# Contents

## 1 General Issues

1.1 Troubleshooting Slow Access of a Website Outside the Chinese Mainland over an ECS ........................................ 1
1.2 Troubleshooting a Ping Failure or Packet Loss Using a Link Test ............................................................. 3
1.3 Troubleshooting Network Freezing on an ECS ....................................................................................... 8
1.4 Troubleshooting a Website Access Error Occurred on an ECS ......................................................... 10
1.5 Troubleshooting an Unreachable ECS Port ......................................................................................... 14
1.6 Troubleshooting High Bandwidth Usage on an ECS ............................................................................ 18
1.7 Troubleshooting High Bandwidth or CPU Usage of a Windows ECS ................................................. 20
1.8 Troubleshooting High Bandwidth or CPU Usage of a Linux ECS ..................................................... 25
1.9 How Can I Handle Slow ECS Startup? ............................................................................................ 29
1.10 Troubleshooting Multi-IP-Address Access on an ECS with Multiple NICs Attached ..................... 29

## 2 Windows Issues

2.1 Retaining a Session on a Windows ECS ................................................................................................. 32
2.2 Troubleshooting Difference Between System Time and Local Standard Time ................................. 34
2.3 Troubleshooting Internet Access on an Extension NIC Newly Attached to a Windows ECS ........... 38
2.4 Troubleshooting Disabled Copy and Paste Options ...................................................................... 40
2.5 Configuring File Sharing and Network Disk Mapping for a Windows ECS .................................... 42
2.6 Troubleshooting an In-Service Port During Tomcat Startup .......................................................... 48
2.7 Troubleshooting Unavailable Input Methods ................................................................................... 50
2.8 Troubleshooting File Sharing Between Windows ECSs ................................................................. 57
2.9 Troubleshooting Data Restoration in the Event of a Startup Failure on a Windows ECS ................ 59
2.10 Viewing Login Logs of a Windows ECS .......................................................................................... 60

## 3 Linux Issues

3.1 Troubleshooting Emergency Mode .................................................................................................. 63
3.2 What Can I Do If Switching from a Non-root User to User root Times Out? ................................ 67

## 4 Managing Disk Space

4.1 Troubleshooting the Creation of a Swap Partition or File on Linux ................................................ 68

## 5 Multi-user Login Issues

5.1 Troubleshooting Multi-User Logins for an ECS Running Windows Server 2012 ............................ 70
5.2 Troubleshooting a Browser Launch Error Occurred in Multi-User Login ........................................ 84
5.3 Applying for a License for Authenticating Multi-User Sessions and Activating the ECS ............... 86
6 Troubleshooting Remote Login Errors On a Windows ECS ........................................101
6.1 What Should I Do If an Authentication Failure Occurs After I Attempt to Remotely Log In to a Windows ECS? .. 101
6.2 What Should I Do If the Local Computer Cannot Connect to My Windows ECS? ........................................ 103
6.3 What Should I Do If I Do Not Have the Permission to Remotely Log In to a Windows ECS? ......................... 108
6.4 What Should I Do If the System Displays No Remote Desktop License Servers Available to Provide a License When I Log In to a Windows ECS? ................................................................. 110
6.5 What Should I Do If the System Displays Error Code 0x112f When I Log In to a Windows ECS? .................... 113
6.6 What Should I Do If the System Displays Error Code 0x1104 When I Log In to a Windows ECS? .................... 114
6.7 What Should I Do If the System Displays Error Code 122.112... When I Log In to a Windows ECS? ............... 118
6.8 What Should I Do If the System Displays Invalid Certificate or Associated Chain When I Log In to a Windows ECS from a Mac? ................................................................. 120
6.9 What Should I Do If the System Displays a Message Indicating Invalid Credentials? ................................. 124
6.10 What Should I Do If an Internal Error Occurs When I Log In to My Windows ECS? ............................... 130
6.11 Troubleshooting Disconnected Session Because of a Protocol Error ..................................................... 131
6.12 Troubleshooting an Identity Error of the Remote Computer ............................................................... 134
6.13 Troubleshooting the Connection Error of Two Computers in the Allotted Time ................................. 135
6.14 Troubleshooting a Denied Connection Because of Unauthorized User Account ......................... 136
6.15 Troubleshooting a Lost Connection Because of Another User’s Login .............................................. 140

7 Passwords and Key Pairs .............................................................................................................. 144
7.1 Troubleshooting Password Reset for User root in the Single-User Mode on a Linux ECS ......................... 144

8 Configuring a Firewall ................................................................................................................ 151
8.1 Disabling a Windows ECS Firewall and Adding a Port Exception on a Windows ECS Firewall .......................... 151
8.2 Disabling a Linux ECS Firewall and Adding a Port Exception on a Linux ECS Firewall ............................. 156

9 Installing IIS ............................................................................................................................... 158
9.1 Troubleshooting IIS Installation on a Windows ECS ............................................................................ 158
9.2 Troubleshooting Domain Name Modification on IIS Manager .......................................................... 163
1 General Issues

1.1 Troubleshooting Slow Access of a Website Outside the Chinese Mainland over an ECS

Scenarios

Accessing a website outside the Chinese Mainland may be slow on an ECS. This is caused by the slow access of a DNS server outside the Chinese Mainland.

NOTE
If you are required to access websites outside the Chinese Mainland, purchase an ECS in a region outside the Chinese Mainland. To do so, select the target region when purchasing the ECS.

You are advised to perform the operations described in this section to identify the cause of slow website access outside the Chinese Mainland. The following uses a Windows ECS as an example to describe how to troubleshoot slow access to www.example.com.

- Checking Whether DNS Has Been Correctly Configured
- Checking Whether the Request Is Responded
- Modifying the hosts File to Speed Up the Website Access

Checking Whether DNS Has Been Correctly Configured

1. Run `cmd` and then `ipconfig /all` to check whether a default HUAWEI CLOUD DNS server address is used.
   You are advised to use the default HUAWEI CLOUD DNS server addresses.

NOTE
To obtain the addresses, see What Are the Private DNS Server Addresses Provided by the DNS Service?

2. Run the following command to check whether your ECS and the DNS server are reachable to each other:
   `ping IP address of the DNS server`
   Taking the CN North-Beijing 1 region as an example, run the `ping 100.125.1.250` command.

3. Run the following command to check whether domain name resolution is functional:
   `nslookup Target website`
For example, run `nslookup www.example.com`.
Access the target website again and check whether the fault has been rectified.
If the fault persists, perform the following operations to continue the fault locating.

### Checking Whether the Request Is Responded

- **Linux**
  Run executable curl commands delivered with Linux.
  ```
curl -I Target website
  ```
  For example, run `curl -I www.example.com`.

- **Windows**
  Try to access the target website. If the website can be accessed but the loading is slow, packet loss may occur when you access the destination server. 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. The slow website access may be caused by loss of packets sent to the destination server.
Contact customer service to check for packet loss.

### Modifying the hosts File to Speed Up the Website Access

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

1. Log in to the ECS as user **Administrator**.
2. Use a browser to access the ping check tool. The following uses `http://ping.chinaz.com` as an example.
3. Ping the target website for test. Take `www.example.com` as an example. Record the IP address with the lowest response time in detection results.
4. Download **PingInfoView**, decompress it, and run **PingInfoView.exe**.
5. Open **PingInfoView**, copy the IP addresses obtained in step 3 to the text box, and click **OK**.

6. Copy the IP address with the lowest response time in the search result.
7. Open the C:\Windows\System32\drivers\etc\ hosts file and paste the IP address in the end of the file.

**NOTE**

The hosts file is one of the core OS files. Therefore, exercise caution when modifying it. You are advised to back up the hosts file using either of the following methods: Copy and paste the hosts file for file backup; copy and paste the data of the hosts file for content backup. 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 target website again.

If the fault persists, use an ECS purchased in a region outside the Chinese Mainland to access the target website.

