructions provided in "Check Whether the ECS Has Been Configured" in **Manually Changing a Xen ECS to a KVM ECS (Linux)**.

If the drivers failed to install, the script may not match the ECS OS. In such a case, manually install the drivers on the Linux ECS by following the instructions provided in **Manually Changing a Xen ECS to a KVM ECS (Linux)**.

Certain Linux ECSs do not have the virtio_scsi driver installed because the kernel version is too early or the kernel has been modified. Such ECSs cannot be attached with SCSI disks. However, this issue will not affect the ECS specifications modification from Xen to KVM. If the ECSs do not use SCSI disks, you can still modify their specifications without the virtio_scsi driver.

19.5 Why Do the Disks of a Windows ECS Go Offline After I Modify the ECS Specifications?

Scenarios

After you modify specifications of a Windows ECS, the disks may go offline. You need to check the number of disks after you modify the specifications.

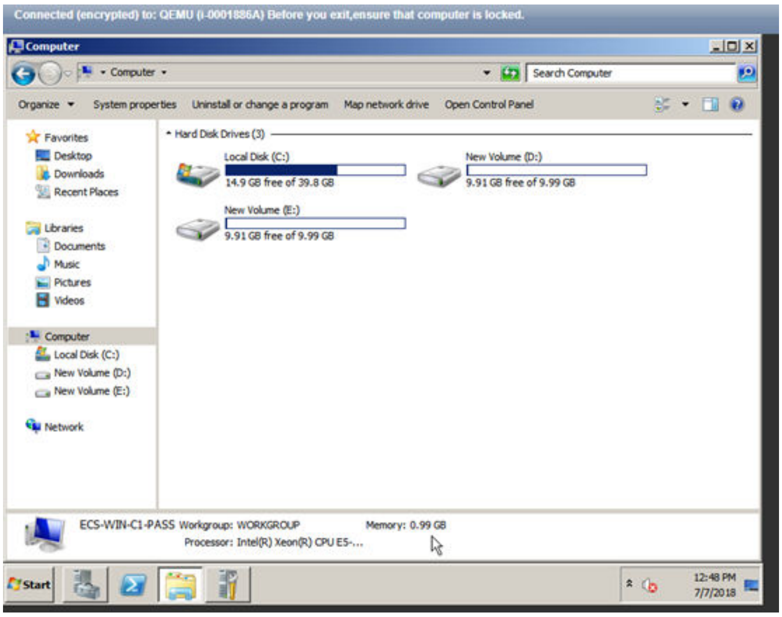
Procedure

1. Check whether the number of disks displayed on the **Computer** page after you modified ECS specifications is the same as the number of disks before you modified ECS specifications.
   - If the numbers are the same, the disks are properly mounted. No further action is required.
   - If the numbers are different, the disks are offline. In this case, go to step 2.

   For example:

   An ECS running Windows Server 2008 has one system disk and two data disks attached before you modified the specifications.

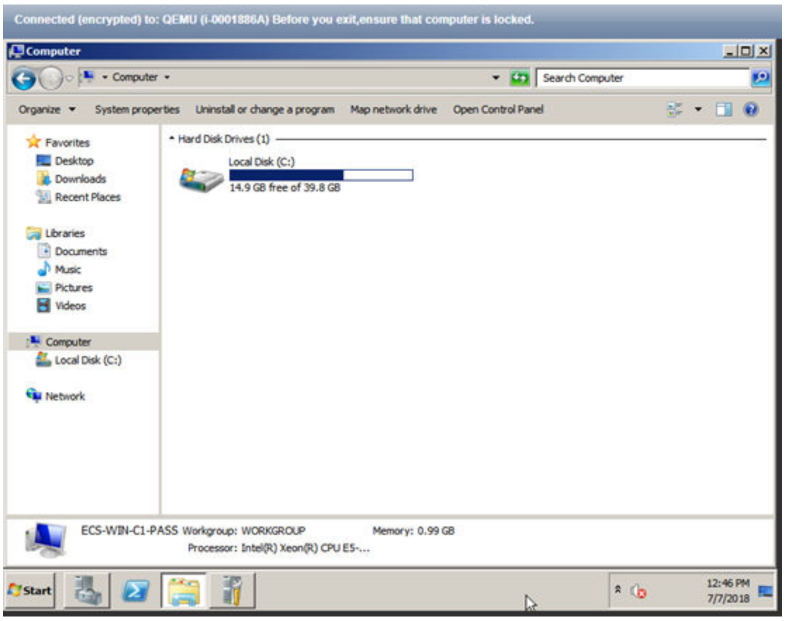
   Figure 19-3 Disks before modifying ECS specifications



Connected (encrypted) to: QEMU (i-0001886A) Before you exit,ensure that computer is locked.

   After the specifications are modified, check the number of disks.

Figure 19-4 Disks after modifying ECS specifications



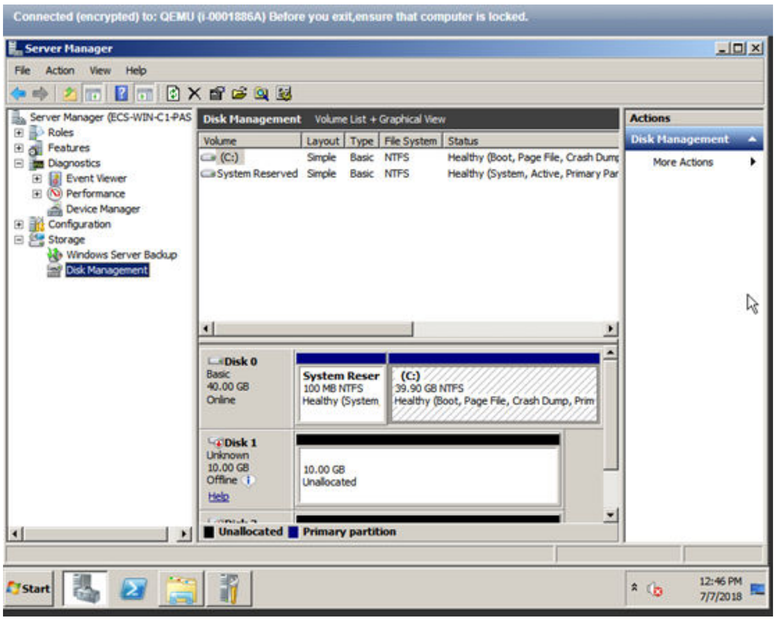
Only one system disk is displayed. The data disks are offline after you modify the specifications.

2. Bring the disks 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.
   b. In the left navigation pane, choose **Storage** > **Disk Management**.

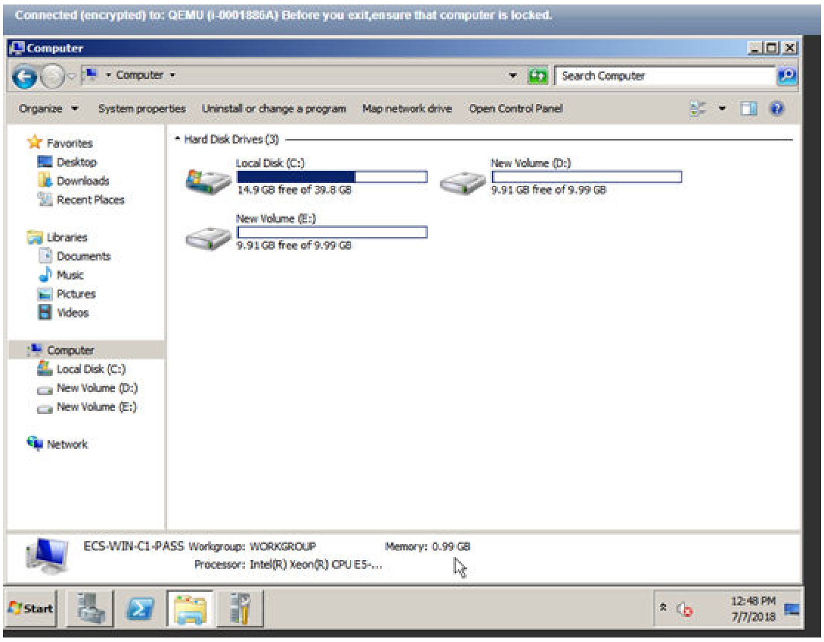
      The **Disk Management** page is displayed.
   c. In the left pane, the disk list is displayed. Right-click the offline disk and choose **Online** from the shortcut menu to bring it online.

Figure 19-5 Bringing the disk online



3. On the **Computer** page, check whether the number of disks after you modified ECS specifications is the same as the number of disks before you modified the ECS specifications.
   - If the numbers are the same, no further action is required.
   - If the numbers are different, contact customer service.

Figure 19-6 Disks after you bring the disks online



Connected (encrypted) to: QEMU (i-0001886A) Before you exit,ensure that computer is locked.

19.6 Why Does the Disk Attachment of a Linux ECS Fail After I Modify the ECS Specifications?

Scenarios

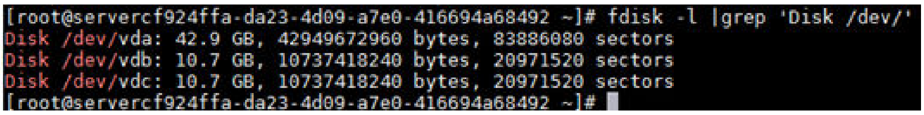
After you modify specifications of a Linux ECS, disk attachment may fail. You need to check the disk attachment after you modify the specifications.

Procedure

1. Log in to the ECS as user **root**.
2. Run the following command to view the disks attached before specifications modification:

   fdisk -l | grep 'Disk /dev/'

   Figure 19-7 Viewing disks attached before specifications modification

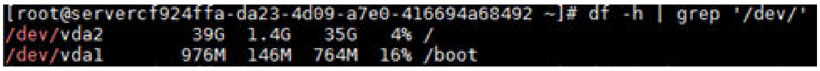
```
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# fdisk -l |grep 'Disk /dev/'
Disk /dev/vda: 42.9 GB, 42949672960 bytes, 83886080 sectors
Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Disk /dev/vdc: 10.7 GB, 10737418240 bytes, 20971520 sectors
[root@servercf924ffa-da23-4d09-a7e0-416694a68492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

   As shown in Figure 19-7, the ECS has three disks attached: **/dev/vda**, **/dev/vdb**, and **/dev/vdc**.

3. Run the following command to view disks attached after specifications modification:

   df -h| grep '/dev/'

   Figure 19-8 Viewing disks attached after specifications modification

```
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# df -h | grep '/dev/'
/dev/vda2         39G  1.4G   35G   4% /
/dev/vda1        976M  146M  764M  16% /boot
```

   As shown in **Figure 19-8**, only one disk **/dev/vda** is attached to the ECS.

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 attachment is successful. No further action is required.
   - If the numbers are different, the disk attachment failed. In this case, go to step **5**.
5. Run the **mount** command to attach the affected disks.

   For example, run the following command:

   mount /dev/vdb1 /mnt/vdb1

   In the preceding command, **/dev/vdb1** is the disk to be attached, and **/mnt/vdb1** is the path for disk attachment.

   NOTICE

   Ensure that **/mnt/vdb1** is empty. Otherwise, the attachment will fail.

   ---

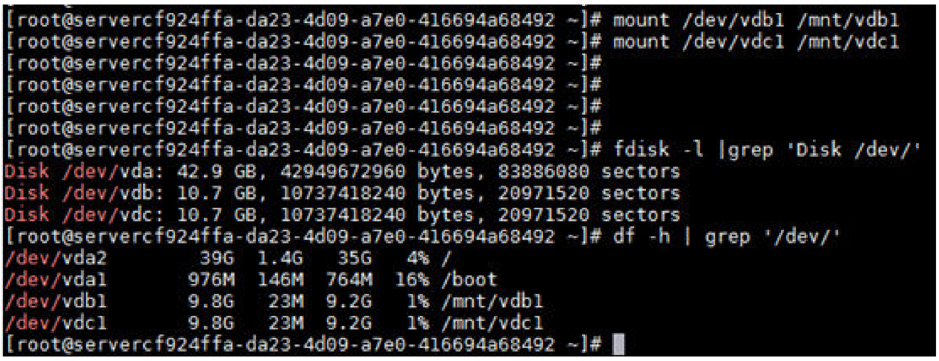
6. Run the following commands to check whether the numbers of disks before and after specifications modifications are the same:

   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 19-9 Checking the number of disks attached

```
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# mount /dev/vdb1 /mnt/vdb1
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# mount /dev/vdc1 /mnt/vdc1
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]#
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]#
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]#
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]#
[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 ~]# df -h | grep '/dev/'
/dev/vda2         39G  1.4G   35G   4% /
/dev/vda1        976M  146M  764M  16% /boot
/dev/vdb1        9.8G   23M  9.2G   1% /mnt/vdb1
/dev/vdc1        9.8G   23M  9.2G   1% /mnt/vdc1
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# 
```

   As shown in **Figure 19-9**, the numbers of disks before and after specifications modifications are the same. The disks are **/dev/vda**, **/dev/vdb**, and **/dev/vdc**.

19.7 What Should I Do If a Blue Screen or Service Exception Occurs After a QingTian ECS Running Windows Is Changed to a KVM ECS?

Symptom

When a QingTian ECS running Windows is changed to a KVM ECS, there may be a blue screen of death (BSOD) of startup failure, with the Windows Boot Manager showing an error status code of 0xc000000f.

Possible Causes

ECSs with different architectures load different protocols and different drivers.

- KVM Windows ECSs load the virtio-blk driver, and the corresponding registry is **Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\viostor**.
- Certain C6 series Windows ECSs load the virtio-scsi driver, and the corresponding registry is **Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\vioscsi**.

Check whether there is the **StartOverride** item in the registry path of the driver.

- If the value of the **REG_DWORD** field is **0**, the ECSs use the driver in this path upon the next startup.
- If the value of the **REG_DWORD** field is not **0**, the ECSs do not use the driver in this path upon the next startup.

When a QingTian Windows ECS is changed to a KVM ECS, if the driver of the corresponding protocol used by the system disk is not loaded, the system disk cannot be identified and the ECS cannot be started.

Solution

Rolling back to the original specifications

Before troubleshooting, you can roll back the target ECS to its original specifications by referring to **Modifying Specifications of Individual ECSs**.

Troubleshooting

After a KVM Windows ECS is rolled back to a QingTian ECS, if you want to change the QingTian ECS to a KVM ECS again, to prevent startup exceptions, do as follows:

1. Make preparations.
    a. Log in to the ECS.
    b. In the **Run** dialog box, enter **regedit** to access the registry editor.
    c. In the registry, locate the following entries:

       Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\vioscsi

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\viostor

Check whether the **StartOverride** item exists.

- If **StartOverride** does not exist and there are only **Enum** and **Parameters** in the directory, no changes need to be made.
- If **StartOverride** exists in the **vioscsi** directory, go to step **1.d**.
- If **StartOverride** exists in the **viostor** directory, go to step **1.e**.

d. Check the **StartOverride** item in the **vioscsi** directory. Change the value of the field whose type is **REG_DWORD** from **0** to **3**. (If the value is already **3**, you do not need to change it.)

e. Check the **StartOverride** item in the **viostor** directory. Change the value of the field whose type is **REG_DWORD** from **3** to **0**. (If the value is already **0**, you do not need to change it.)

f. Restart the ECS.

g. Repeat steps **1.b** to **1.c** to check whether **StartOverride** exists in the registry.

If there are only **Enum** and **Parameters** in the path, the modification is successful.

2. Modify specifications.

Change the Windows ECS specifications to the target specifications.

20 OS Change

20.1 Does OS Change Incur Fees?

Changing an OS is not billed.

After an OS is changed, different images are used and system disk capacity may increase. You will be billed based on the new configurations.

If you change the OS from Linux to Windows, the Windows image is provided and billed by a third party.

For details about the OS change, see **Changing the OS**.

20.2 Can I Install or Upgrade the OS of an ECS?

You can install or upgrade ECS OSs provided on the cloud platform.

- When you create an ECS, you can select a public image or a private image created from a public image to install the ECS OS. Select an OS image based on the programming language in the actual application scenario. For details about image selection, see **Should I Choose Windows OS or Linux OS for My ECS?**
- You can change your ECS OS through the management console, for example, you can upgrade CentOS 7.2 to CentOS 7.3.

20.3 Can I Change the OS of an ECS?

Yes, you can change the OS of an ECS.

If the OS running on an ECS cannot meet service requirements, for example, a higher OS version is required, you can change the ECS OS.

The cloud platform allows you to change the image type (public images, private images, and shared images) and OS. You can change the OS by changing the ECS image.

For instructions about how to change an ECS OS, see **Changing the OS**.

20.4 How Long Does It Take to Change an ECS OS?

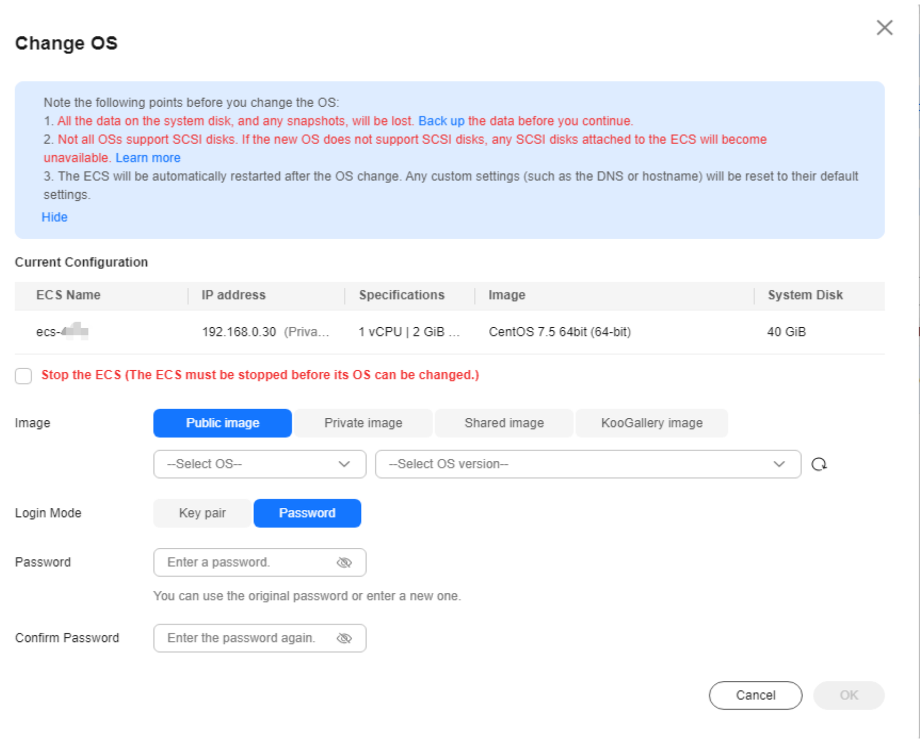
To change an ECS OS, do as follows:

1. Stop the ECS.
2. Choose **More** > **Manage Image** > **Change OS**.

   This operation takes about 1 to 4 minutes.

During this process, the ECS is in **Changing OS** state.

Figure 20-1 Changing an OS



Change OS

Note the following points before you change the OS:
1. All the data on the system disk, and any snapshots, will be lost. Back up the data before you continue.
2. Not all OSs support SCSI disks. If the new OS does not support SCSI disks, any SCSI disks attached to the ECS will become unavailable. Learn more
3. The ECS will be automatically restarted after the OS change. Any custom settings (such as the DNS or hostname) will be reset to their default settings.

Current Configuration

ECS Name	IP address	Specifications	Image	System Disk
ecs-[redacted]	192.168.0.30 (Priva...	1 vCPU | 2 GiB ...	CentOS 7.5 64bit (64-bit)	40 GiB

☐ Stop the ECS (The ECS must be stopped before its OS can be changed.)

Image: Public image

Login Mode: Password

You can use the original password or enter a new one.

20.5 Will I Lose My Disk Data If I Reinstall ECS OS, Change the OS, or Change the ECS Specifications?

Table 20-1 Impact

Item	OS Reinstallation	OS Change	Specifications Modification
Application scenario	Initialize an ECS. The ECS OS remains unchanged after OS change.	Change the OS of an ECS by changing its image. OS change between Windows and Linux is supported only in the Chinese mainland regions. For details about OS change constraints, see **Changing the OS**.	Change ECS specifications, such as increasing the number of vCPUs or adding memory, to meet your service requirements.
Billing	OS reinstallation is free of charge. The ECS price remains unchanged.	OS change is free of charge. However, you will be billed based on your new image type after OS change. . For details, see **Product Price Details**.	Modifying ECS specifications is free of charge. However, you will be billed based on the new specifications after modification. For details, see **Pricing of a Changed Specification**.
IP address	The private IP address, EIP, and MAC address remain unchanged.	The private IP address, EIP, and MAC address remain unchanged.	The private IP address, EIP, and MAC address remain unchanged.
System disk	Reinstalling the OS clears the data in all partitions of the system disk, including the system partition. Back up data before reinstalling the OS.	Changing the OS clears the data in all partitions of the system disk, including the system partition. Back up data before changing the OS.	No impact on system disk.
Data disk	No impact on data disk.	No impact on data disk	No impact on data disk.

Item	OS Reinstallation	OS Change	Specifications Modification
Backup	Back up data before reinstalling the OS to prevent data loss.	Back up data before changing the OS to prevent data loss.	Create a system disk snapshot before modifying ECS specifications to prevent data loss.

20.6 Does OS Reinstallation Incur Fees?

Reinstalling an OS for an ECS allows you to use the original image to reinstall the ECS and does not incur fees.

If you want to use a new OS image, change the OS.

For details, see **Changing the OS**.

20.7 Can I Select Another OS During ECS OS Reinstallation?

No. You can only use the original image of the ECS to reinstall the OS.

If you want to use a new OS image, change the OS.

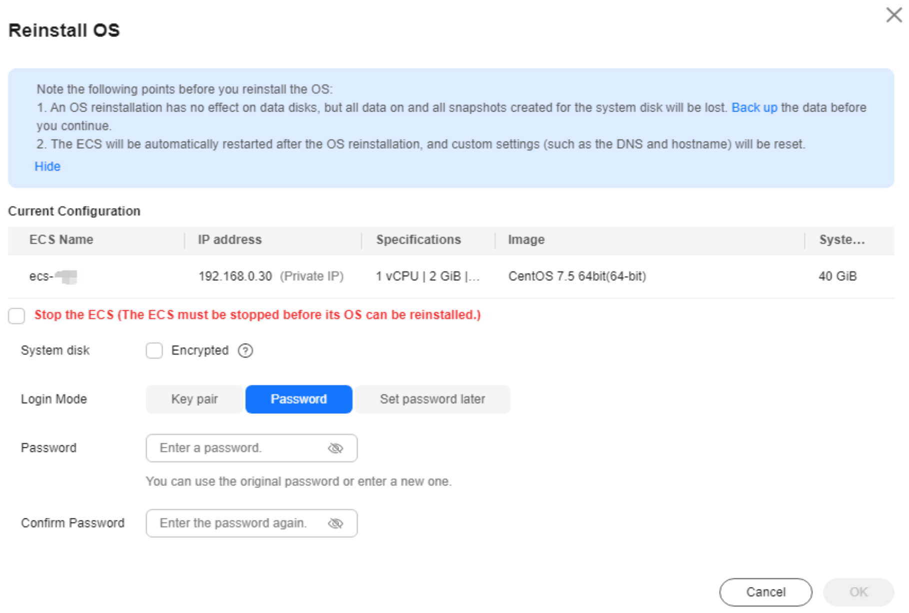
For details, see **Changing the OS**.

20.8 How Long Does It Take to Reinstall an ECS OS?

Generally, the process of reinstalling the OS of an ECS takes about 1 to 2 minutes to complete. On the ECS console, stop the ECS and choose **More** > **Manage Image** > **Reinstall OS** in the **Operation** column.

During this process, the ECS is in **Reinstalling OS** state.

Figure 20-2 Reinstalling an OS



Reinstall OS

Note the following points before you reinstall the OS:
1. An OS reinstallation has no effect on data disks, but all data on and all snapshots created for the system disk will be lost. Back up the data before you continue.
2. The ECS will be automatically restarted after the OS reinstallation, and custom settings (such as the DNS and hostname) will be reset.

Current Configuration

ECS Name	IP address	Specifications	Image	Syste...
ecs-[redacted]	192.168.0.30 (Private IP)	1 vCPU | 2 GiB |...	CentOS 7.5 64bit(64-bit)	40 GiB

☐ Stop the ECS (The ECS must be stopped before its OS can be reinstalled.)

System disk ☐ Encrypted

Login Mode: Password

Password: Enter a password.

You can use the original password or enter a new one.

Confirm Password: Enter the password again.

21 ECS Security Check

21.1 How Does an ECS Defend Against DDoS Attacks?

What Is a DDoS Attack?

Denial of Service (DoS) attacks, also known as flood attacks, intend to exhaust the network or system resources on the target computer, causing service interruption or suspension. Consequently, legitimate users fail to access network services. When an attacker uses multiple compromised computers on the network as attack machines to launch DoS attacks to specific targets, the attacks are called Distributed Denial of Service (DDoS) attacks.

What Is Anti-DDoS?

Anti-DDoS defends ECSs against DDoS attacks and sends real time alarms when detecting attacks. In addition, Anti-DDoS improves the bandwidth utilization to further safeguard your services.

Anti-DDoS monitors the service traffic from the Internet to public IP addresses and detects attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting service running. It also generates monitoring reports that provide visibility into the security of network traffic.

Anti-DDoS

Anti-DDoS defends ECSs against DDoS attacks and sends real time alarms when detecting attacks. In addition, Anti-DDoS improves the bandwidth utilization to further safeguard your services.

Anti-DDoS monitors the service traffic from the Internet to public IP addresses and detects attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting service running. It also generates monitoring reports that provide visibility into the security of network traffic.

Anti-DDoS helps you mitigate the following attacks:

- Web server attacks

Include SYN flood, HTTP flood, Challenge Collapsar (CC), and low-rate attacks

- Game attacks

  Include User Datagram Protocol (UDP) flood, SYN flood, TCP-based, and fragmentation attacks
- HTTPS server attacks

  Include SSL DoS and DDoS attacks
- DNS server attacks

  Include attacks exploiting DNS protocol stack vulnerabilities, DNS reflection attacks, DNS flood attacks, and DNS cache miss attacks

Anti-DDoS also provides the following functions:

- Monitors a single EIP and offers a monitoring report, covering the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.
- Provides attack statistics reports on all protected EIPs, covering the traffic scrubbing frequency, scrubbed traffic amount, top 10 attacked EIPs, and number of blocked attacks.

21.2 Are ECSs with Simple Passwords Easily Attacked?

It is recommended that your password contain 8 to 26 characters that consists of digits, uppercase and lowercase letters, and special characters. It is a good practice to download virtualization antivirus products and host security hardening products from Huawei Cloud KooGallery and install them on your ECSs to enhance security.

If your ECS has been intruded, contact customer service for technical support.

Table 21-1 Password complexity requirements

Password complexity requirements	ECS Creation	Password Reset
Length	Must contain 8 to 26 characters.	Must contain 8 to 26 characters.
Characters	Must contain at least three of the supported four character types.	Must contain at least three of the supported four character types.
Security	• Cannot contain the username or the username spelled backwards. • Cannot contain more than two consecutive characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)	• Cannot contain the username or the username spelled backwards. • Cannot contain more than two consecutive characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)

Password complexity requirements	ECS Creation	Password Reset
Other	None	Cannot start with a slash (/) for Windows ECSs.
Supported Characters	Uppercase letters	Uppercase letters
	Lowercase letters	Lowercase letters
	Digits	Digits
	• Special characters for Linux ECSs: !@$%^-_=+[{}]:,./?~#* • Special characters for Windows ECSs: !@$%^-_=+[{()}]:,./?~#*	• Online password reset: @%-_=+[]:./^,{}? (only applied to Linux) $@%-_=+[]:./,? (only applied to Windows) • Offline password reset: Special characters for Linux ECSs: !@%-_=+[]:./? Special characters for Windows ECSs: !@%-_=+[]:./?

21.3 How Is ECS Security Ensured?

Host Security Service (HSS) helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

After installing the HSS agent on your ECSs, you will be able to check the ECS security status and risks in a region on the HSS console.

If you use a public image to create an ECS, protection is enabled by default for your ECS. Its basic edition is free of charge. HSS automatically installs an agent on the ECS and protects the security of the ECS.

How Do I Use HSS?

21.4 How Can I Disable Operation Protection?

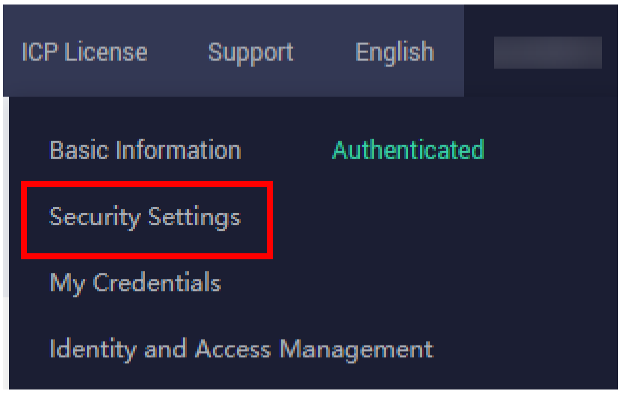
Symptom

When I perform critical operations on my ECS with operation protection enabled, for example, deleting my ECS or modifying ECS specifications, I have to enter the password and verification code for authentication. To disable operation protection, perform the operations described in this section.

Procedure

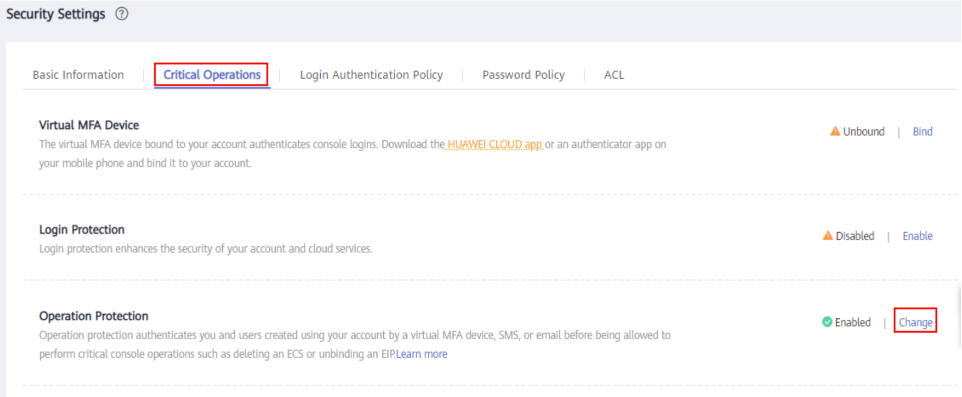
1. Log in to the management console.
2. Move the cursor to the username in the upper right corner of the page and select **Security Settings** from the drop-down list.

Figure 21-1 Security Settings



3. On the **Security Settings** page, choose **Critical Operations** > **Operation Protection** > **Change**.

Figure 21-2 Modifying operation protection settings



Virtual MFA Device

The virtual MFA device bound to your account authenticates console logins. Download the HUAWEI CLOUD app or an authenticator app on your mobile phone and bind it to your account.

Login Protection

Login protection enhances the security of your account and cloud services.

Operation Protection

Operation protection authenticates you and users created using your account by a virtual MFA device, SMS, or email before being allowed to perform critical console operations such as deleting an ECS or unbinding an EIP.Learn more

4. On the **Operation Protection** page, select **Disable** and click **OK**.

22 Resource Management and Tag

22.1 How Can I Create and Delete Tags and Search for ECSs by Tag?

Creating a Tag

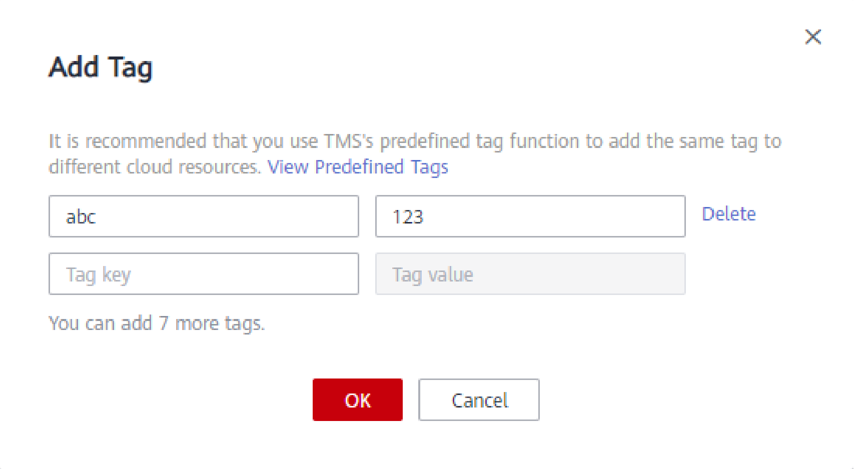
1. Log in to the **management console**.
2. Select the region where the ECS is located.
3. Under **Compute**, click **Elastic Cloud Server**.
4. Click the name of the target ECS.

   The ECS details page is displayed.
5. Click **Tags** and then **Add Tag**.
6. Enter the tag key and value, and click **OK**.

   NOTE

   If your organization has created a tag policy for ECS, you need to add tags for ECS based on the tag policy. If a tag does not comply with the tag rules, the creation may fail. Contact the organization administrator to learn details about the tag policy.

   Figure 22-1 Adding tags



Add Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View Predefined Tags

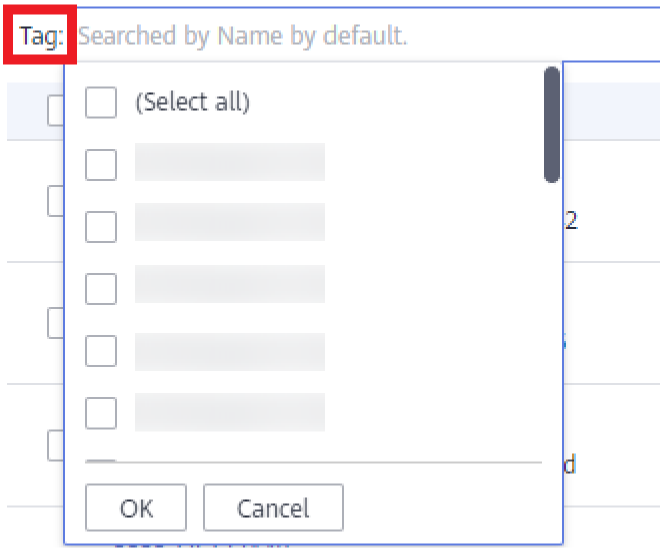
abc 123

You can add 7 more tags.

Searching for ECSs by Tag

1. Log in to the **management console**.
2. Select the region where the ECS is located.
3. On the **Elastic Cloud Server** page, search for ECSs by tag.

Figure 22-2 Searching for ECSs by tag

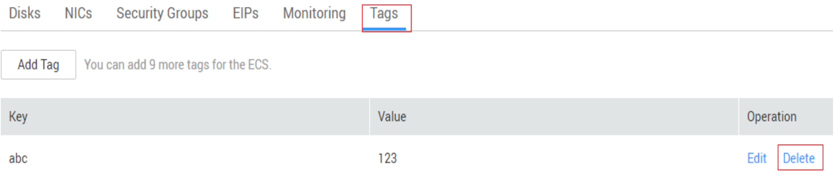


4. In the search bar, choose **Tag** and then select the tag key and value, and click **OK**.

Deleting a Tag

1. Log in to the **management console**.
2. Select the region where the ECS is located.
3. Click **Elastic Cloud Server**.
4. Click the name of the target ECS.
5. On the page providing details about the ECS, click **Tags**, locate the row containing the target tag, and click **Delete** in the **Operation** column.

Figure 22-3 Deleting a tag



You can add 9 more tags for the ECS.

Key	Value	Operation
abc	123	Edit Delete

23 Image Source Management

23.1 How Can I Use a PyPI Image Source (x86_64 or Kunpeng) Provided by Huawei Cloud?

Scenarios

When updating the OS or software of an ECS, you can access the Internet through the ECS and use an external PyPI image source. However, if your ECS cannot access the Internet, or the external PyPI image source cannot provide services stably, you can use the PyPI image source provided by Huawei Cloud.

Constraints

- This section applies only to the following regions: CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN-Hong Kong.
- The operations described in this section apply to both x86_64 and Kunpeng ECSs.
- You have configured the intranet DNS server provided by Huawei Cloud.

  To obtain the intranet DNS server address, see **What Are Huawei Cloud Private DNS Server Addresses?**

  For instructions about how to configure a DNS server, see **How Do I Configure DNS for an ECS?**.

Procedure

1. Log in to the ECS as user **root** or **Administrator**.
2. Run the following commands to create the **pip.conf** configuration file:

   mkdir ~/.pip

   touch ~/.pip/pip.conf
3. Modify the **pip.conf** configuration file as follows:
   ```
   [global]
   index-url = http://mirrors.myhuaweicloud.com/pypi/web/simple
   format = columns
   ```