### 1.2 Troubleshooting a Ping Failure or Packet Loss Using a Link Test

**Symptom**

When a user accessed other network resources on an ECS, network freezing occurred. The ping command output showed that packet loss occurred or the network delay was long.

This section uses Tracert and MTR as an example to describe how to troubleshoot packet loss or long delay.

**Possible Causes**

Packet loss or long delay may be caused by link congestion, link node faults, high server load, or incorrect system settings.

After verifying that the issue was not caused by the ECS, use Tracert or MTR for further fault locating.
MTR is used to detect network faults.

This section provides the following information:

- **Windows**
  - (Recommended) **Using Tracert in Windows**
  - **Using WinMTR in Windows**
- **Linux**
  - **Using WinMTR in Linux**

### Using Tracert in Windows

Tracert shows the path through which packets reach the destination server and the time when the packets reach each node. Tracert offers similar functions as the ping command but it provides more detailed information, including the entire path the packets take, IP address of each pass-through node, and time when the packets arrive at each node.

1. Log in to the Windows ECS.
2. Open the cmd window and run the following command to trace the IP address:

   ```tracert IP address or website```

   For example, `tracert www.example.com`

   ![Tracert Command Output](image)

   The command output shows that:
   - The maximum number of hops is 30 by default. The first column shows the sequence number of the start hop.
   - Tracert sends three packets each time. The second, third, and fourth columns show the time when the three packets are returned. The last column shows the IP addresses of the nodes where the packets were redirected.
   - If the message `*     *     *    request timed out` was reported, troubleshoot the affected link and node.

### Using WinMTR in Windows

1. Log in to the Windows ECS.
2. Download the WinMTR installation package on the official website based on the OS.
3. Decompress the WinMTR installation package.
4. Double-click `WinMTR.exe` to start the tool.
5. In the WinMTR window, enter the IP address or domain name of the destination server in **Host** and click **Start**.
6. Wait for WinMTR to run for a period of time and click Stop to stop the test.

The test results are as follows:
- **Hostname**: IP address or domain name of each node that the packets pass through to the destination server
- **Nr**: Number of nodes that the packets pass through
- **Loss%**: Packet loss rate of a node
- **Sent**: Number of sent data packets
- **Recv**: Number of received responses
- **Best**: Shortest response time
- **Avrg**: Average response time
- **Worst**: Longest response time
- **Last**: Last response time

**Using WinMTR in Linux**

**Installing MTR**
MTR has been installed on all Linux distributions. If MTR is not installed on your Linux ECS, run the following command to install it:

- **CentOS**
  
  ```bash
  yum install mtr
  ```

- **Ubuntu**
  
  ```bash
  sudo apt-get install mtr
  ```

**MTR parameters**

- `-h/--help`: Help menu
- `-v/--version`: MTR version
- `-r/--report`: Results of all traces
- `-p/--split`: Results of each trace
- `-c/--report-cycles`: Number of packets (10 by default) sent per second
- `-s/--psize`: Size of a packet
- `-n/--no-dns`: Domain name resolution is not performed for IP addresses
- `-a/--address`: IP address for sending packets, which is set if a single host has multiple IP addresses
- `-4`: IPv4
- `-6`: IPv6

The following uses the link between the local server and the destination server with IP address 119.xx.xx.xx as an example.

Run the following command to obtain the MTR diagnosis results in a report:

```
mtr 119.xx.xx.xx --report
```

Information similar to the following is displayed:

```
[root@ecs-420652 ~]# mtr 119.xx.xx.xx --report
Start: Thu Aug 22 15:41:22 2019
HOST: ecs-652                  Loss%   Snt   Last   Avg  Best  Wrst StDev
1.|-- 100.70.0.1                 0.0%    10    3.0   3.4   2.8  7.5   1.3
2.|-- 10.242.7.174               0.0%    10   52.4  51.5  34.2  58.9   6.3
3.|-- 10.242.7.237               0.0%    10    3.2   5.0   2.7  20.8   5.5
4.|-- 10.230.2.146               0.0%    10    1.0   1.0   1.0  1.1   0.0
5.|-- 192.168.21.1               0.0%    10    3.5   4.2   2.8 11.6   2.5
6.|-- 10.242.7.238               0.0%    10  35.3  34.5   6.0 56.4  22.6
7.|-- 10.242.7.173               0.0%    10    3.3   4.7  3.1 14.7   3.6
8.|-- ???: 100.0    10    0.0   0.0   0.0   0.0   0.0
```

The following information is displayed:

- **HOST**: IP address or domain name of the node
- **Loss%**: Packet loss rate
- **Snt**: Number of packets sent per second
- **Last**: Last response time
- **Avg**: Average response time
- **Best**: Shortest response time
- **Wrst**: Longest response time
- **StDev**: standard deviation, a larger deviation indicates a larger difference between the response time for each data packet on the node.

### Handling WinMTR and MTR Reports

The following figure is an example of analyzing the reports of WinMTR and MTR.

- **Local network of the server**: Area A in the preceding figure, indicating that the local area network and local ISP network.
  - If a node in the local network of the client malfunctions, check the local network.
  - If the local ISP network malfunctions, report the issue to the local carrier.
- **Carrier backbone network**: Area B in the preceding figure. If an error occurs in this area, locate the carrier to which the faulty node belongs based on the node IP address and report the issue to the carrier.
- **Local network on the destination end**: Area C in the preceding figure, indicating the network of the provider to which the destination server belongs.
  - If packet loss occurs on the destination server, the network configuration of the destination server may be incorrect. Then, check the firewall configuration on the destination server.
  - If packet loss occurs on certain nodes with several hops close to the destination server, the network of the provider to which the destination server belongs may be faulty.

### Common Link Faults

- **Incorrectly configured destination server**
  As shown in the following example, 100% of packets are lost at the destination address. According to the data, the data packets are not received by the destination server. The fault might be caused by incorrect network configuration on the destination server. In such a case, check the firewall configuration on the destination server.

<table>
<thead>
<tr>
<th>Host</th>
<th>Loss%</th>
<th>Snt</th>
<th>Last</th>
<th>Avg</th>
<th>Best</th>
<th>Wrst</th>
<th>StDev</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ??</td>
<td>0.0%</td>
<td>10</td>
<td>521.3</td>
<td>90.1</td>
<td>2.7</td>
<td>521.3</td>
<td>211.3</td>
</tr>
<tr>
<td>2. ??</td>
<td>0.0%</td>
<td>10</td>
<td>2.9</td>
<td>4.7</td>
<td>1.6</td>
<td>10.6</td>
<td>3.9</td>
</tr>
<tr>
<td>3. 1XX.X.X.X</td>
<td>80.0%</td>
<td>10</td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
<td>0.0</td>
</tr>
<tr>
<td>4. 11X.X.X.X</td>
<td>0.0%</td>
<td>10</td>
<td>1.7</td>
<td>7.2</td>
<td>1.6</td>
<td>34.9</td>
<td>13.6</td>
</tr>
<tr>
<td>5. 1XX.1XX.X.X</td>
<td>0.0%</td>
<td>10</td>
<td>5.2</td>
<td>5.2</td>
<td>5.1</td>
<td>5.2</td>
<td>0.0</td>
</tr>
<tr>
<td>6. 2XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>5.3</td>
<td>5.3</td>
<td>5.1</td>
<td>5.3</td>
<td>0.1</td>
</tr>
<tr>
<td>7. 1XX.1XX.XX.X</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>8. 1XX.1XX.XX.XX</td>
<td>100.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

- **ICMP rate limit**
As shown in the following example, packet loss occurs on the fifth hop, but the issue does not occur on subsequent nodes. Therefore, it is determined that the fault is caused by ICMP rate limit on the fifth node. This issue does not affect data transmission between the client and the destination server. Therefore, ignore this issue.

<table>
<thead>
<tr>
<th>Host</th>
<th>Loss%</th>
<th>Snt</th>
<th>Last</th>
<th>Avg</th>
<th>Best</th>
<th>Wrst</th>
<th>StDev</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.3</td>
<td>0.6</td>
<td>0.3</td>
<td>1.2</td>
<td>0.3</td>
</tr>
<tr>
<td>2. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.4</td>
<td>1.0</td>
<td>0.4</td>
<td>6.1</td>
<td>1.8</td>
</tr>
<tr>
<td>3. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.8</td>
<td>2.7</td>
<td>0.8</td>
<td>19.0</td>
<td>5.7</td>
</tr>
<tr>
<td>4. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>6.7</td>
<td>6.8</td>
<td>6.7</td>
<td>6.9</td>
<td>0.1</td>
</tr>
<tr>
<td>5. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>27.2</td>
<td>25.3</td>
<td>23.1</td>
<td>26.4</td>
<td>2.9</td>
</tr>
<tr>
<td>6. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>39.1</td>
<td>39.4</td>
<td>39.1</td>
<td>39.7</td>
<td>0.2</td>
</tr>
<tr>
<td>7. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>39.6</td>
<td>40.4</td>
<td>39.4</td>
<td>46.9</td>
<td>2.3</td>
</tr>
<tr>
<td>8. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>39.6</td>
<td>40.5</td>
<td>39.5</td>
<td>46.7</td>
<td>2.2</td>
</tr>
</tbody>
</table>

**Loop**

As shown in the following example, the data packets are cyclically transferred after the fifth hop. As a result, they cannot reach the destination server. This fault is caused by incorrect routing configuration on the nodes of the carrier. Contact the carrier to rectify the fault.

<table>
<thead>
<tr>
<th>Host</th>
<th>Loss%</th>
<th>Snt</th>
<th>Last</th>
<th>Avg</th>
<th>Best</th>
<th>Wrst</th>
<th>StDev</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.3</td>
<td>0.6</td>
<td>0.3</td>
<td>1.2</td>
<td>0.3</td>
</tr>
<tr>
<td>2. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.4</td>
<td>1.0</td>
<td>0.4</td>
<td>6.1</td>
<td>1.8</td>
</tr>
<tr>
<td>3. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.8</td>
<td>2.7</td>
<td>0.8</td>
<td>19.0</td>
<td>5.7</td>
</tr>
<tr>
<td>4. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>6.7</td>
<td>6.8</td>
<td>6.7</td>
<td>6.9</td>
<td>0.1</td>
</tr>
<tr>
<td>5. 1XX.XX.XX.65</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>6. 1XX.XX.XX.65</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>7. 1XX.XX.XX.65</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>8. 1XX.XX.XX.65</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>9. ???</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

**Link interruption**

As shown in the following example, no response can be received after the data packets are transferred to the fourth hop. This is generally caused by link interruption between the affected nodes. You are advised to perform a further check using a reverse link test. In such a case, contact the carrier to which the affected nodes belong.

<table>
<thead>
<tr>
<th>Host</th>
<th>Loss%</th>
<th>Snt</th>
<th>Last</th>
<th>Avg</th>
<th>Best</th>
<th>Wrst</th>
<th>StDev</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.3</td>
<td>0.6</td>
<td>0.3</td>
<td>1.2</td>
<td>0.3</td>
</tr>
<tr>
<td>2. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.4</td>
<td>1.0</td>
<td>0.4</td>
<td>6.1</td>
<td>1.8</td>
</tr>
<tr>
<td>3. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.8</td>
<td>2.7</td>
<td>0.8</td>
<td>19.0</td>
<td>5.7</td>
</tr>
<tr>
<td>4. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>6.7</td>
<td>6.8</td>
<td>6.7</td>
<td>6.9</td>
<td>0.1</td>
</tr>
<tr>
<td>5. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>6. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>7. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>8. 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>9 1XX.XX.XX.XX</td>
<td>0.0%</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

### 1.3 Troubleshooting Network Freezing on an ECS

#### Symptom

A complete HTTP request includes domain name resolution, TCP connection establishment, request initiation, processing of the request received by the server and returning a processing result, parsing of the HTML code by the browser and requesting other resources, and...
rendering and presentation of the page. The HTTP request process goes through a local client of the user, network nodes between the client and the access server, and the access server. An error occurred on any of the preceding nodes will lead to network freezing on the ECS.

### Checking Whether DNS Has Been Correctly Configured

1. Open the cmd window and run `ipconfig /all` to check whether a default HUAWEI CLOUD DNS server address is used.
   
   You are advised to use the default HUAWEI CLOUD DNS server addresses.

   ![NOTE](https://www.example.com/note.png)

   To obtain the addresses, see [What Are the Private DNS Server Addresses Provided by the DNS Service?](https://www.example.com)

2. Run the following command to check whether your ECS and the DNS server are reachable to each other:

   ```
   ping IP address of the DNS server
   ```

   Taking the CN North-Beijing 1 region as an example, run the `ping 100.125.1.250`

3. Run the following command to check whether domain name resolution is functional:

   ```
   nslookup Target website
   ```

   For example, `nslookup www.example.com`

   Access the target website again and check whether the fault has been rectified.

   If the fault persists, perform the following operations to continue the fault locating.

### Checking Network Links

1. On the local client, ping the public IP address of the server to check whether packet loss or network delay occurs.
   
   - If packet loss or long network delay occurs, use MTR to locate the fault. For details, see [Troubleshooting a Ping Failure or Packet Loss Using a Link Test](https://www.example.com).
   
   - If not, go to step 2.

2. Run the `dig/nslookup` command to check whether the DNS resolution is functional.

   Alternatively, use the public IP address to access the target web page and check whether slow access is caused by a DNS fault.

   For details, see:

   - [Why Does My Record Set Not Take Effect?](https://www.example.com)
   
   - [How Do I Test Whether a Record Set Is Working?](https://www.example.com)

### Checking the ECS

1. Log in to the management console.

2. Click in the upper left corner and select the desired region and project.


4. In the search box above the upper right corner of the ECS list, enter the ECS name, IP address, or ID for searching.

5. Click the name of the target ECS. The page providing details about the ECS is displayed.

6. Click the *Monitoring* tab to view the monitoring data.

Check whether there are any applications running on the ECS have strict requirements on network and CPU configurations.
• If the CPU or memory usage is too high, see Troubleshooting High Bandwidth or CPU Usage of a Windows ECS or Troubleshooting High Bandwidth or CPU Usage of a Linux ECS for troubleshooting.

• If the bandwidth usage is too high, see Troubleshooting High Bandwidth Usage on an ECS for troubleshooting.
  
  − To upgrade ECS specifications, see General Operations for Modifying Specifications.
  
  − To upgrade the bandwidth, see Modifying EIP Bandwidth.

1.4 Troubleshooting a Website Access Error Occurred on an ECS

Scenarios

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.

If the website is inaccessible, the network is disconnected. In such a case, check whether the routing, port, security groups, and system firewall are correctly configured.

Routing Configurations

• Linux
  
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.