```
[install]
trusted-host=mirrors.myhuaweicloud.com
```

NOTE

If certain packages are unavailable, this issue may be caused by in-progress data synchronization. In such a case, try again several hours later.

23.2 What Can I Do If the Download Speed Is Slow After the yum makecache Command Is Executed?

Symptom

After the **yum makecache** command is executed to create a local cache, the download speed becomes slow.

Solution

Configure the EPEL source.

- **Learn what is EPEL source.**
- EPEL repository: https://repo.huaweicloud.com/epel/

Constraints

The operations described in this section apply to x86_64 ECSs.

Procedure

1. Run the following commands to back up configuration files:

   cp -a /etc/yum.repos.d/epel.repo /etc/yum.repos.d/epel.repo.backup

   mv /etc/yum.repos.d/epel-testing.repo /etc/yum.repos.d/epel-testing.repo.backup
2. Modify the **epel.repo** file.

   Run the following commands to uncomment the line starting with **baseurl**, comment out the lines starting with **mirrorlist**, and replace **http://download.fedoraproject.org/pub** in the file with **https://repo.huaweicloud.com**, respectively:

   sed -i "s/#baseurl/baseurl/g" /etc/yum.repos.d/epel.repo

   sed -i "s/metalink/#metalink/g" /etc/yum.repos.d/epel.repo

   sed -i "s@http://download.fedoraproject.org/pub@https://repo.huaweicloud.com@g" /etc/yum.repos.d/epel.repo
3. Run the **yum update** command to update the software list.

NOTE

- After you execute the **yum makecache** command, if the system displays the message "Another app is currently holding the yum lock", run the **rm -rf /var/run/yum.pid** command to delete the **yum.pid** file. Then, run the **yum makecache** command again to generate the cache.
- After you execute the **yum makecache** command, if the system displays the message "Error: Cannot retrieve metalink for repository: epel. Please verify its path and try again", run the following command to update the certificate and temporarily disable the EPEL image source:

  yum --disablerepo=epel -y update ca-certificates
- If certain packages are unavailable, this issue may be caused by in-progress data synchronization. In this case, try again after a few hours.

24 Internet Access Failures

24.1 Why Cannot My Windows ECS Access the Internet?

Symptom

Your attempt to access the Internet from your Windows ECS failed.

Fault Locating

The following fault causes are sequenced based on their occurrence probability.

If the fault persists after you have ruled out a cause, check other causes.

Table 24-1 Possible causes and solutions

Possible Cause	Solution
The ECS is frozen or stopped, or has no EIP bound.	Check whether the ECS is in **Running** state and has an EIP bound. For details, see **Checking the ECS Status**.
The ECS is overloaded.	Check whether the bandwidth and vCPU usage of the ECS are too high. For details, see **Checking Whether the ECS Is Overloaded**.
The EIP bandwidth exceeds the limit.	Increase the bandwidth and try again. For details, see **Checking Whether the EIP Bandwidth Exceeded the Limit**.
The access is blocked by the ISP.	Check whether you can access the ECS using another hotspot or network. For details, see **Checking Whether the ISP Network Is Functional**.
The network configuration on the ECS is incorrect.	Check whether the NIC and DNS configurations are correct. For details, see **Checking the NIC Configuration**.

Possible Cause	Solution
Routing is incorrectly configured.	Check whether the default route of 0.0.0.0 designates to the default gateway. For details, see **Checking Whether the Default Route Is Destined for the Default Gateway**.
The security group is incorrectly configured.	Check whether the security group allows the network traffic in the outbound direction. For details, see **Checking Whether the Security Group Is Correctly Configured**.
A network ACL has been associated with the ECS.	Disassociate the network ACL with the ECS and try again. For details, see **Checking ACL Rules**.
The website you want to visit is outside the Chinese mainland.	Optimize the website link configurations and try again. For details, see **Checking Whether the Website to Be Visited Is Outside the Chinese Mainland**. If the fault persists, use an ECS purchased in a region outside the Chinese mainland to access the website.
The EIP is blocked.	If the EIP is blocked, the ECS cannot access the Internet. For details, see **Checking Whether the EIP Is Blocked**.
The access is blocked by the firewall.	Disable the firewall and try again. For details, see **Checking the Firewall Configuration**.
The gateway is inaccessible.	Run the **ping** command to check whether the DNS server is running properly. For details, see **Checking Whether the Gateway Is Accessible**.
The ECS performance cannot meet service requirements.	Run the **netstat** command to check the network connection status. For details, see **Checking the ECS Performance**.
The access is blocked by third-party antivirus software.	Disable or uninstall the third-party antivirus software and try again. For details, see **Checking Whether the Access Is Blocked by Antivirus Software**.
The ECS has been attacked by viruses or Trojan horses.	Check whether the ECS is affected by viruses or Trojan horses. For details, see **Checking the ECS Security Status**.

Checking the ECS Status

- Check whether the ECS is in the **Running** state on the management console.
- Check whether an ECS has an EIP bound.

  An ECS can access the Internet only if it has an EIP bound.

  For details about how to bind an EIP to the ECS, see **Assigning an EIP**.

Checking Whether the ECS Is Overloaded

If the bandwidth and CPU usage of an ECS are too high, the network may be disconnected.

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

To resolve this issue, perform the operations described in **Why Is My Windows ECS Running Slowly?**

Checking Whether the EIP Bandwidth Exceeded the Limit

An ECS with an EIP bound accesses the Internet using the bandwidth configured for the EIP.

If Internet access fails, check whether the EIP bandwidth exceeds the limit.

Check whether the bandwidth exceeds the configured bandwidth size. For details, see **How Do I Know If My EIP Bandwidth Limit Has Been Exceeded?**

If the bandwidth exceeds the limit, increase the bandwidth. For details, see **Changing an EIP Bandwidth**.

Checking Whether the ISP Network Is Functional

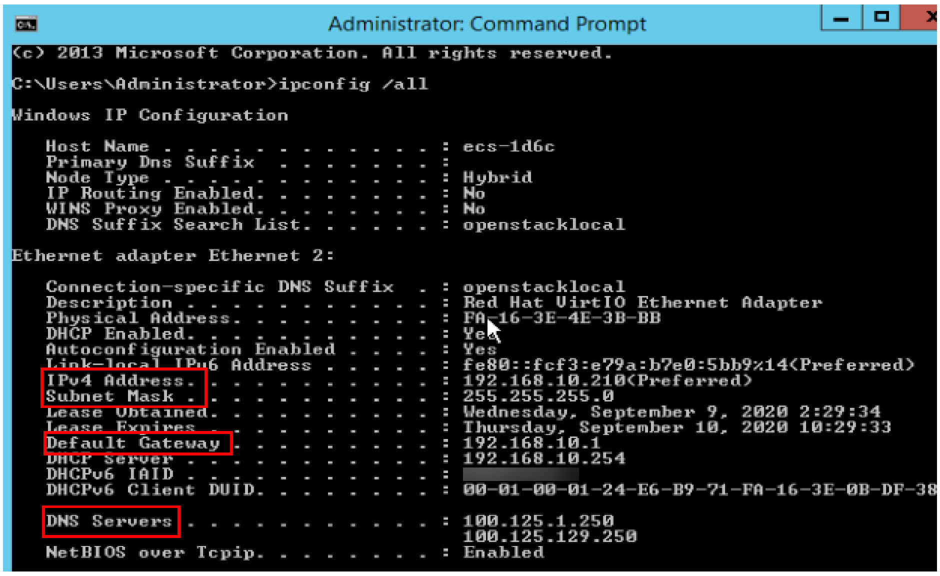
Check whether the fault occurs for a specific IP address. If so, the IP address may be blocked by the ISP.

Try another hotspot for access. If the access is successful, the fault may lie in the local carrier network. Contact the carrier to resolve this issue.

Checking the NIC Configuration

- Check whether the NIC and DNS configurations on the ECS are consistent with those displayed on the ECS management console.
    a. On the CLI of the ECS, run the **ipconfig /all** command to check whether the NIC and DNS configurations are correct, as shown in **Figure 24-1**.

Figure 24-1 NIC and DNS configurations

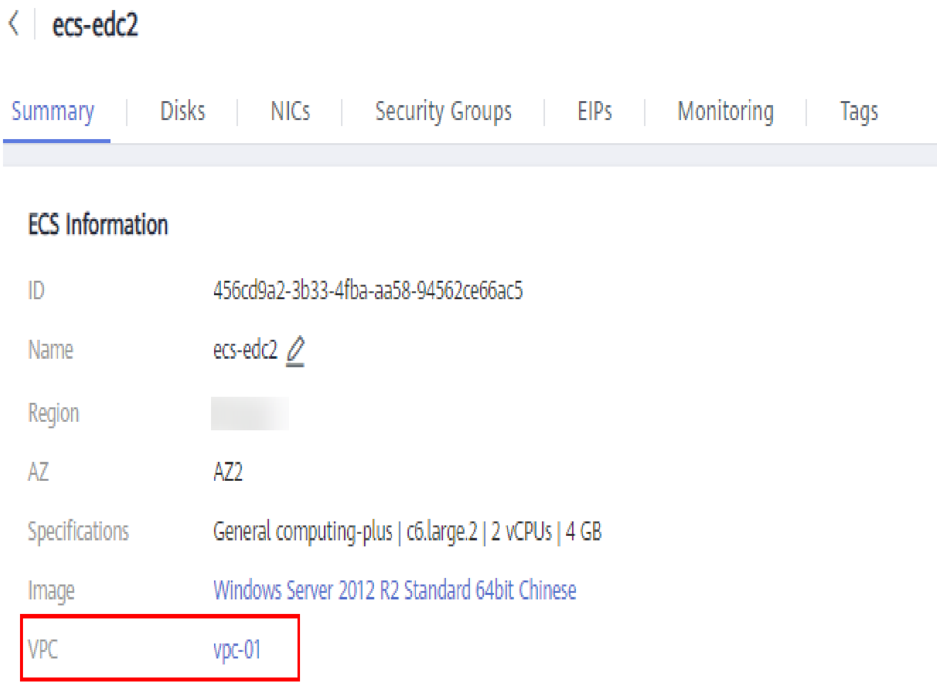


```
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : ecs-1d6c
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : openstacklocal

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : openstacklocal
   Description . . . . . . . . . . . : Red Hat VirtIO Ethernet Adapter
   Physical Address. . . . . . . . . : FA-16-3E-4E-3B-BB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::fcf3:e79a:b7e0:5bb9%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.210(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, September 9, 2020 2:29:34
   Lease Expires . . . . . . . . . . : Thursday, September 10, 2020 10:29:33
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.254
   DHCPv6 IAID . . . . . . . . . . . : [redacted]
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-E6-B9-71-FA-16-3E-0B-DF-38

   DNS Servers . . . . . . . . . . . : 100.125.1.250
                                       100.125.129.250
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

b. Log in to the management console. On the ECS list page, click the name of the target ECS.

c. On the page providing details about the ECS, click the VPC name.

Figure 24-2 VPC name on the ECS details page



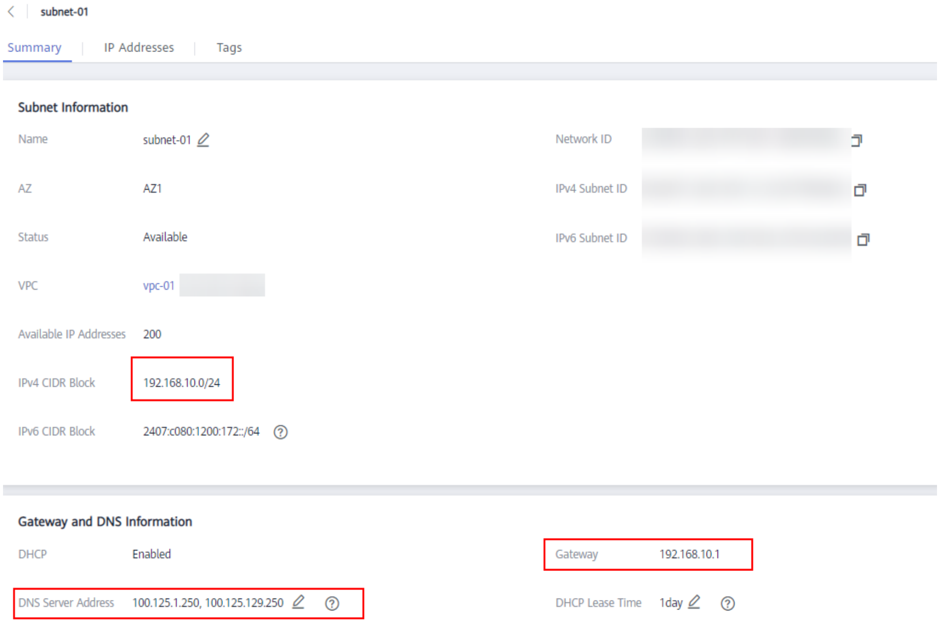
ECS Information

ID 456cd9a2-3b33-4fba-aa58-94562ce66ac5
Name ecs-edc2
Region [redacted]
AZ AZ2
Specifications General computing-plus | c6.large.2 | 2 vCPUs | 4 GB
Image Windows Server 2012 R2 Standard 64bit Chinese
VPC vpc-01

d. On the VPC list page, click the number displayed in the **Subnets** column.

e. On the subnet list page, click the name of the target subnet. The subnet details page is displayed , as shown in **Figure 24-3**.

Figure 24-3 Subnet details



Subnet Information

Name subnet-01

AZ AZ1

Status Available

VPC vpc-01 [redacted]

Available IP Addresses 200

IPv4 CIDR Block 192.168.10.0/24

IPv6 CIDR Block 2407:c080:1200:172::/64

Network ID [redacted]

IPv4 Subnet ID [redacted]

IPv6 Subnet ID [redacted]

Gateway and DNS Information

DHCP Enabled

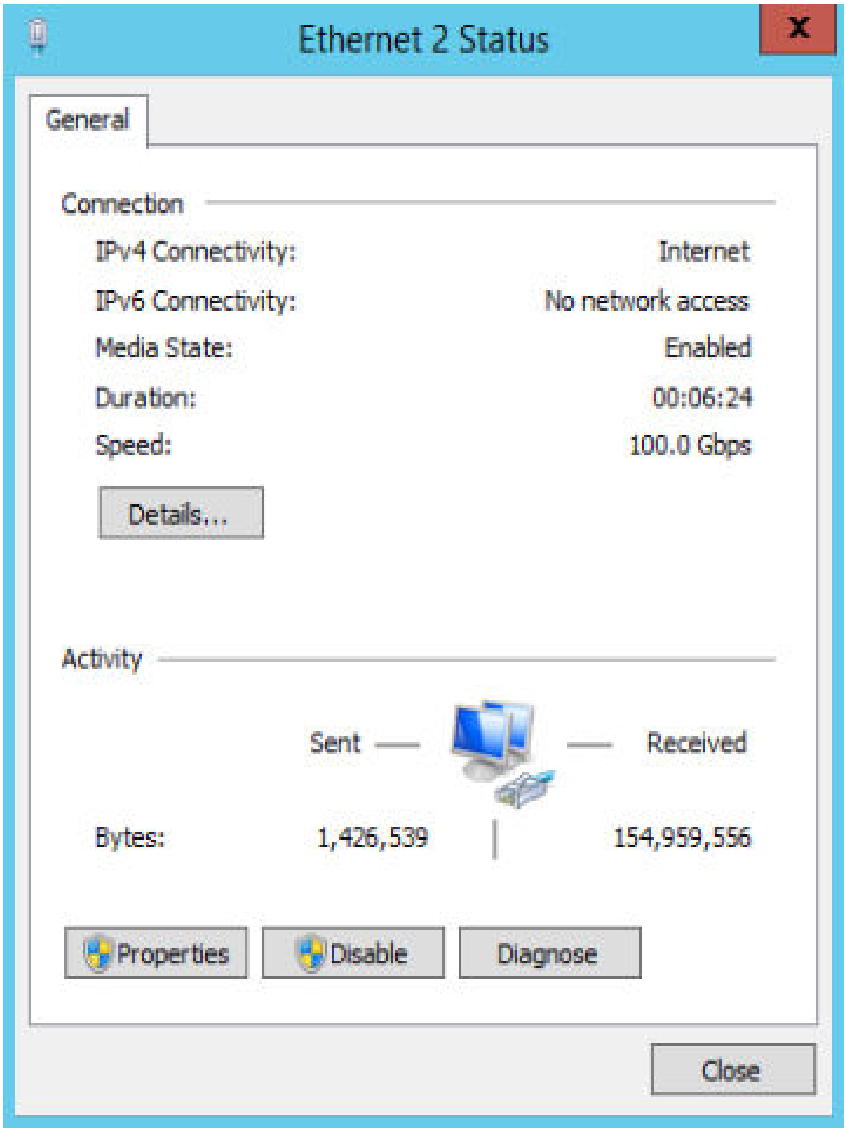
Gateway 192.168.10.1

DNS Server Address 100.125.1.250, 100.125.129.250

DHCP Lease Time 1day

- Open the **cmd** window, run the **ncpa.cpl** command to start Network and Sharing Center, and check whether the NIC is functional.

Figure 24-4 NIC status



Ethernet 2 Status

General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	00:06:24
Speed:	100.0 Gbps

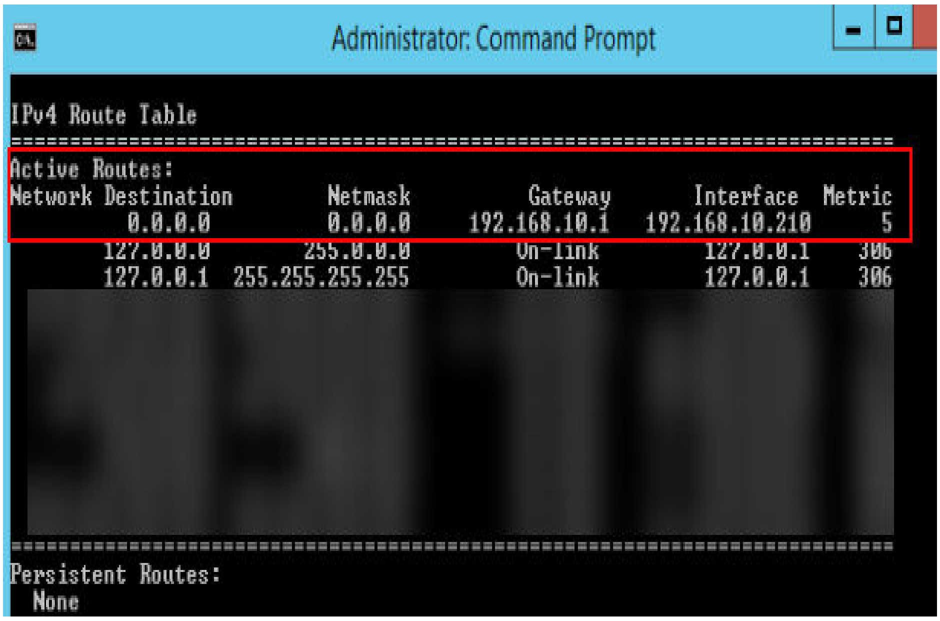
Activity

	Sent	Received
Bytes:	1,426,539	154,959,556

Checking Whether the Default Route Is Destined for the Default Gateway

Run the **route print** command to obtain the routing table of the ECS and check whether the default route of 0.0.0.0 is destined for the default gateway.

Figure 24-5 Default route settings



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1  192.168.10.210      5
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    306
[redacted]
===========================================================================
Persistent Routes:
  None
```

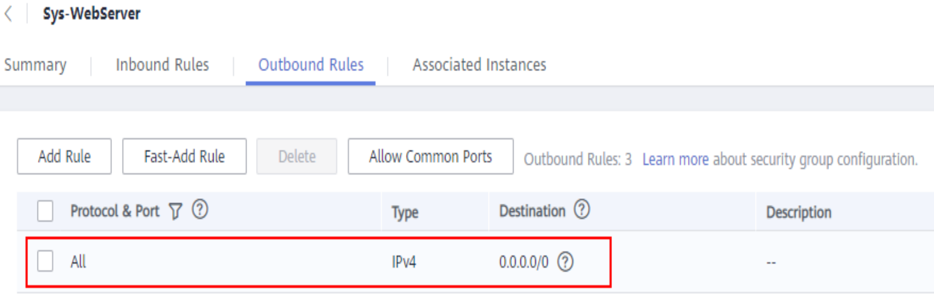
Checking Whether the Security Group Is Correctly Configured

Check whether the security group of the ECS is correctly configured. If an allowlist is configured for the outbound rules of the security group, the network traffic in the outbound direction is permitted.

As shown in **Figure 24-6**, all network traffic in the outbound direction is permitted.

For instructions about how to permit a protocol or port, see **Configuring Security Group Rules**.

Figure 24-6 Permitting all network traffic in the outbound direction



Outbound Rules: 3 Learn more about security group configuration.

☐	Protocol & Port	Type	Destination	Description
☐	All	IPv4	0.0.0.0/0	--

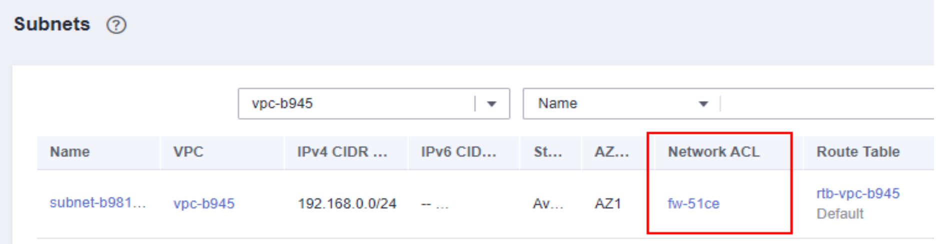
Checking ACL Rules

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

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

   If an ACL name is displayed, the network ACL has been associated with the ECS.

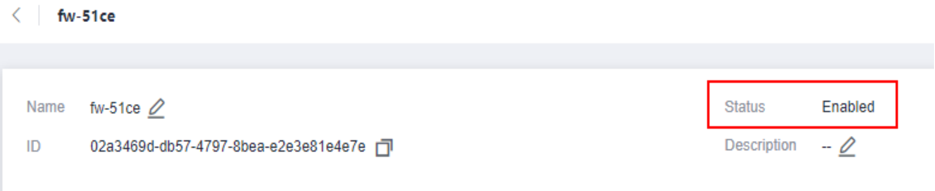
Figure 24-7 Network ACL



Name	VPC	IPv4 CIDR ...	IPv6 CID...	St...	AZ...	Network ACL	Route Table
subnet-b981...	vpc-b945	192.168.0.0/24	-- ...	Av...	AZ1	fw-51ce	rtb-vpc-b945 Default

2. Click the ACL name to view its status.

Figure 24-8 Enabled network ACL

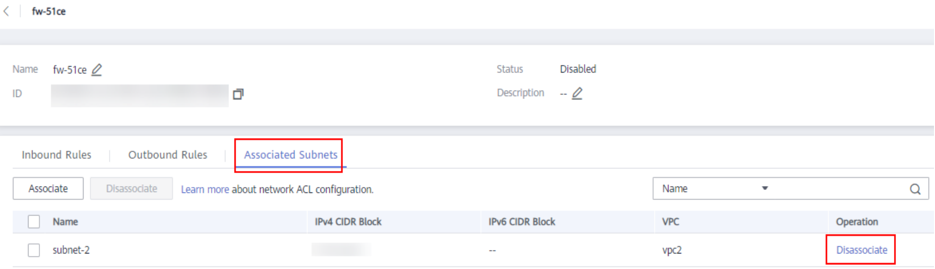


Name fw-51ce
ID 02a3469d-db57-4797-8bea-e2e3e81e4e7e
Status Enabled
Description --

3. Disassociate the network ACL from the subnet of the ECS.

   On the page providing details about the network ACL, choose **Associated Subnets** > **Disassociate**.

Figure 24-9 Disassociating a network ACL



Name fw-51ce
ID [redacted]
Status Disabled
Description --

Name	IPv4 CIDR Block	IPv6 CIDR Block	VPC	Operation
subnet-2	[redacted]	--	vpc2	Disassociate

NOTE

The default network ACL rule denies all incoming and outgoing packets. If a network ACL is disabled, the default rule is still effective.

4. Try to access the Internet through the ECS again.

Checking Whether the Website to Be Visited Is Outside the Chinese Mainland

Websites outside the Chinese mainland may not be accessible or respond slowly when you access them through an ECS. This is caused by the slow access of a DNS server outside the Chinese mainland.

NOTE

If you intend to access websites outside the Chinese mainland, select a region according to the website when purchasing an ECS.

To speed up the access to a website outside the Chinese mainland, see **Why Accessing a Website Outside the Chinese Mainland Is Slow on an ECS?**

Checking Whether the EIP Is Blocked

IP address blocking indicates that all traffic is destined to a null route. If the EIP is blocked, the ECS cannot access the Internet.

Generally, blocked EIPs will be automatically unblocked after 24 hours if no subsequent attack occurs.

It is recommended that you use **Advanced Anti-DDoS (AAD)** to prevent attacks.

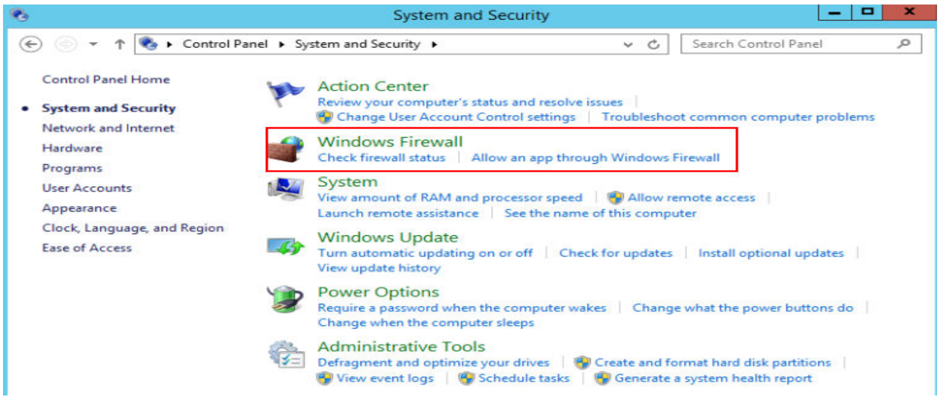
Checking the Firewall Configuration

Disable firewall rules for the ECS and check whether the Internet connection is restored.

If the connection is restored, check the firewall settings.

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

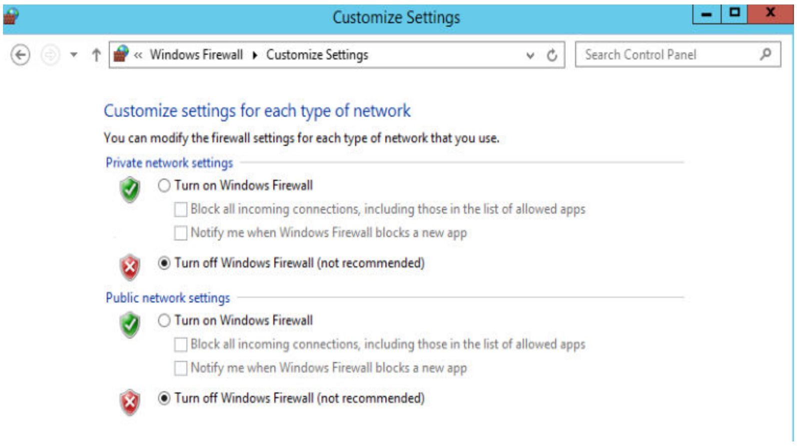
Figure 24-10 Windows Firewall


System and Security
Control Panel ▸ System and Security ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware
Programs
User Accounts
Appearance
Clock, Language, and Region
Ease of Access
Action Center
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Windows Update
Turn automatic updating on or off
Check for updates
Install optional updates
View update history
Power Options
Require a password when the computer wakes
Change what the power buttons do
Change when the computer sleeps
Administrative Tools
Defragment and optimize your drives
Create and format hard disk partitions
View event logs
Schedule tasks
Generate a system health report

3. Click **Check firewall status** and select **Turn on Windows Firewall** or **Turn off Windows Firewall**.

   View and set the firewall status.

Figure 24-11 Turning off a firewall



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☐ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Public network settings

○ Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☐ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Checking Whether the Gateway Is Accessible

1. Run the **ping** command to check whether data can be exchanged between the ECS and the gateway.

   Use an IP address in a different network segment to ping the gateway to check network connections.

2. Run the **ping** command to obtain the IP address of the DNS server.

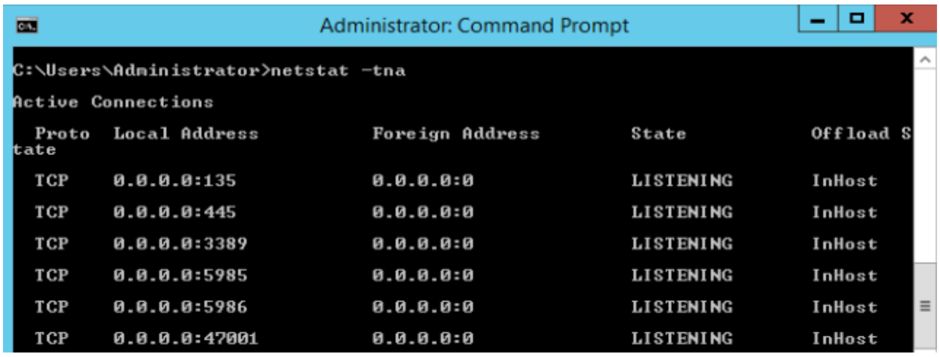
   Compare the time required for pinging the DNS server and the time for pinging a specific IP address, and determine whether the DNS server is running properly.

Checking the ECS Performance

Run the **netstat** command to check whether SYN-SENT, CLOSE_WAIT, or FIN_WAIT is found.

If any of them is found, port resources are used up. This issue is generally caused by a software bug. After the bug is fixed, restart the ECS.

Figure 24-12 Checking network connection