```
    route
Kernel IP routing table
Destination     Gateway      Genmask         Flags Metric    Ref    Use    Iface
default         gateway      0.0.0.0         UG    100     0      0      eth0
    gateway         0.0.0.0         UG    100     0      0      eth0
    gateway         255.255.255.0    U      101     0      0      eth1
    gateway         255.255.255.0    U      101     0      0      eth2
[root]#
```

b. Run the `ifconfig` or `ip addr` command to obtain the ECS IP address.
Figure 1-1 `ifconfig` command output

```
[root@elb-mq02 ~]# ifconfig -a
eth0: flags=4163<UP,BROADCAST, RUNNING, MULTICAST> mtu 1500
       inet 192.168.0.145 netmask 255.255.255.0 broadcast 192.168.0.255
       inet6 fe80::f826:3eff:fe24:1e7f prefixlen 64 scopeid 0x20<link>
       ether 00:16:33:24:1e:7f txqueuelen 1000 <bROADCAST,Multicast>
       RX packets 22750083 bytes 21186287838 (19.7 GiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 14951501 bytes 27529932634 (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 1-2 `ip addr` command output

```
[root@elb-mq02 ~]# ip addr
1: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/ether 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 noqueue state UP group default qlen 1000
   link/ether 00:16:33:24:1e:7f brd 00:00:00:00:00:ff
   inet 192.168.0.145/24 brd 192.168.0.255 scope global noprefixroute eth0
      valid_lft forever preferred_lft forever
   inet6 fe80::f826:3eff:fe24:1e7f prefixlen 64 scope link
      valid_lft forever preferred_lft forever
```

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

Figure 1-3 `route -n` command output

```
[root@elb-mq02 ~]# route -n
Kernel IP routing table
Destination Gateway      Genmask    Flags Metric Ref Use Iface
0.0.0.0      127.0.0.1         0.0.0.0     UG    100    0    0  eth0
192.168.1   192.168.0.1       0.0.0.0     UH    0    0    0    eth0
192.168.0.0  0.0.0.0           0.0.0.0     UG    100    0    0  eth0
```

- Windows
  a. Run `cmd.exe`.
  b. Run the `ipconfig` command to obtain the ECS IP address.
Figure 1-4 ipconfig command output

![ipconfig command output]

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

Figure 1-5 route print command output

![route print command output]

Port Communication

Ensure that service processes and ports are in **LISTEN** state. The following table lists common TCP statuses.

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

- **Linux**
  a. Run the `netstat -antp` command to check whether the port is in LISTEN state.

![Figure 1-6 Checking port listening status](image1)

- **Windows**
  Perform the following operations to check port communication:
  a. Run `cmd.exe`.
  b. Run the `Tasklist /svc | findstr "Ter"` command to obtain the TermService PID.

![Figure 1-7 Checking the TermService PID](image2)

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

![Figure 1-8 Checking the PID used by the process](image3)
Security Group Rules

If the port used by the target website or remote connection tool 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.
3. In the ECS list, click the name of the ECS with security group rules to be modified.
4. Click the Security Groups tab and view security group rules.
5. Click Modify Security Group Rule.
6. Configure the rule to allow the access of the port used by the website.

Firewall Configurations

- A Linux ECS cannot be logged in using SSH, and the login is successful after the system firewall is disabled.
  a. Run the `iptables -nvL --line-number` command to obtain firewall policies.
  b. Run the following commands to allow the access of default SSH port 22:

```bash
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -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. Use SSH to access the ECS again.

- A Windows ECS cannot be remotely logged in, and the login is successful after the OS firewall is disabled.
  a. Modify the firewall policy so that the remote access port on the local end is allowed on the firewall. The default port is TCP 3389.
  b. After the firewall policy is modified, log in to the ECS again.

1.5 Troubleshooting an Unreachable ECS Port

Scenarios

If a website cannot be accessed, the security group may deny traffic to the port used by the website or remote connection tool.

This section uses port 80 as an example to describe how to troubleshoot an unreachable ECS port.

Locating the Fault

If the affected ECS cannot provide the HTTP service, check whether the port used by the web service (TCP 80 by default) is working properly.

1. On the ECS management console, ensure that the port is permitted in the security group.
2. Remotely log in to the ECS and ensure that HTTP is enabled on it.
3. Ensure that the port is listened to properly. If not, change the listened IP address.
4. Ensure that HTTP is permitted on the ECS firewall.

Windows

The following uses an ECS running Windows Server 2012 with Internet Information Services (IIS) deployed as an example.

**Step 1** Ensure that port 80 is permitted in the security group.

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Computing**, 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. Make sure that the following security group rules have been added to the security group to which the ECS belongs:

![Security Group Rules](image)

**Step 2** Remotely log in to the ECS and verify that IIS is enabled on it.

1. In the **Server Manager** window, choose **Tools > Internet Information Services (IIS) Manager**.
   If this option is unavailable, IIS is not successfully deployed. In such a case, deploy IIS again.
2. In the **Internet Information Services (IIS) Manager** window, check the following information:
   - In the **Connections** navigation pane, right-click the ECS ID. If **Connect** is unavailable, IIS has been enabled.
   - Click **Sites**. Then, view the website status on the right side of the page. If the website is stopped, click the website and then **Start** under **Manage Server** on the right side of the page to start the website.

**Step 3** Check whether the port is properly listened to on the ECS.

Open the cmd window and run the following command:
netstat -ano | findstr :80

If information similar to the following is displayed, port 80 is being properly listened to on the entire network. If not, change the listened IP address.

---End

Linux

The following uses an ECS running CentOS 6 with Nginx deployed as an example.

Step 1 Ensure that port 80 is permitted in the security group.

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
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. Make sure that the following security group rules have been added to the security group to which the ECS belongs:
Step 2  Remotely log in to the ECS and ensure that Nginx is enabled on it.

Run the following command to check whether Nginx has been enabled:

```
systemctl status nginx
```

If the following information is displayed, Nginx has been enabled:

```
Sep 12 21:14:08 i77yvkk5yphz systemd[1]: Starting The nginx HTTP and reverse proxy server
Sep 12 21:14:08 i77yvkk5yphz nginx[9622]: nginx: the configuration file /etc/nginx/nginx.conf is missing
```

If Nginx has not been enabled, run the following command to enable it:

```
systemctl start nginx
```

Step 3  Run the following command to check whether the port is properly listened to on the ECS:

```
netstat -an | grep 80
```

If information similar to the following is displayed, port 80 is being properly listened to on the entire network. If not, change the listened IP address.

```
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN
```

Step 4  View the iptables rules of the ECS firewall.

Run the following command to obtain the iptables rules of the ECS firewall:

```
iptables --line -vnL
```
Elastic Cloud Server
Troubleshooting

1.6 Troubleshooting High Bandwidth Usage on an ECS

Scenarios

If an ECS responds slowly or even cannot be accessed, this issue may be caused by high bandwidth usage. To troubleshoot this issue, see this section.

Windows

1. Remotely log in to the ECS on the management console.
   The following uses an ECS running Windows Server 2012 as an example.
2. In the lower left corner of the ECS desktop, choose Start > Run.
3. In the Open dialog box, enter `perfmon -res`.

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

- If port TCP 80 is intercepted by default, run the following command to add a rule to permit the port:
  `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
- If port TCP 80 is set to DROP, run the following command to permit the port:
  `iptables -R INPUT [Rule ID for port TCP 80] -p tcp --dport 80 -j ACCEPT`
  Run the following command to save the rules:
  `service iptables save`

----End
5. View the processes with high bandwidth usage.
   − If such processes are service processes, you are advised to modify ECS specifications.
   − If such processes are abnormal ones, they may be caused by viruses or Trojan horses. You are advised to stop the processes or use security software to scan for and stop them.

Linux

1. Log in to the ECS through the management console.
The following uses an ECS running CentOS 6.8 64bit as an example.
2. Run the following command to install the Linux traffic monitoring tool iftop:

   ```bash
yum install iftop -y
   ```

3. Run the following command to check the ports that cause heavy traffic and the IP addresses that consume high bandwidth (taking port eth0 as an example):

   ```bash
   iftop -i eth0 -P
   ```
4. Run the following command to check the processes related to the port (taking port 38366 as an example):