```
C:\Users\Administrator>netstat -tna

Active Connections

  Proto  Local Address          Foreign Address        State           Offload S
tate
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:5986           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       InHost
```

Checking Whether the Access Is Blocked by Antivirus Software

Disable or uninstall the third-party antivirus software on the ECS, and check whether the fault is rectified.

Checking the ECS Security Status

Check the ECS security status and determine whether the ECS is affected by viruses or Trojan horses.

24.2 Why Does My Linux ECS Fail to Access the Internet?

Symptom

Your attempt to access the Internet from your Linux ECS failed.

Fault Locating

The following fault causes are sequenced based on their occurrence probability.

If the fault persists after you have ruled out a cause, check other causes.

Table 24-2 Possible causes and solutions

Possible Cause	Solution
The ECS is frozen or stopped, or has no EIP bound.	Check whether the ECS is in **Running** state and has an EIP bound. For details, see **Checking the ECS Status**.
The ECS is overloaded.	Check whether the bandwidth and vCPU usage of the ECS are too high. For details, see **Checking Whether the ECS Is Overloaded**.
The EIP bandwidth exceeds the limit.	Increase the bandwidth and try again. For details, see **Checking Whether the EIP Bandwidth Exceeded the Limit**.
The DNS configuration is incorrect.	Change the DNS server to a private one. For details, see **Checking the DNS Configuration**.
Specified resolution has been configured in the hosts file.	Check whether the mappings in the hosts configuration file are correct. For details, see **Checking the hosts Configuration File**.
Both Network and NetworkManager are enabled.	Use either of the two tools to prevent incompatibility issues. For details, see **Checking Whether Both Network and NetworkManager Have Been Enabled**.
The security group is incorrectly configured.	Check whether the security group allows the network traffic in the outbound direction. For details, see **Checking Whether the Security Group Is Correctly Configured**.

Possible Cause	Solution
A network ACL has been associated with the ECS.	Disassociate the network ACL with the ECS and try again. For details, see **Checking ACL Rules**.
The website you want to visit is outside the Chinese mainland.	Optimize the website link configurations and try again. For details, see **Checking Whether the Website to Be Visited Is Outside the Chinese Mainland**. If the fault persists, use an ECS purchased in a region outside the Chinese mainland to access the website.
The EIP is blocked.	If the EIP is blocked, the ECS cannot access the Internet. For details, see **Checking Whether the EIP Is Blocked**.
The private IP address is lost.	Check whether the **dhclient** process is running. If it is not running, the private IP address may be lost. For details, see **Checking Whether a Private IP Address Can Be Obtained**.
NICs are incorrectly configured.	Check whether the NIC and DNS configurations are correct. For details, see **Checking the NIC Configuration**.
Firewall is enabled on the ECS.	Disable the firewall and try again. For details, see **Checking the Firewall Configuration**.

Checking the ECS Status

- Check whether the ECS is in the **Running** state on the management console.
- Check whether an ECS has an EIP bound.

  An ECS can access the Internet only if it has an EIP bound.

  For details about how to bind an EIP to the ECS, see **Assigning an EIP**.

Checking Whether the ECS Is Overloaded

If the bandwidth and CPU usage of an ECS are too high, the network may be disconnected.

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

To resolve this issue, perform the operations described in **Why Is My Linux ECS Running Slowly?**

Checking Whether the EIP Bandwidth Exceeded the Limit

An ECS with an EIP bound accesses the Internet using the bandwidth configured for the EIP.

If Internet access fails, check whether the EIP bandwidth exceeds the limit.

Check whether the bandwidth exceeds the configured bandwidth size. For details, see **How Do I Know If My EIP Bandwidth Limit Has Been Exceeded?**

If the bandwidth exceeds the limit, increase the bandwidth. For details, see **Changing an EIP Bandwidth**.

Checking the DNS Configuration

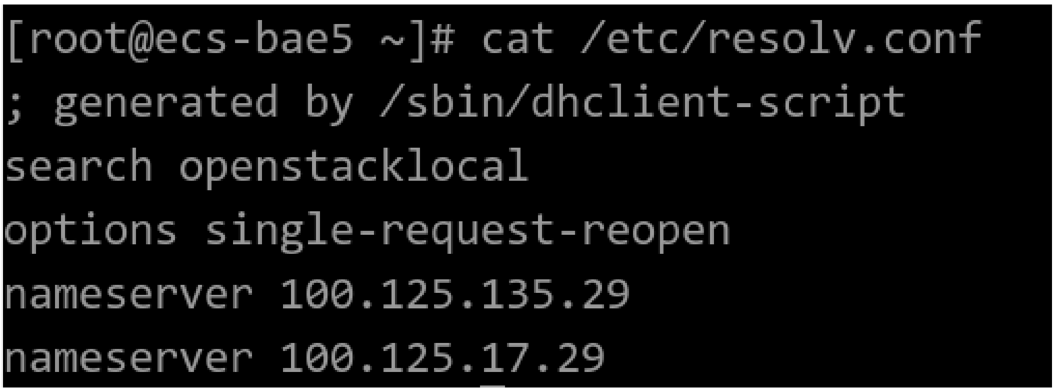
Private DNS servers resolve domain names for the ECSs created using a public image by default. The private DNS servers do not affect the domain name resolution for the ECSs to access the Internet. Additionally, you can use the private DNS servers to directly access the internal addresses of other cloud services, such as OBS. Compared with the access through the Internet, this access mode features high performance and low latency.

For Linux ECSs, run the following command to check the DNS configuration:

cat /etc/resolv.conf

If the command output shown in **Figure 24-13** is displayed, the domain name is resolved using the private DNS server.

Figure 24-13 DNS configuration



```
[root@ecs-bae5 ~]# cat /etc/resolv.conf
; generated by /sbin/dhclient-script
search openstacklocal
options single-request-reopen
nameserver 100.125.135.29
nameserver 100.125.17.29
```

If the domain name of the ECS is resolved using a non-private DNS server and you want to switch to a private DNS server, change the DNS server to a private one.

For details, see **How Can I Configure the NTP and DNS Servers for an ECS?**

Checking the hosts Configuration File

If the DNS configuration is correct but the ECS still cannot access the Internet, check whether the mapping information in the hosts configuration file is correct. In case of any incorrect mapping, comment it out.

For Linux, run the following command to view the hosts configuration:

vim /etc/hosts

If there is an incorrect domain name mapping, comment it out and save the hosts file.

Checking Whether Both Network and NetworkManager Have Been Enabled

Network and NetworkManager are two network management tools, and either one of them can be enabled each time. If both of them are enabled, they are incompatible with each other.

Take CentOS 7 as an example. NetworkManager is recommended for CentOS 7.

1. Check the Network or NetworkManager running status.

   systemctl status network

   systemctl status NetworkManager

   In the check result:
   - If the **Active** values of both Network and NetworkManager are **active (running)**, go to step 2.
   - If the **Active** value of Network is **active (running)** and that of NetworkManager is **inactive (dead)**, go to step 2.
   - If the **Active** value of Network is **inactive (dead)** and that of NetworkManager is **active (running)**, no further action is required.
2. Run the following commands to disable Network:

   systemctl stop network

   systemctl disable network
3. Run the following commands to enable NetworkManager:

   systemctl start NetworkManager

   systemctl enable NetworkManager

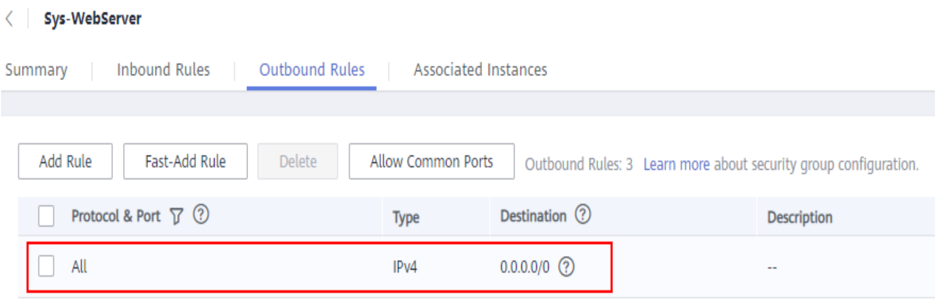
Checking Whether the Security Group Is Correctly Configured

Check whether the security group of the ECS is correctly configured. If an allowlist is configured for the outbound rules of the security group, the network traffic in the outbound direction is permitted.

As shown in **Figure 24-14**, all network traffic in the outbound direction is permitted.

For instructions about how to permit a protocol or port, see **Configuring Security Group Rules**.

Figure 24-14 Permitting all network traffic in the outbound direction



☐ Protocol & Port	Type	Destination	Description
☐ All	IPv4	0.0.0.0/0	--

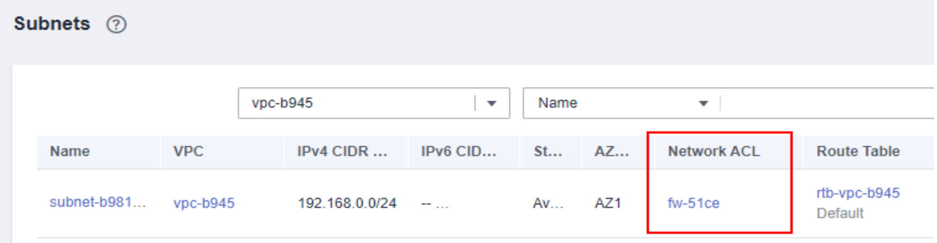
Checking ACL Rules

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

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

   If an ACL name is displayed, the network ACL has been associated with the ECS.

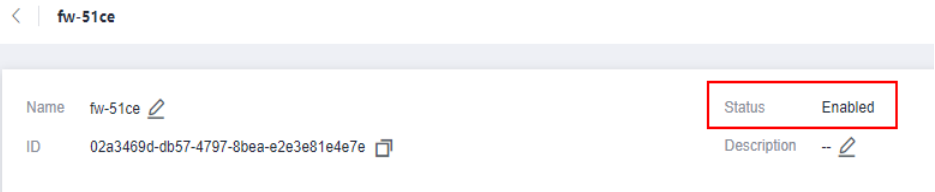
   Figure 24-15 Network ACL

Name	VPC	IPv4 CIDR ...	IPv6 CID...	St...	AZ...	Network ACL	Route Table
subnet-b981...	vpc-b945	192.168.0.0/24	-- ...	Av...	AZ1	fw-51ce	rtb-vpc-b945 Default

2. Click the ACL name to view its status.

   Figure 24-16 Enabled network ACL

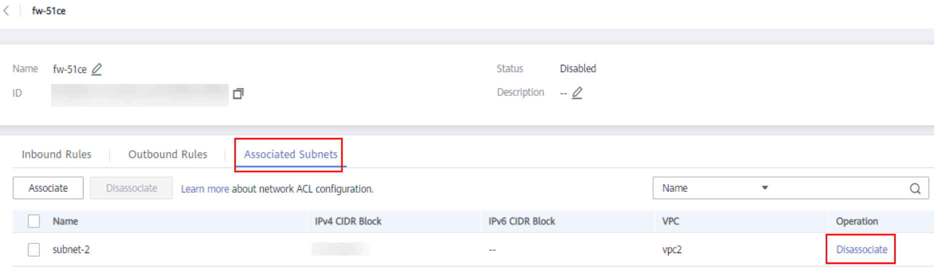
   

   Name fw-51ce
   ID 02a3469d-db57-4797-8bea-e2e3e81e4e7e
   Status Enabled
   Description --

3. Disassociate the network ACL from the subnet of the ECS.

   On the page providing details about the network ACL, choose **Associated Subnets** > **Disassociate**.

   Figure 24-17 Disassociating a network ACL

   Name fw-51ce
   ID [redacted]
   Status Disabled
   Description --

   Learn more about network ACL configuration.

Name	IPv4 CIDR Block	IPv6 CIDR Block	VPC	Operation
☐ subnet-2	[redacted]	--	vpc2	Disassociate

   NOTE

   The default network ACL rule denies all incoming and outgoing packets. If a network ACL is disabled, the default rule is still effective.

4. Try to access the Internet through the ECS again.

Checking Whether the Website to Be Visited Is Outside the Chinese Mainland

Websites outside the Chinese mainland may not be accessible or respond slowly when you access them through an ECS. This is caused by the slow access of a DNS server outside the Chinese mainland.

NOTE

If you intend to access websites outside the Chinese mainland, select a region according to the website when purchasing an ECS.

To speed up the access to a website outside the Chinese mainland, see **Why Accessing a Website Outside the Chinese Mainland Is Slow on an ECS?**

Checking Whether the EIP Is Blocked

IP address blocking indicates that all traffic is destined to a null route. If the EIP is blocked, the ECS cannot access the Internet.

Generally, blocked EIPs will be automatically unblocked after 24 hours if no subsequent attack occurs.

It is recommended that you use **Advanced Anti-DDoS (AAD)** to prevent attacks.

Checking Whether a Private IP Address Can Be Obtained

Private IP addresses may be lost if the dhclient process is not running or the target NIC is not managed by NetworkManager because NetworkManager automatic startup is not enabled. Perform the following operations to locate the fault:

Consider an ECS running CentOS 7 as an example.

1. Run the following command to check whether dhclient is running:

   ```
   ps -ef |grep dhclient |grep -v grep
   ```

2. If dhclient is not detected, run the following command to check whether NetworkManager is running:

   ```
   systemctl status NetworkManager
   ```

   - If NetworkManager is in **Active: inactive (dead)** state, NetworkManager is not enabled. Run the following command to check whether NetworkManager is automatically started upon system startup:

     ```
     systemctl is-enabled NetworkManager
     ```

     If the command output is **disabled**, run the following command to enable NetworkManager automatic startup:

     ```
     systemctl enable NetworkManager && systemctl start NetworkManager
     ```

   - If NetworkManager is in **Active: active (running)** state, run the following command to check whether the target NIC is managed by NetworkManager:

     ```
     nmcli device status
     ```

     If the NIC is in **unmanaged** state, run the following command to enable it to be managed by NetworkManager:

```
nmcli device set eth0 managed yes
```

3. Run the following commands to restart NetworkManager:

   ```
   systemctl restart NetworkManager
   ```

4. Run the following command to check whether the private IP address can be allocated:

   ```
   ip add
   ```

Checking the NIC Configuration

1. Run the following command to open the **/etc/sysconfig/network-scripts/ifcfg-eth0** file:

   ```
   vi /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

2. Modify the following configuration in this file.

   Consider an ECS running CentOS 7 as an example.

   ```
   DEVICE="eth0"
   BOOTPROTO="dhcp"
   ONBOOT="yes"
   TYPE="Ethernet"
   PERSISTENT_DHCLIENT="yes"
   ```

3. Run the following command to restart the network:

   ```
   service network restart
   ```

Checking the Firewall Configuration

Consider an ECS running CentOS 7 as an example. Check whether the firewall is enabled.

For more details, see **How Do I Disable a Linux ECS Firewall and Add a Port Exception on a Linux ECS Firewall?**

```
firewall-cmd --state
```

The command output is as follows:

```
[root@ecs-centos7 ~]# firewall-cmd --state
running
```

Run the following command to disable the firewall:

```
systemctl stop firewalld.service
```

⚠ **CAUTION**

Enabling a firewall and configuring a security group protect your ECSs. If you disable a firewall, exercise caution when you enable ports in the security group.

---

25 Website or Application Inaccessible

25.1 How Do I Troubleshoot an Unresponsive Website Hosted on My ECS?

Symptom

Websites running on an ECS might become unreachable for multiple reasons. Check whether the configurations of network, port, firewall, or security group of the ECS are correct.

Fault Locating

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 description in **Returned Values for General Requests**.

NOTE

If the error message cannot help you locate the fault, record the resource details and fault occurred time. Then, choose **Service Tickets** > **Create Service Ticket** in the upper right corner of the management console to submit a ticket.

You can also locate the fault based on the following possible causes which are listed in order of their probability.

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

Figure 25-1 Fault locating

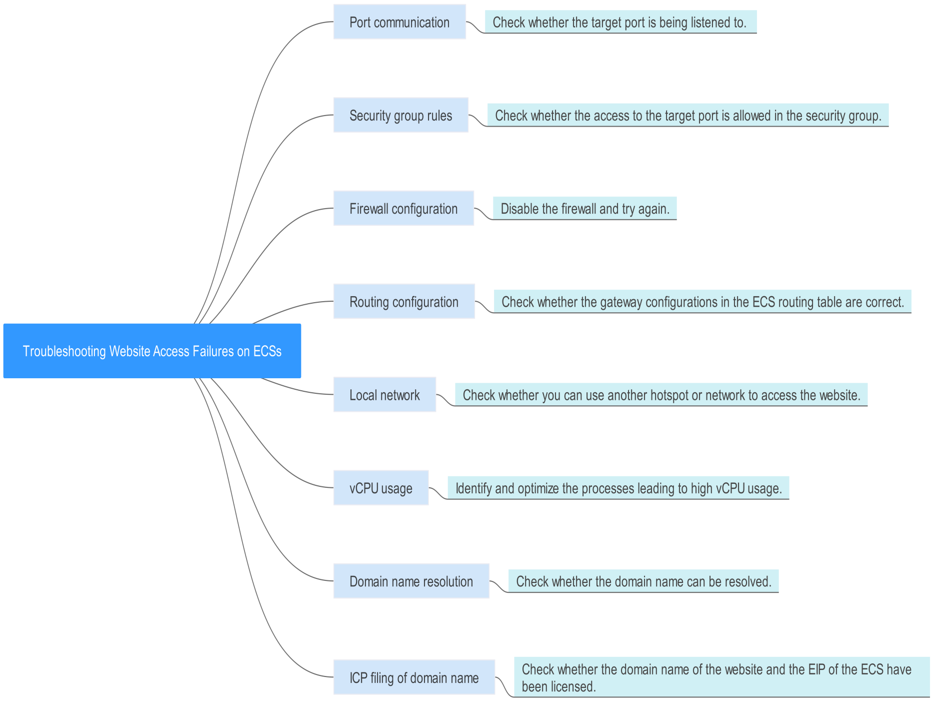

Troubleshooting Website Access Failures on ECSs
Port communication
Check whether the target port is being listened to.
Security group rules
Check whether the access to the target port is allowed in the security group.
Firewall configuration
Disable the firewall and try again.
Routing configuration
Check whether the gateway configurations in the ECS routing table are correct.
Local network
Check whether you can use another hotspot or network to access the website.
vCPU usage
Identify and optimize the processes leading to high vCPU usage.
Domain name resolution
Check whether the domain name can be resolved.
ICP filing of domain name
Check whether the domain name of the website and the EIP of the ECS have been licensed.

Table 25-1 Possible causes and solutions

Possible Causes	Solution
Port communication	Check whether the web port used by the target website is properly listened to on the ECS. For details, see **Checking Port Communication**.
Security group rules	Check whether the access to the Web port is allowed in the security group of the ECS. For details, see **Checking Security Group Rules**.
Firewall configuration	Disable the firewall and try again. For details, see **Checking the Firewall Configuration**.
Route configuration	Check whether the gateway configurations in the ECS route table are correct. For details, see **Checking the ECS Route Configuration**.
Local network	Check whether you can use another hotspot or network to access the website. For details, see **Checking the Local Network**.
CPU usage	Identify and optimize the processes leading to high vCPU usage. For details, see **Checking the CPU Usage**.

Checking Port Communication

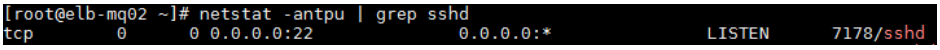
Ensure that service processes and ports are in **LISTEN** state. **Table 25-2** lists the common TCP statuses.

- Linux

  Run the **netstat -antpu** command to check whether the port used by the target website is in **LISTEN** status.

  For example, run **netstat -antpu |grep sshd**.

  Figure 25-2 Checking port listening status (Linux)

```
[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 status is **LISTEN**, go to **Checking Security Group Rules**.
  - If the port status is not **LISTEN**, check whether the web service process has been started and correctly configured.

- Windows

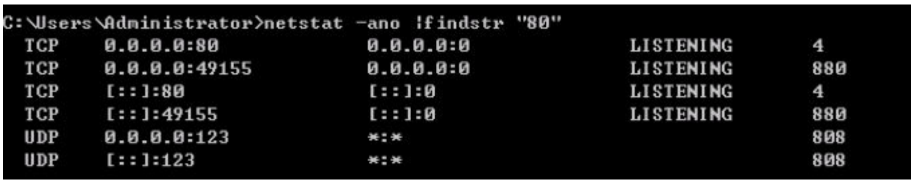
  Perform the following operations to check port communication:

  a. Run **cmd.exe**.

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

     For example, run **netstat -ano | findstr "80"**.

     Figure 25-3 Checking port listening status (Windows)

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

Table 25-2 Common TCP statuses

TCP 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.

TCP Status	Description	Application Scenario
TIME-WAIT	Waits until the remote TCP server receives the acknowledgment 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 an infinite loop 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 the 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 acknowledgment 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, restart the OS to resolve this issue.

Checking Security Group Rules

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

1. Log in to the management console.
2. Under **Compute**, choose **Elastic Cloud Server**.
3. In the ECS list, click the name of the target ECS.
4. Click the **Security Groups** tab.
5. In the **All** area on the left, click **Manage Rule** on the right of the target security group.
6. Configure the rule to allow the access of the port used by the website.

   For details, see **Configuring Security Group Rules**.

Checking the Firewall Configuration

- Linux ECS

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

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

  b. Run the following commands to allow access to 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.

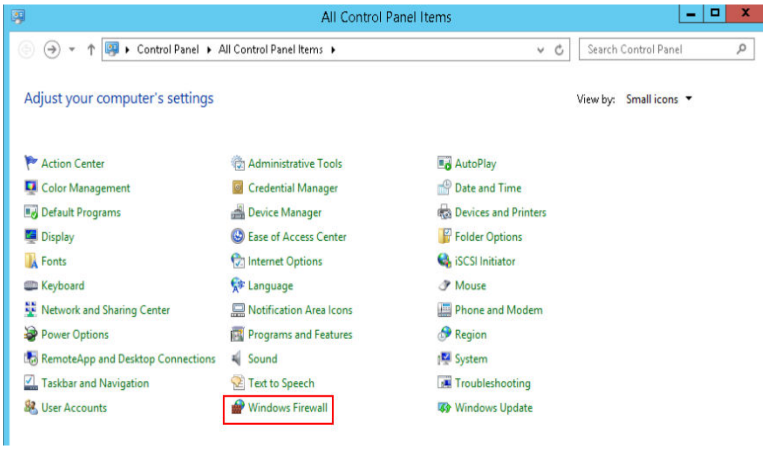
  e. Run the **iptables -nvL --line-number** command to check whether the added rules have taken effect.

  f. Disable the firewall and try again.

- Windows ECS

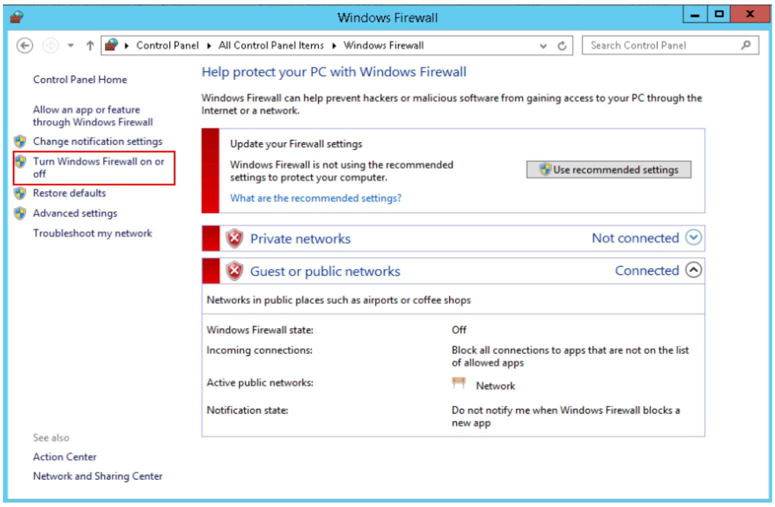
  a. Log in to the Windows ECS.

  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.



Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

Private networks Not connected

Guest or public networks Connected

Networks in public places such as airports or coffee shops

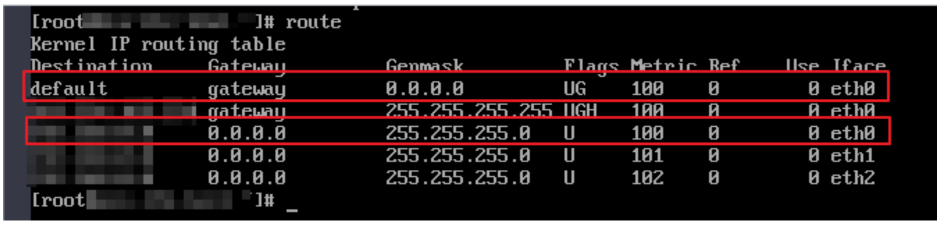
Windows Firewall state: Off
Incoming connections: Block all connections to apps that are not on the list of allowed apps
Active public networks: Network
Notification state: Do not notify me when Windows Firewall blocks a new app

d. Disable the firewall and try again.

Checking the ECS Route Configuration

- Linux ECS

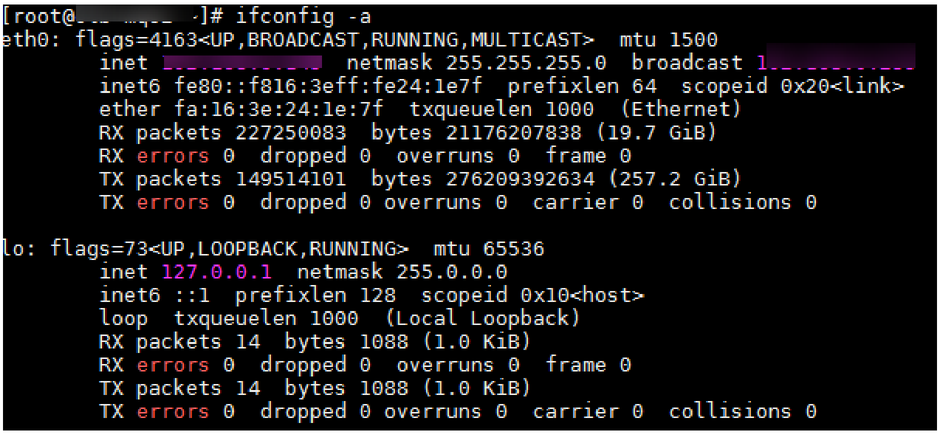
a. Run the **route** command to check the routing policy. Ensure that the default route of 0.0.0.0 is destined for the gateway and that the IP address and the gateway are in the same network segment, as shown in the first and third lines in the following figure.



```
[root[redacted]]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         gateway         0.0.0.0         UG    100    0        0 eth0
[redacted]      gateway         255.255.255.255 UGH   100    0        0 eth0
[redacted]      0.0.0.0         255.255.255.0   U     100    0        0 eth0
[redacted]      0.0.0.0         255.255.255.0   U     101    0        0 eth1
[redacted]      0.0.0.0         255.255.255.0   U     102    0        0 eth2
[root[redacted]]# _
```

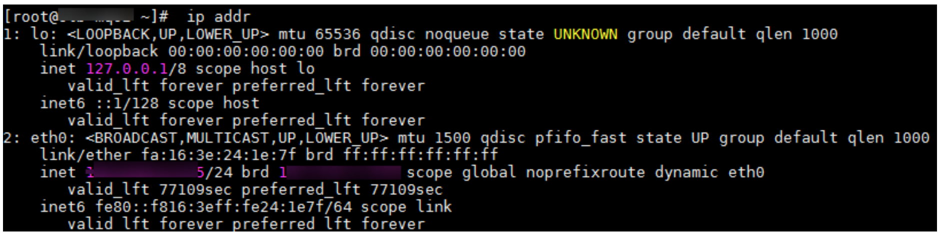
b. Run the **ifconfig** or **ip addr** command to obtain the ECS IP address.

Figure 25-4 ifconfig command output



```
[root@[redacted]]# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask 255.255.255.0  broadcast [redacted]
        inet6 fe80::f816:3eff:fe24:1e7f  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:24:1e:7f  txqueuelen 1000  (Ethernet)
        RX packets 227250083  bytes 21176207838 (19.7 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 149514101  bytes 276209392634 (257.2 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 14  bytes 1088 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 1088 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 25-5 ip addr command output

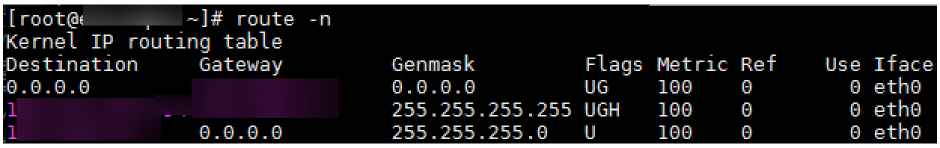


```
[root@[redacted] ~]#  ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether fa:16:3e:24:1e:7f brd ff:ff:ff:ff:ff:ff
    inet [redacted]5/24 brd [redacted] scope global noprefixroute dynamic eth0
       valid_lft 77109sec preferred_lft 77109sec
    inet6 fe80::f816:3eff:fe24:1e7f/64 scope link
       valid_lft forever preferred_lft forever
```

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

Figure 25-6 shows an example just for reference.

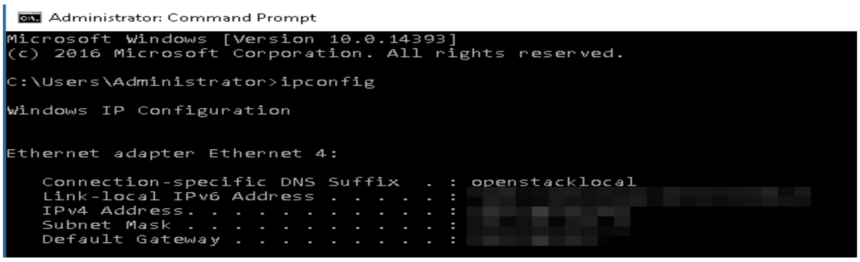
Figure 25-6 route -n command output



```
[root@[redacted] ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         [redacted]      0.0.0.0         UG    100    0        0 eth0
[redacted]      [redacted]      255.255.255.255 UGH   100    0        0 eth0
[redacted]      0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

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

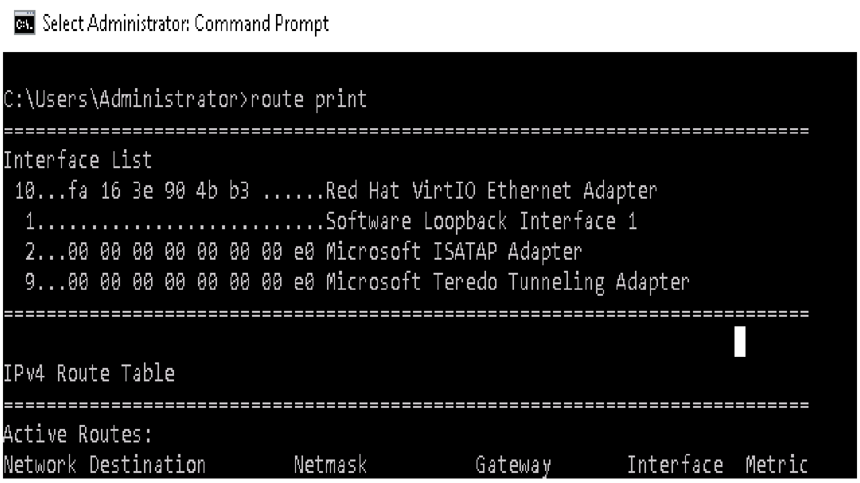
Figure 25-7 ipconfig command output



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . : openstacklocal
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . :
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . :
```

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

Figure 25-8 route print command output



```
C:\Users\Administrator>route print
===========================================================================
Interface List
 10...fa 16 3e 90 4b b3 ......Red Hat VirtIO Ethernet Adapter
  1...........................Software Loopback Interface 1
  2...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
  9...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
```

Checking the Local Network

Try another hotspot or network for access.