```bash
netstat -tunlp | grep 38366
```

- `=>` indicates transmitted data, and `<=` indicates received data.
- `TX` indicates TX traffic, `RX` indicates RX traffic, and `TOTAL` indicates the total traffic.
- `cum` indicates the total traffic in the first column.
- `peak` indicates the peak traffic in the first column.
- `rates` indicates the average traffic within 2, 10, and 40 seconds in the first column.

5. View the processes with high bandwidth usage.

- If such processes are service processes, you are advised to modify ECS specifications.
- If such processes are abnormal ones, they may be caused by viruses or Trojan horses. You are advised to stop the processes or use security software to scan for and stop them.

## 1.7 Troubleshooting High Bandwidth or CPU Usage of a Windows ECS

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

To handle this issue, perform the following operations:

1. **Fault locating**: identifies the processes leading to high bandwidth or CPU usage.
   - Windows OSs offer multiple tools to locate faults, including Task Manager, Performance Monitor, Resource Monitor, Process Explorer, Xperf (supported by versions later than Windows Server 2008), and obtained full memory dump.

2. **Troubleshooting**: Check whether the processes are malicious and handle the issue accordingly.
   - If the processes are not malicious, optimize their programs or modify ECS specifications.
   - If the processes are malicious, use a third-party tool to automatically stop the processes.

### Locating the Fault

1. In the lower left corner of the ECS desktop, choose **Start > Run**.
2. In the **Open** dialog box, enter **perfmon -res**.
3. On the **Resource Monitor** page, click the **CPU** or **Network** tab to view the CPU or bandwidth usage.

4. Obtain the IDs and names of the processes with high CPU or bandwidth usage.

5. Press **Ctrl+Alt+Delete** to start Windows Task Manager.

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

   a. Click the **Processes** tab.
   
   b. Choose **View > Select Columns**.
c. Select **PID (Process Identifier)**.
d. Click OK.
   On the Processes tab, the PID column is displayed.

e. Click PID to sort the data.

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

g. Check whether the process is malicious.
Solution

Before troubleshooting, determine whether the process leading to the high CPU or bandwidth usage is malicious, and then take measure accordingly.

Suggestions for non-malicious processes

1. If your ECS runs Windows Server 2008 or 2012, ensure that the available memory capacity is 2 GB or higher.
2. Check whether Windows Update is running on the backend.
3. Check whether the antivirus software is scanning on the backend.
4. Check whether there are applications running on the ECS with strict requirements on CPU or bandwidth usage. If so, modify ECS specifications or enlarge bandwidth.
5. If the ECS configuration meets application requirements, deploy applications separately. For example, deploy the database and applications separately.

Suggestions for malicious processes

If the high CPU or bandwidth usage is due to viruses or Trojan horses, manually stop the affected processes. The recommended processing sequence is as follows:
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 **How to perform a clean boot in Windows**.
4. If the ECS or site encounters a DDoS or CC attack, which leads to a large number of access requests within a short period of time, log in to the management console and perform the following operations:
   - Check whether Anti-DDoS has been enabled and whether the protection rules are proper. To configure a protection rule, see **Enabling Anti-DDoS**.
   - Check whether CC attack protection has been enabled and whether the protection rules are proper. To configure a protection rule, see **Configuring CC Attack Protection Rules**.

### 1.8 Troubleshooting High Bandwidth or CPU Usage of a Linux ECS

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

To handle this issue, perform the following operations:

1. Fault locating: identifies the processes leading to high bandwidth or CPU usage.
2. Troubleshooting: Check whether the processes are malicious and handle the issue accordingly.
   - If the processes are not malicious, optimize their programs or modify ECS specifications.
   - If the processes are malicious, use a third-party tool to automatically stop the processes or manually stop them.

#### Common Commands

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

The common commands for checking Linux ECS performance metrics, such as 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, 2:39, 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 sw, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 30988224 total, 2963304 free, 1735564 used, 730336 buff/cache
KiB Swap: 0 total, 0 free, 0 used, 3413008 available
```

<table>
<thead>
<tr>
<th>PID</th>
<th>USER</th>
<th>PR</th>
<th>NI</th>
<th>VIRT</th>
<th>RES</th>
<th>SHR</th>
<th>S</th>
<th>%CPU</th>
<th>%MEM</th>
<th>TIME+</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>161956</td>
<td>2216</td>
<td>1564</td>
<td>R</td>
<td>0.3</td>
<td>0.1</td>
<td>0:00.01</td>
<td>top</td>
</tr>
<tr>
<td>1</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>125416</td>
<td>2614</td>
<td>2595</td>
<td>S</td>
<td>0.0</td>
<td>0.1</td>
<td>0:11.32</td>
<td>systemd</td>
</tr>
<tr>
<td>2</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>65871</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>3</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>4</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>kswapd/0</td>
</tr>
<tr>
<td>5</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>kswapd/0</td>
</tr>
<tr>
<td>6</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>kswapd/0</td>
</tr>
<tr>
<td>7</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>kswapd/0</td>
</tr>
<tr>
<td>8</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>kswapd/0</td>
</tr>
<tr>
<td>9</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>kswapd/0</td>
</tr>
<tr>
<td>10</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>kswapd/0</td>
</tr>
</tbody>
</table>

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.
   - i: 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 **ls /proc/PID/exe** command to obtain the program file specified by a PID.

**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: 01 total, 1 running, 79 sleeping, 0 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: 3889824 total, 2961520 free, 928328 used, 735644 buff/cache
   PID USER PR NI VIQT RES SHR S %CPU %MEM TIME COMMAND
   1 root 20 0 125100 3004 2604 S 0.0 0.1 0:11:32 system
   z root 20 0 0 0 S 0.0 0.0 0:00.00 kthreadd
   2
   ```

   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: 01 total, 1 running, 79 sleeping, 0 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: 3889824 total, 2961520 free, 928328 used, 735644 buff/cache
   PID USER PR NI VIQT RES SHR S %CPU %MEM TIME COMMAND
   1 root 20 0 125100 3004 2604 S 0.0 0.1 0:11:32 system
   z root 20 0 0 0 S 0.0 0.0 0:00.00 kthreadd
   2
   ```

   • For the kswapd0 process

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

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

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

   ```
   top - 21:07:38 up 37 days, 9:21, 1 user, load average: 0.01, 0.02, 0.05
   Tasks: 01 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: 3889824 total, 3014120 free, 875704 used, 764100 buff/cache
   PID USER PR NI VIQT RES SHR S %CPU %MEM TIME COMMAND
   1 root 20 0 125100 3004 2604 S 0.0 0.1 0:11:32 system
   z root 20 0 0 0 S 0.0 0.0 0:00.00 kthreadd
   2
   ```

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

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

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

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

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

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

   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`:

     ```bash
     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 1.
     - `-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:

     ```bash
     nethogs eth1
     ```

     The parameters in the command output are as follows:
     - `PID`: ID of the process.
     - `USER`: user who runs the process.
     - `PROGRAM`: IP addresses and port numbers of the process and connection, respectively. The former is for the server and the latter is for the client.
     - `DEV`: Network port to which the traffic is destined.
     - `SENT`: Volume of data sent by the process per second.
     - `RECEIVED`: Volume of data received by the process per second.

  c. Stop malicious programs or blacklist malicious IP addresses.

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

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

- Using Web Application Firewall (WAF) to protect the 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 CC Attack Protection Rules.
1.9 How Can I Handle Slow ECS Startup?

If an ECS requires a long period of time to start, you can change the default timeout to speed up the startup.

1. Log in to the ECS.
2. Run the following command to switch to user root:
   ```
   sudo su
   ```
3. Run the following command to obtain the grub version:
   ```
   rpm -qa | grep grub
   ```

   ![Figure 1-9 Viewing the grub version](image)

4. Change the timeout in the grub file to 0s.
   - If the grub version is earlier than 2:
     Open the `/boot/grub/grub.cfg` or `/boot/grub/menu.lst` file and change the `timeout` value to 0.
   - If the grub version is 2:
     Open the `/boot/grub2/grub.cfg` file and change the `timeout` value to 0.

   ![Figure 1-10 Changing timeout duration](image)

1.10 Troubleshooting Multi-IP-Address Access on an ECS with Multiple NICs Attached

**Symptom**

If an ECS has multiple NICs, perform the following operations to configure policy-based routing for the ECS to enable the network communication of secondary NICs.

**Possible Causes**

No routing rules are configured for the EIPs bound to the extension NICs.
### Linux

1. Run the following command and add two route tables (net1 and net2) and their priorities to the `/etc/iproute2/rt_tables` file. The priorities of net1 and net2 are 252 and 251, respectively. A smaller value indicates a higher priority.

   ```bash
   vi /etc/iproute2/rt_tables
   # added for dual net
   252     net1
   251     net2
   ```

2. Run the following command and add the NIC routing information to the `/etc/rc.local` file:

   ```bash
   vi /etc/rc.local
   The IP addresses of NICs eth0 and eth1 are 192.168.1.23 and 192.168.2.4, respectively. The subnet mask is 24 bits. The gateway addresses of NICs eth0 and eth1 are 192.168.1.1 and 192.168.2.1, respectively. The information to be added is as follows:
   # Request IP address for eth1
dhclient eth1
   # Add routes
   ip route flush table net1
   ip route add default via 192.168.1.1 dev eth0 src 192.168.1.23 table net1
   ip route add 192.168.1.0/24 dev eth0 src 192.168.1.23 table net1
   ip rule add from 192.168.1.23 table net1
   ip route flush table net2
   ip route add default via 192.168.2.1 dev eth1 src 192.168.2.4 table net2
   ip route add 192.168.2.0/24 dev eth1 src 192.168.2.4 table net2
   ip rule add from 192.168.2.4 table net2
   ```

3. Run the following command to add the execute permission for the `rc.local` file:

   ```bash
   chmod +x /etc/rc.local
   ```

4. Run the `reboot` command to restart the ECS.

### Windows

1. Choose Control Panel > Network and Internet > Network Connections. Right-click Local Area Connection 2 and then click Properties.

   ![Control Panel window](image)

   **NOTE**
   
   Right-click to add NICs based on the site requirements.


3. Click Properties.


5. On the IP Settings tab, click Add in the Default gateways area.
6. Enter the gateway address of the secondary NIC and click **Add**.

![Advanced TCP/IP settings](image)

**Figure 1-11** Advanced TCP/IP settings

7. Click **OK**.

![TCP/IP Gateway Address](image)

**Figure 1-12** TCP/IP Gateway Address
2.1 Retaining a Session on a Windows ECS

Scenarios

This section describes how to configure a Windows ECS so that its remote desktop connection will not be automatically disconnected.

Procedure

The following uses an ECS running Windows Server 2008 as an example.

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

   **Figure 2-1** `gpedit.msc`

   ![gpedit.msc dialog box](image)

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

   - **Open:** `gpedit.msc`

   - **This task will be created with administrative privileges.**

   - **OK**
   - **Cancel**
   - **Browse...**

3. Set time limit for disconnected sessions.
   - Select **Enabled**.
   - Set **End a disconnected session** to **Never**.

4. Set time limit for active but idle Remote Desktop Services sessions.
   - Select **Enabled**.
   - Set **Idle session limit** to **Never**.
2.2 Troubleshooting Difference Between System Time and Local Standard Time

Symptom

The system time on my Windows ECS is different from the local standard time.

Possible Causes

Affected by the network state, some drivers, or processes, the system time may be different from the standard time.
Solution 1

Manually synchronize system time.

1. Click Change date and time settings in the lower right corner of the desktop. The Date and Time window is displayed.

Figure 2-3 Date and time

2. Click the Internet Time tab.
3. Click **Change settings** and select a time source. The default time source is **time.windows.com**.

4. Click **Update now** and then click **OK**.
5. Check whether system time is consistent with the local standard time.

**Solution 2**

**Change the update frequency of system time by editing the Windows registry.**

1. In the **Run** dialog box, enter `regedit` to access the registry editor.
2. Choose `HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > TimeProviders > NtpClient` and double-click `SpecialPollInterval`.
3. In the dialog box that is displayed, set **Base** to **Decimal**.
4. Set the time synchronization interval.

The value displayed in **Value data** is the interval (in seconds) for automatic time synchronization. Set this parameter as required.

**Figure 2-6 Setting the time synchronization interval**

5. Click **OK**.
6. After the configuration is complete, enter `cmd` to open the CLI and run the following command to update the group policy: `gpupdate`

7. Check the Internet time. As shown in Figure 2-7, the time synchronization frequency is changed to once every 15 minutes.

### Figure 2-7 Viewing time synchronization frequency

![Figure 2-7 Viewing time synchronization frequency](image)

## 2.3 Troubleshooting Internet Access on an Extension NIC Newly Attached to a Windows ECS

### Scenarios

A Windows ECS has one primary NIC and one extension NIC attached. Both the NICs have an EIP bound to access the Internet.

### Constraints

Do not modify the primary NIC settings.

### Procedure

1. Log in to the management console and click **Elastic Cloud Server** under **Computing**.
2. On the **Elastic Cloud Server** page, select the target ECS.
3. Click the name of the ECS to switch to the page providing details about the ECS.
4. Click the **NICs** tab.
5. Click **Add NIC** and add an extension NIC as prompted.
   - Ensure that the security group and subnet of the extension NIC are the same as those of the primary NIC.
   - After the extension NIC is added, the system automatically obtains a private IP address.
6. Remotely log in to the ECS.
7. Click **Open Network and Sharing Center** in the lower right corner. Then, click **Change adapter settings** in the upper left corner and find the newly added NIC.
8. Right-click the target network connection and choose **Properties** from the shortcut menu.

9. In the **Local Area Connection 3 Properties** dialog box, click the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)**, and click **Properties**.

10. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, click the **General** tab and configure the private IP address automatically obtained in step 5 for the newly added NIC.

   ![Internet Protocol Version 4 (TCP/IPv4) Properties dialog box]

   Example configurations:
   - Private IP address: 192.168.1.11
   - IP address: 192.168.1.11
   - Subnet mask: 255.255.255.0
   - Default gateway: 192.168.1.1
   - Preferred DNS server: 114.114.114.114
   - Alternate DNS server: 114.114.115.115

11. After the configuration, select **Validate settings upon exit**.

12. Restart the NIC and bind an EIP to it.
2.4 Troubleshooting Disabled Copy and Paste Options

Symptom

After remotely logging in to a Windows ECS, I cannot copy or paste content and find that the Paste option grayed out.

Possible Causes

- Local drive is not mapped.
- An error has occurred in the rdpclip.exe process.
- Data cannot be copied and pasted between the ECS and the local server.

Solution

- The local drive is not mapped. Figure 2-8 uses local drive C and drive D as an example.
  a. Open the Run dialog box, enter mstsc, and click OK to start Remote Desktop Connection.
  b. Click the Local Resources tab and select Clipboard in the Local devices and resources pane. Click More and select the drives you want to use in the remote session.
  c. Click OK and check whether the copy and paste options work.

![Figure 2-8 Local resources](image)

- An error has occurred in the rdpclip.exe process.
  a. Enable remote desktop connection, start Windows Task Manager, and stop the rdpclip.exe process on the Processes tab page.
Figure 2-9 Ending the rdpclip.exe process

![Windows Task Manager](image)

b. Open the Run dialog box, enter rdpclip.exe, and click OK to restart it.

Figure 2-10 Starting the rdpclip.exe process

![Run dialog box](image)

c. Check whether the copy and paste options work.
   
   - Data cannot be copied and pasted between the ECS and the local server.
   
   a. Choose Start > Run. In the Run dialog box, enter gedit.msc and click OK to start Local Group Policy Editor.
   
   
   c. Set Do not allow Clipboard redirection, Do not allow COM port redirection, Do not allow drive redirection, and Do not allow LPT port redirection to Disabled.
d. Restart the ECS and check whether the copy and paste options work.

2.5 Configuring File Sharing and Network Disk Mapping for a Windows ECS

Scenarios

This section describes how to share a folder between Windows ECSs over an intranet.