If the access is successful, the fault may occur in the local carrier network. In such a case, rectify the local network fault and try again.

Checking the CPU Usage

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

1. Identify the processes leading to a high bandwidth or vCPU usage.
   - Windows

     Windows offers multiple tools to locate faults, including Task Manager, Performance Monitor, Resource Monitor, Process Explorer, Xperf (supported by versions later than Windows Server 2008), and full memory dump analysis.

  - Linux

    Run the **top** command to check the OS running status.

2. Check whether the processes are normal and handle any issues accordingly.
   - If the processes are normal, optimize them or modify ECS configurations by referring to **Modifying Specifications**.
   - If the processes are abnormal, stop these processes manually or use a third-party tool to stop them automatically.

25.2 Why Did I See "Invalid argument" or "neighbour table overflow" During an Access to a Linux ECS?

Symptom

1. When a Linux ECS sends a request to a server in the same subnet, the server has received the request but does not return a response. When the server pings the client, the message "sendmsg: Invalid argument" is displayed.
```
64 bytes from 192.168.0.54: icmp_seq=120 ttl=64 time=0.064 ms
64 bytes from 192.168.0.54: icmp_seq=122 ttl=64 time=0.071 ms
ping: sendmsg: Invalid argument
ping: sendmsg: Invalid argument
ping: sendmsg: Invalid argument
```
2. "neighbor table overflow" is displayed in the **/var/log/messages** log file or the **dmesg** command output of a Linux ECS.
```
[21208.317370] neighbour: ndisc_cache: neighbor table overflow!
[21208.317425] neighbour: ndisc_cache: neighbor table overflow!
[21208.317473] neighbour: ndisc_cache: neighbor table overflow!
[21208.317501] neighbour: ndisc_cache: neighbor table overflow!
```

Possible Causes

The Neighbour table references the ARP cache. When the Neighbour table overflows, the ARP table is full and will reject connections.

You can run the following command to check the maximum size of the ARP cache table:

# cat /proc/sys/net/ipv4/neigh/default/gc_thresh3

Check the following parameters in the ARP cache table:
```
/proc/sys/net/ipv4/neigh/default/gc_thresh1
/proc/sys/net/ipv4/neigh/default/gc_thresh2
/proc/sys/net/ipv4/neigh/default/gc_thresh3
```

- gc_thresh1: The minimum number of entries to keep in the ARP cache. The garbage collector will not run if there are fewer than this number of entries in the cache.
- gc_thresh2: The soft maximum number of entries to keep in the ARP cache. The garbage collector will allow the number of entries to exceed this for 5 seconds before collection will be performed.

- gc_thresh3: The hard maximum number of entries to keep in the ARP cache. The garbage collector will always run if there are more than this number of entries in the cache.

To verify the actual number of IPv4 ARP entries, run the following command:

# ip -4 neigh show nud all | wc -l

Solution

1. Make sure that the number of servers in a subnet is less than the **default.gc_thresh3** value.
2. Adjust parameters: change **gc_thresh3** to a value much greater than the number of servers in the same VPC network segment, and make sure that the **gc_thresh3** value is greater than the **gc_thresh2** value, and the **gc_thresh2** value is greater than the **gc_thresh1** value.

   For example, if a subnet has a 20-bit mask, the network can accommodate a maximum of 4,096 servers. The **default.gc_thresh3** value of this network segment must be a value much greater than 4,096.

   Temporary effective:

   ```
   # sysctl -w net.ipv4.neigh.default.gc_thresh1=2048
   # sysctl -w net.ipv4.neigh.default.gc_thresh2=4096
   # sysctl -w net.ipv4.neigh.default.gc_thresh3=8192
   ```

   Always effective:

   CAUTION

   The operations involve modifying kernel parameters, which may cause kernel instability. Evaluate risks before performing this operation.

   Add the following content to the **/etc/sysctl.conf** file:

   ```
   net.ipv4.neigh.default.gc_thresh1 = 2048
   net.ipv4.neigh.default.gc_thresh2 = 4096
   net.ipv4.neigh.default.gc_thresh3 = 8192
   ```

   Add IPv6 configuration if required:

   ```
   net.ipv6.neigh.default.gc_thresh1 = 2048
   net.ipv6.neigh.default.gc_thresh2 = 4096
   net.ipv6.neigh.default.gc_thresh3 = 8192
   ```

26 Slow Website or Application Response

26.1 Why Accessing a Website Outside the Chinese Mainland Is Slow on an ECS?

Symptom

Websites outside the Chinese mainland, including those in Hong Kong (China), Macao (China), Taiwan (China), and other countries and regions, may be slow to access.

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

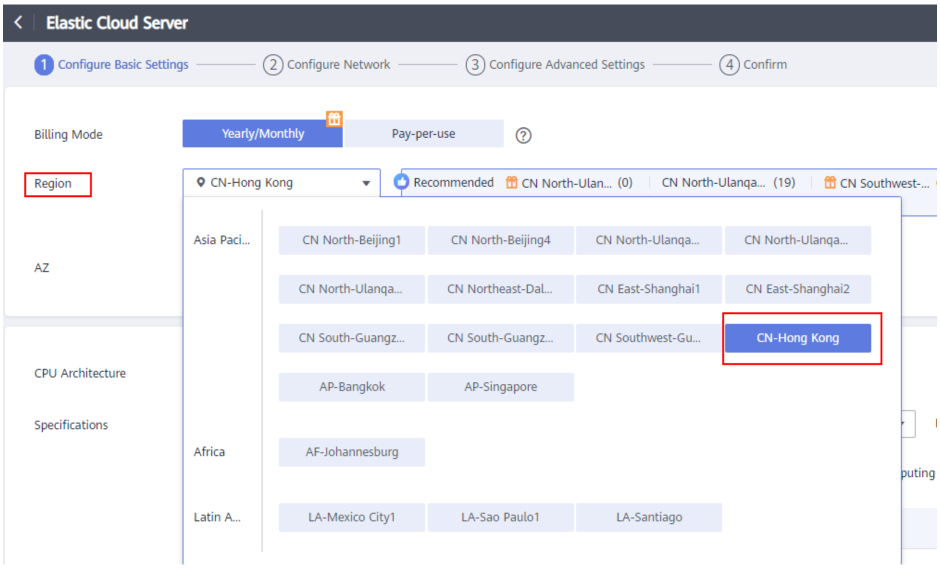
Solution

- Purchase an ECS in a region (such as **CN-Hong Kong**) outside the Chinese mainland.

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

  For example, select the **CN-Hong Kong** region during the ECS purchase.

Figure 26-1 Buying an ECS in **CN-Hong Kong**



- Improve the access speed.

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

  – **Modifying the DNS Configuration**

  – **Modifying the hosts File**

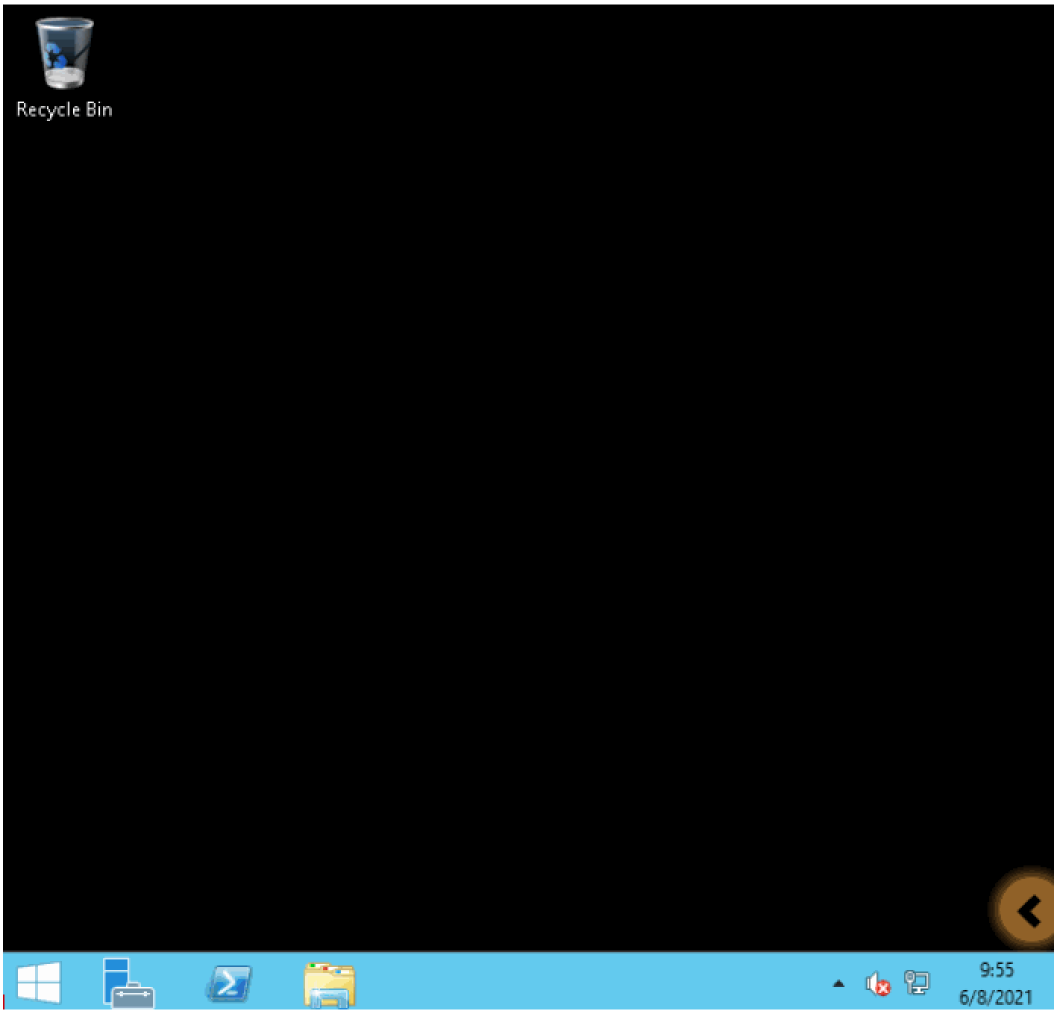
  After that, run the **ping -t** *Website address* command to check the packet loss. For details, see **Checking Whether the Request Is Responded**.

Modifying the DNS Configuration

Change the DNS server addresses to public DNS server addresses, for example, 101.226.4.6 and 1.1.1.1.

The following figure demonstrates how to modify the DNS configuration on an ECS running Windows Server 2012.

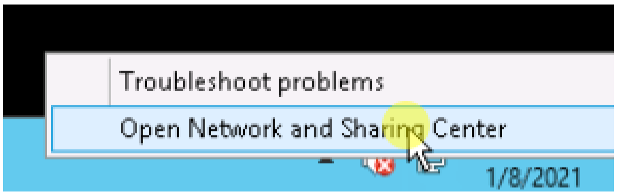
Figure 26-2 Modifying the DNS configuration



The following are detailed operations:

1. Log in to the Windows ECS 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**.

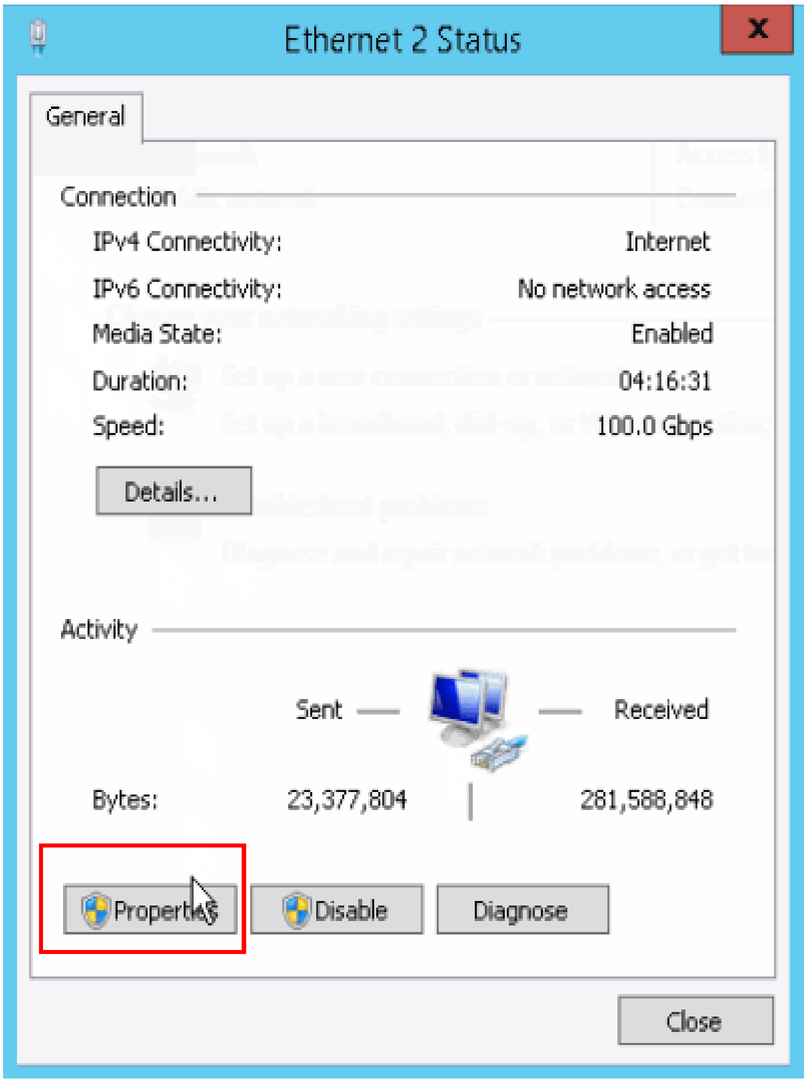
Figure 26-3 Open Network and Sharing Center



    c. In the navigation pane on the left, click **Change adapter settings**.
3. Configure the DNS server for the ECS.
    a. Double-click network connections.