Constraints

Some carriers may block ports 139 and 445. As a result, you cannot access the shared folders over the Internet. Therefore, you are advised to share a folder between Windows ECSs only over an intranet.

Procedure

Step 1 Check whether the two Windows ECSs that are to share a folder are correctly configured.

- Ensure that TCP/IP NetBIOS Helper is started.
  Open the CLI, run the services.msc command, and locate TCP/IP NetBIOS Helper to check its status.
Ensure that **Enable NetBIOS over TCP/IP** is selected on the NIC.

**Figure 2-12** Tcp/IP NetBIOS Helper

- Ensure that the inbound rules are added for ports 139 and 445 on the Windows ECS firewall.

**Step 2** Configure **Network and Sharing Center**

1. Click **Open Network and Sharing Center**.
2. Click **Change advanced sharing settings**.
3. Ensure the network types of the two Windows ECSs are same. For example, both are public or private. Select **Turn on network discovery** and **Turn on sharing so anyone with network access can read and write files in the Public folder**.

If the network discovery function cannot be enabled, you can run the `services.msc` command to start the Services manager. Check whether the following services on which the network discovery function depends are enabled:

- Function Discovery Resource Publication
- SSDP Discovery
- UPnP Device Host
4. In the Services manager, start the **Workstation** service. This service depends on the **Computer Browser** and **Remote Desktop Configuration** components. Before starting the **Workstation** service, you need to start the two components.

**Figure 2-16 Enabling the Workstation service**

![Enabling the Workstation service](image)

**Step 3** Configure disk sharing on the ECS that needs to access the shared disk.

1. Right-click the disk to be shared and select **Properties**.
2. Click the **Sharing** tab and then click **Advanced Sharing**.
3. Set **Share name** and click **OK**.
   Customize a name for the folder to be shared.

**Figure 2-18** Entering a name for the folder to be shared
Step 4  Start another ECS in the same region and access the shared folder over the intranet.

1. Start the **Run** dialog box.
2. Enter `\Intranet IP address\123` and click **OK** to open the shared folder.

**Figure 2-19** Assessing the shared folder

![Search](image)

Step 5  (Optional) Create a network drive mapping for the shared path. Perform this operation to access the shared folder more conveniently.

1. Click **Map network drive**.

**Figure 2-20** Creating a mapping

![Creating a mapping](image)

2. Map the network drive.
3. Right-click the name of the mapped network drive, choose **Create Shortcut**, and send the shortcut to the desktop.

4. Double-click the shortcut to quickly access the shared folder.

---End

### 2.6 Troubleshooting an In-Service Port During Tomcat Startup

**Symptom**

The system prompts that the required port is being used when Tomcat is started on a Windows ECS.
This section uses Windows Server 2008 R2 and port 80 as an example describe how to resolve this issue.

**Possible Causes**

The port 80 required by Tomcat is being used by other programs, viruses, or Trojan horses.

1. Run the `netstat -ano | find "80"` command and find that the ID of the process that is using port 80 is 4.

   **NOTE**
   
   Change the port number as required.

   ![Figure 2-23 Checking the process using port 80](image)

2. Run the `tasklist /svc | find "4"` command and find that the process using port 80 is the System process.

   **NOTE**
   
   Change the process ID as required.

   ![Figure 2-24 System process](image)

Port 80 is used by the System process.

**Solutions**

**NOTE**

Stopping the process that is using port 80 may stop the applications that are running or restart the ECS.

**Solution 1:**

1. Run the `cmd` command as the administrator and enter `net stop http`.
2. To stop the process that is using port 80, enter `y`.
3. Run the `sc config http start= disabled` command.

**Solution 2:**

1. In the `cmd` window, run `regedit` to open the registry editor.
2. In Registry Editor, choose `HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > HTTP` and change the value of `Start` to `0`.
3. Restart the ECS.
2.7 Troubleshooting Unavailable Input Methods

Symptom
- On your Windows ECS, you cannot switch input methods using Ctrl+Shift. The input method is not shown.
- You do not know how to add a language to the input methods.

Possible Causes
- The ctfmon.exe process is not started.
- The input indication icon is turned off.

Solutions to Unavailable Input Methods
Check whether the ctfmon.exe process is started.
1. Open the C:\Windows\System32 file.
2. Double-click ctfmon.exe and check whether the input method is shown in the lower right corner and whether you can switch the input method.
3. Enable the automatic input method startup upon ECS startup.
   a. In the Run dialog box, enter regedit and click OK to open the registry editor.
   b. In the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run directory, create a file named ctfmon.exe in string type.
   c. Right-click the file you create and click Modify. Change the value data to C:\Windows\System32\ctfmon.exe in which ctfmon.exe is stored.
Figure 2-26 Editing the value data

<table>
<thead>
<tr>
<th>Value name:</th>
<th>ctfmon.exe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value data:</td>
<td>C:\Windows\System32\ctfmon.exe</td>
</tr>
</tbody>
</table>

OK Cancel

In the Run dialog box, enter **msconfig** and click **OK** to open the System Configuration.

Click the Start tab, find and select **ctfmon.exe**, and click **Apply** and **OK**. Save the configurations and log out. Restart the ECS.

Figure 2-27 Selecting ctfmon.exe

Enable the input indication icon.

1. Log in to the ECS and click **Customize** in the lower right corner.
2. In the Notification Area Icon window, click Turn system icons on or off.

3. Set Input Indicator to On and click OK.
Adding Another Input Language

For example, add Japanese on an ECS running Windows Server 2008.

1. Log in to the ECS and choose Start > Control Panel.
2. Click Region and Language.

3. On the Keyboards and Languages tab, click Change keyboards.
4. Right-click the language bar and click **Settings** to open the **Text Services and Input Languages** dialog box. On the **General** tab, click **Add**.
5. In the **Add Input Language** dialog box, find and double-click **Japanese (Japan)** and then **Keyboard**.
6. Select **Japanese** and **Microsoft IME**. Click **OK** and then **Apply** to save the configurations.
2.8 Troubleshooting File Sharing Between Windows ECSs

Scenarios

This section describes how to share files between Windows ECSs in the same subnet.

Prerequisites

ECSs that share files are in the same subnet and can communicate with each other.

Procedure

1. Log in to the ECS. Right-click the Network icon in the lower right corner and choose Open Network and Sharing Center from the shortcut menu.
2. Click **Change advanced sharing settings**. On the displayed page, select **Turn on file and printer sharing** for the Private and Guest or Public areas and click **Save changes**.

3. In the **cmd** window, run the **services.msc** command, find and enable the TCP/IP NetBIOS Helper service.
   
   If the service is disabled, right-click it and choose **Properties** from the shortcut menu. Set the **Startup Type** to **Automatic** or **Manual** and then enable the service.
2.9 Troubleshooting Data Restoration in the Event of a Startup Failure on a Windows ECS

Symptom

If logging in to a Windows ECS failed, the system automatically starts the recovery option. However, an error is reported after the recovery option is selected, and the system recovery cannot continue.

Possible Causes

Windows files have been damaged.

Solution

1. Log in to the management console and click Elastic Cloud Server under Computing.
2. Detach data disks from the ECS.
   Click the name of the target ECS. On the page providing details about the ECS, click the Disks tab. Locate the target disk and click Detach.
3. Reinstall the OS of the ECS.
   Locate the row containing the target ECS. Click More in the Operation column and select Reinstall OS.
If the ECS is not **Stopped**, stop the ECS before proceeding with reinstallation. Reinstalling the OS will clear the system disk. Back up data before proceeding with reinstallation.

4. Attach the data disk to the ECS again and check whether you can log in to the ECS.

### 2.10 Viewing Login Logs of a Windows ECS

#### Scenarios

This section describes how to view the login logs of a Windows ECS.

#### Procedure

The following operations are performed on an ECS running Windows Server 2012.