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

Figure 26-4 Local area connection



Ethernet 2 Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

Duration: 04:16:31

Speed: 100.0 Gbps

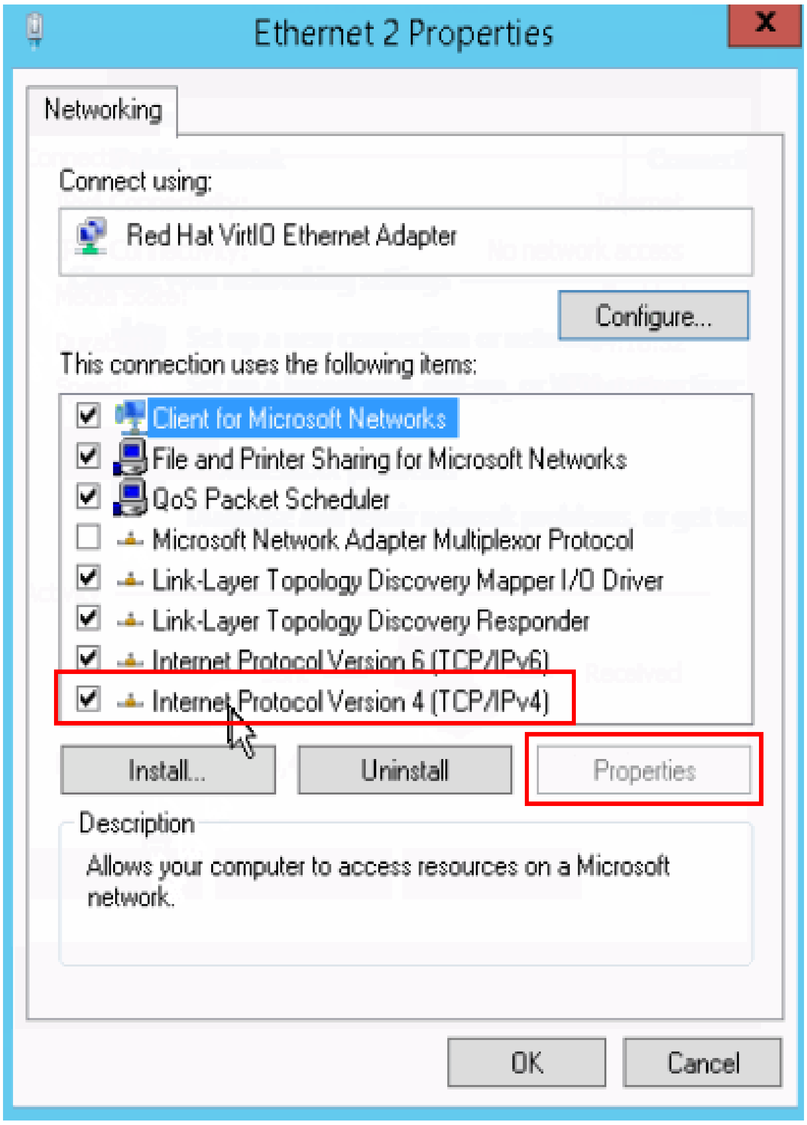
Activity

Sent — — Received

Bytes: 23,377,804 | 281,588,848

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

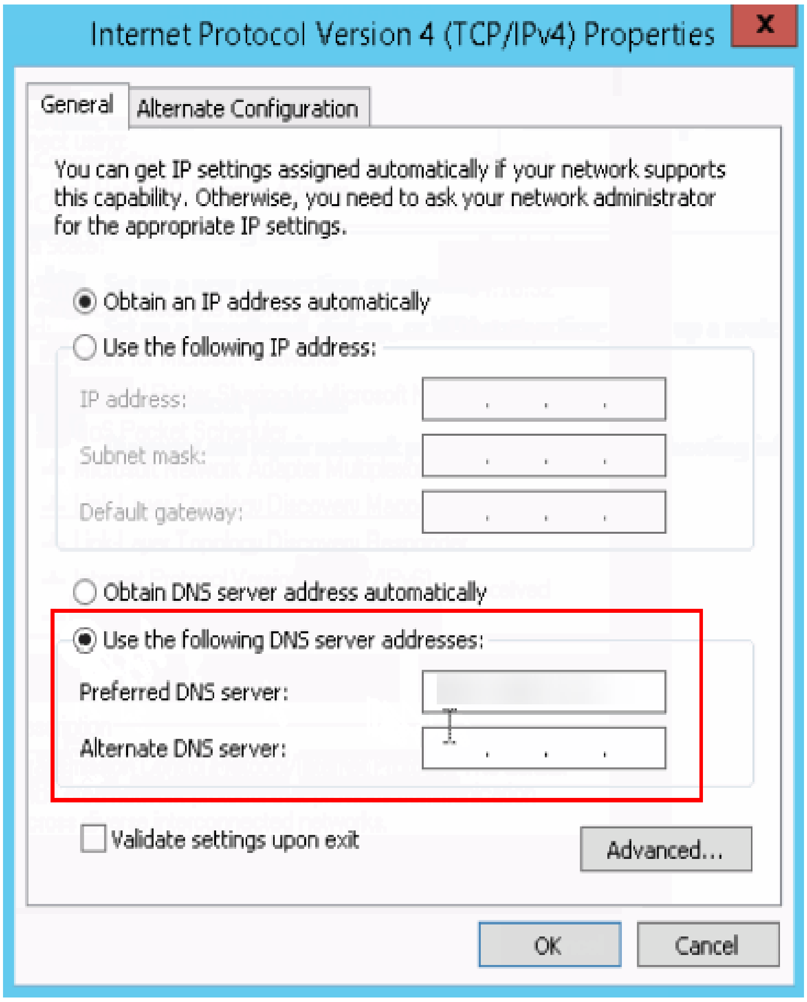
Figure 26-5 Selecting a protocol type



Ethernet 2 Properties
Networking
Connect using:
Red Hat VirtIO Ethernet Adapter
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
Install...
Uninstall
Properties
Description
Allows your computer to access resources on a Microsoft network.
OK
Cancel

d. Select **Use the following DNS server addresses** and set the IP addresses of the DNS servers as prompted.

Figure 26-6 Setting the DNS server addresses



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server: . . .

☐ Validate settings upon exit

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.

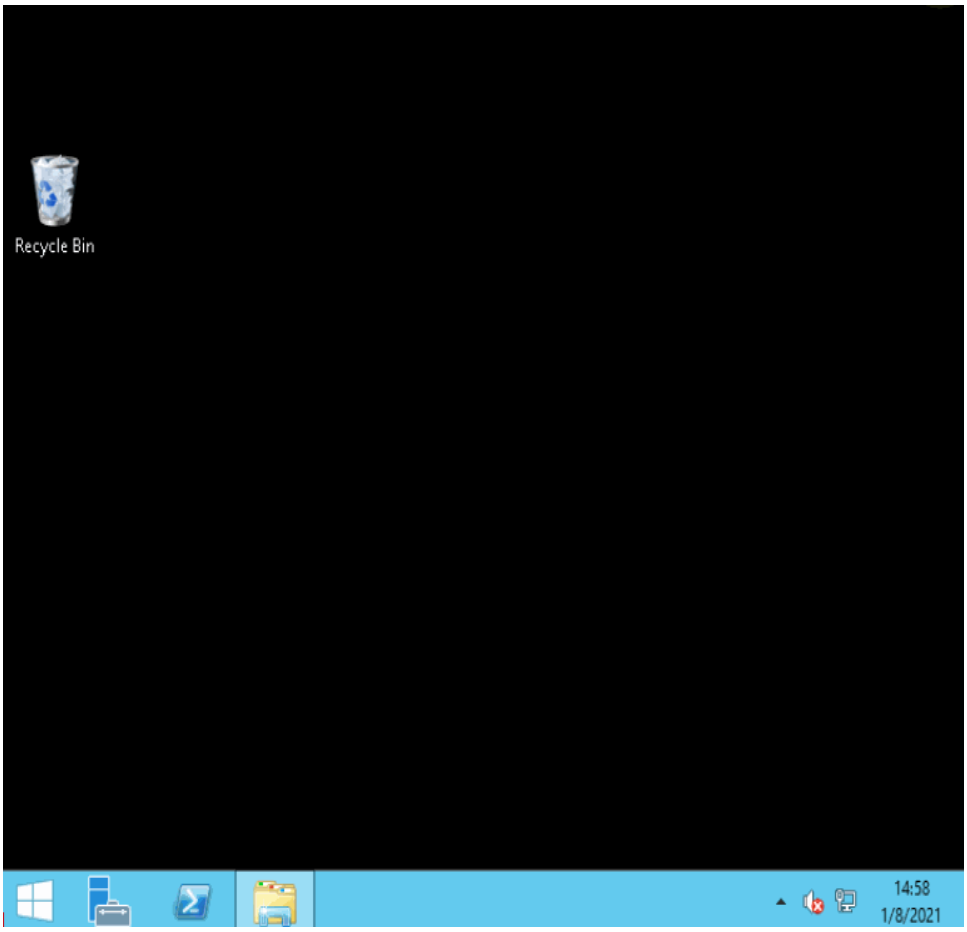
  For details, see **Method 1: Pinging the Domain Name**.
- Use a ping tool and PingInfoView.

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

Method 1: Pinging the Domain Name

The following figure 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.)

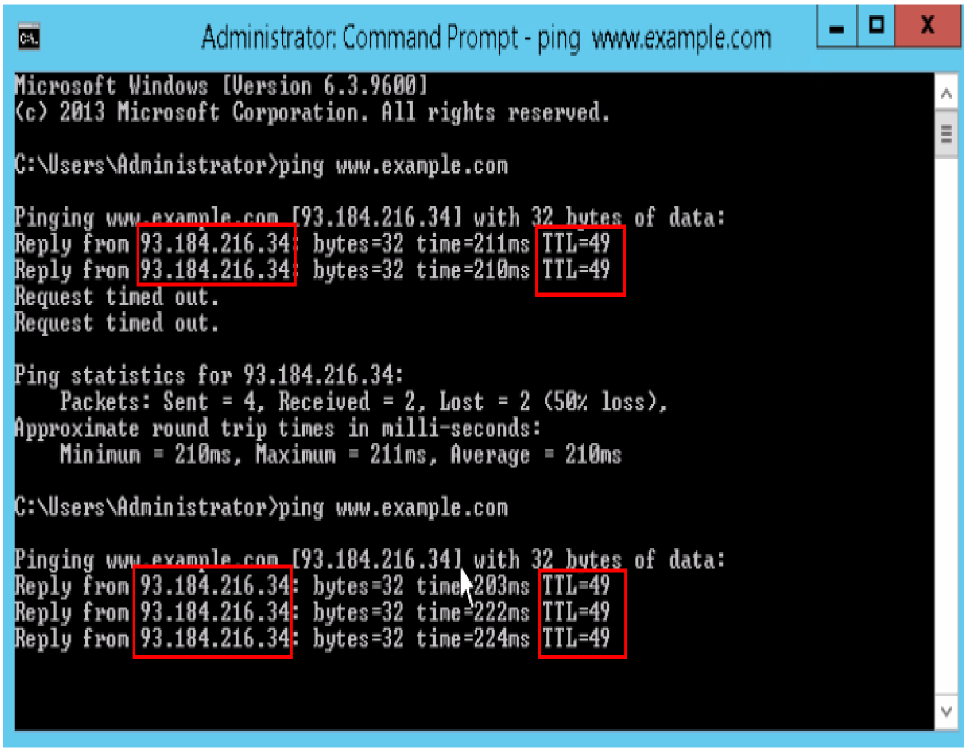
Figure 26-7 Modifying the **hosts** file



The following are detailed operations:

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

Figure 26-8 Command output



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping www.example.com

Pinging www.example.com [93.184.216.34] with 32 bytes of data:
Reply from 93.184.216.34: bytes=32 time=211ms TTL=49
Reply from 93.184.216.34: bytes=32 time=210ms TTL=49
Request timed out.
Request timed out.

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 210ms, Maximum = 211ms, Average = 210ms

C:\Users\Administrator>ping www.example.com

Pinging www.example.com [93.184.216.34] with 32 bytes of data:
Reply from 93.184.216.34: bytes=32 time=203ms TTL=49
Reply from 93.184.216.34: bytes=32 time=222ms TTL=49
Reply from 93.184.216.34: bytes=32 time=224ms TTL=49
```

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

⚠ CAUTION

During the ping operation, run the **ipconfig /flushdns** command to refresh the DNS resolution cache. Otherwise, the same IP address will be pinged continuously.

In this example, IP address 93.184.216.34 has the smallest TTL value.

3. Modify the **hosts** file.

   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.

   For example, if the obtained IP address is 93.184.216.34, enter **93.184.216.34 www.example.com** in the end of the **hosts** file, save and exit the file.

CAUTION

- Exercise caution when you modify the **hosts** file.

  You are advised to back up the **hosts** file using either of the following methods: Copy and paste the **hosts** file, or copy and paste the content of the **hosts** file.
- 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 still slow and you want to replace the IP address, delete the existing mapping from the **hosts** file and repeat the preceding operations to obtain a new IP address.

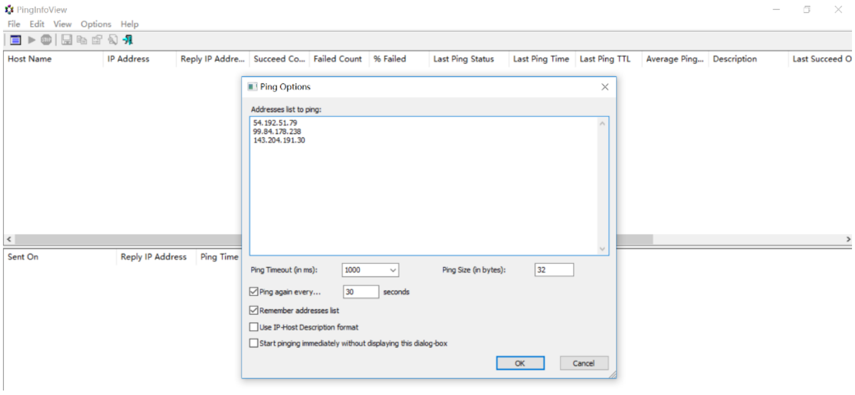
4. Access the website again.

   Modifying the **hosts** file can only speed up the website access. If the problem persists, purchase an ECS in a region outside the Chinese Mainland, for example, **CN-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 your ECS 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**.



Addresses list to ping:

```
54.192.51.79
99.84.178.238
143.204.191.30
```

Ping Timeout (in ms): 1000

Ping Size (in bytes): 32

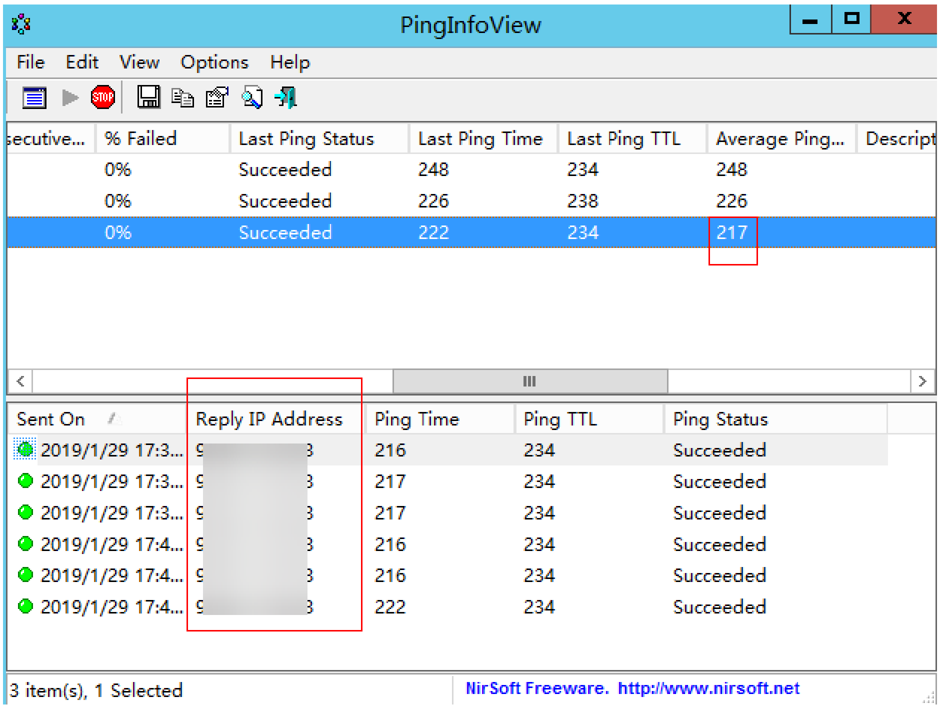
☑ Ping again every... 30 seconds

☑ Remember addresses list

☐ Use IP-Host Description format

☐ Start pinging immediately without displaying this dialog-box

6. Copy one IP address in the search result.



ecutive...	% Failed	Last Ping Status	Last Ping Time	Last Ping TTL	Average Ping...	Descript
	0%	Succeeded	248	234	248	
	0%	Succeeded	226	238	226	
	0%	Succeeded	222	234	217	

Sent On	Reply IP Address	Ping Time	Ping TTL	Ping Status
2019/1/29 17:3...	[redacted]	216	234	Succeeded
2019/1/29 17:3...	[redacted]	217	234	Succeeded
2019/1/29 17:3...	[redacted]	217	234	Succeeded
2019/1/29 17:4...	[redacted]	216	234	Succeeded
2019/1/29 17:4...	[redacted]	216	234	Succeeded
2019/1/29 17:4...	[redacted]	222	234	Succeeded

3 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

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

CAUTION

- Exercise caution when you modify the **hosts** file.

  You are advised to back up the **hosts** file using either of the following methods: Copy and paste the **hosts** file, or copy and paste the content of the **hosts** file.
- 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 still slow and you want to replace the IP address, delete the existing mapping from the **hosts** file and repeat the preceding operations to obtain a new IP address.

For example, if the selected 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 ECS purchased in a region outside the Chinese Mainland to access the target website.

Checking Whether the Request Is Responded

Try to access the target website. If the website can be accessed but the loading is still slow, 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**

For example, run **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.