1. Log in to the ECS.
2. Choose **Start > Administrative Tools > Event Viewer**.

   ![Event Viewer Window](image)

   **Procedure**

   3. On the **Event Viewer** window, choose **Windows Logs > Security > Filter Current Logs**.
4. Filter events with ID 4776 to obtain remote login logs.

**NOTE**

You can also use 4624 and 4625 to view login information.
- 4624: ID of successful login events
- 4625: ID of failed login events
5. Right-click an event and choose **Event Properties** from the shortcut menu. The logon account of the event is displayed.
3 Linux Issues

3.1 Troubleshooting Emergency Mode

Symptom
When a Linux ECS enters the emergency mode during startup, the system displays the message “Welcome to emergency mode” and asks you to enter the password of user root for maintenance.

Possible Causes
The emergency mode allows you to recover the system even if the system fails to enter the rescue mode. In emergency mode, the system installs only the root file system for data reading. It does not attempt to install any other local file systems or activate network interfaces.

The emergency mode is generally due to:

- An error occurred in the /etc/fstab file, leading to the failure in mounting the file system.
- An error occurred in the file system.

Constraints
The operations in this section are applicable to the Linux emergency mode. The operations involve recovering the file system, which may lead to loss of data. Therefore, back up data before recovering the file system.

Solution
1. Enter the password of user root and press Enter to enter the recovery mode.
2. In emergency mode, the root partition is mounted in read-only mode. To modify the files in the root directory, run the following command to mount the root partition in read-write mode:

```
# mount -o rw,remount /
```

3. Run the following command to try to mount all unmounted file systems and check whether the `fstab` file is correct:

```
# mount -a
```

- If the message "mount point does not exist" is displayed, the mount point is unavailable. In such a case, create the mount point.
- If the message "no such device" is displayed, the file system device is unavailable. In such a case, comment out or delete the mount line.
- If the message "an incorrect mount option was specified" is displayed, the mount parameter has been incorrectly set. In such a case, correct the parameter setting.
- If no error occurs and the message "UNEXPECTED INCONSISTENCY:RUN fsck MANUALLY" is displayed, the file system is faulty. In such a case, go to step 7.

4. Run the following command to open the `/etc/fstab` file and correct the error:

```
# vi /etc/fstab
```

The `/etc/fstab` file contains the following parameters separated by space:

<table>
<thead>
<tr>
<th>[file system]</th>
<th>[dir]</th>
<th>[type]</th>
<th>[options]</th>
<th>[dump]</th>
<th>[fsck]</th>
</tr>
</thead>
</table>

**Table 3-1 /etc/fstab parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| [file system] | Specifies the partition or storage device to be mounted. You are advised to set file system in UUID format. To obtain the UUID of a device file system, run the `blkid` command. Format for reference: 

```
# <device> <dir> <type> <options> <dump> <fsck>
```

UUID=b411dc99-9f0a0-4c87-9e05-184977be8539 /home ext4  defaults 0 2

UDIDs are independent of disk order. If the sequence of storage devices is changed manually or undergoes some random changes by some BIOSs, or the storage devices are removed and installed again, using UDIDs is more effective. |
| [dir] | Specifies the mount point of a file system. |
| [type] | Specifies the type of the file system to which a device or partition is mounted. The following file systems are supported: ext2, ext3, ext4, reiserfs, xfs, jfs, smbfs, iso9660, vfat, ntfs, swap, and auto. If type is set to auto, the `mount` command will speculate on the type of the file system that is used, which is useful for mobile devices, such as CD-ROM and DVD. |
| [options] | Specifies the parameters used for mounting. Some parameters are available only for specific file systems. For example, defaults uses default mounting parameters of a file system. The default parameters of the ext4 file system are rw, suid, dev, exec, auto, nouser, and async. For more parameters, run the `# man mount` command to view the man |
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[dump]</td>
<td>Specifies whether file system data is backed up. The parameter value can be 0 or 1. 0 indicates that data is not backed up, and 1 indicates that data is backed up. If you have not installed dump, set the parameter value to 0.</td>
</tr>
<tr>
<td>[fsck]</td>
<td>Specifies the sequence of checking file systems. The parameter value can be 0, 1, or 2. 0 indicates that the devices will not be checked by fsck. 1 indicates the highest priority of the root directory to be checked by fsck, and 2 indicates the lower priority of other devices to be checked.</td>
</tr>
</tbody>
</table>

5. After the modification, run the following command to check the `fstab` file:
   ```shell
   # mount -a
   ```

6. Run the following command to restart the ECS:
   ```shell
   # reboot
   ```

7. If no error occurred, the fault may be caused by the file system. Then, run the following command:
   ```shell
   # dmesg |grep "ext[2..4]|xfs" |grep -i error
   ```

   **NOTE**
   - If the error message "I/O error... inode" is displayed, the fault is caused by a file system error.
   - If no file error is found in the log system, the fault is generally caused by the damaged superblock. The superblock is the header of the file system. It records the status, size, and idle disk blocks of the file system.
   - If the superblock of a file system is damaged, for example, data is written to the superblock partition of the file system by mistake, the system may fail to identify the file system. As a result, the system enters the emergency mode during startup. The ext2fs file system backs up the superblock and stores the backup at the blockgroup boundary of the driver.

8. Run the following command to unmount the directory where the file system error occurred:
   ```shell
   # Unmount Mount point
   ```

9. Check and recover the damaged file system.

---

**NOTICE**

Recovering the file system may lead to loss of data. Back up data before the recovery.

- For the ext file system, run the following command to check whether the file system is faulty:
  ```shell
  # fsck -n /dev/vdb1
  ```

   **NOTE**
   If the message "The super block Cloud no be read or does not describe a correct ext2 filesystem" is displayed, go to step 10.

   To recover the file system, run the following command:
# fsck /dev/vdb1
- For the xfs file system, run the following command to check whether the file system is faulty:

# xfs_repair -n /dev/vdb1

To recover the file system, run the following command:

# xfs_repair /dev/vdb1

10. (Optional) If the message "The super block Cloud no be read or does not describe a correct ext2 filesystem" is displayed, the superblock is damaged. In such a case, use the superblock backup for recovery.

Figure 3-2 Damaged superblock

Run the following command to replace the damaged superblock using the superblock backup:

# e2fsck -b 8193 Device name

As shown in Figure 3-3, the superblock has been replaced.

Figure 3-3 Replacing the damaged superblock

```
[root@ecs ~]# e2fsck -b 8193 /dev/xvda
e2fsck 1.41.12 (17-May-2018)
/dev/xvda is in use.
e2fsck: Cannot continue, aborting.
```

**NOTE**

- **-b 8193** indicates that the backup of superblock 8193 in the file system is used. The backup is used when the active superblock is damaged. The location of the superblock backup varies depending on the block size of the file system.
  
  For a file system with a 1 KB block size, locate the backup at superblock 8,193.
  
  For a file system with a 2 KB block size, locate the backup at superblock 16,384; for a 4 KB block size, locate the backup at superblock 32,768.

- **Device name** is the disk name but not the partition name.

11. Run the following command to restart the ECS:

# reboot
3.2 What Can I Do If Switching from a Non-root User to User root Times Out?

Symptom

When you run the `sudo` command to switch to user `root` on a Ubuntu or Debian ECS, the system prompts connection timeout.

Figure 3-4 Connection timeout

```
linux@ubuntu-test-1:/etc$
linux@ubuntu-test-1:/etc$ sudo su
sudo: unable to resolve host ubuntu-test-1: Connection timed out
root@ubuntu-test-1:/etc#
```

Solution

1. Log in to the ECS.
2. Run the following command to edit the hosts configuration file:
   ```bash
   vi /etc/hosts
   ```
3. Press `i` to enter editing mode.
4. Add the IP address and hostname to the last line of the hosts configuration file.
   ```bash
   Private IP address hostname
   ```
   An example is provided as follows:
   If the ECS hostname is `hostname` and the private IP address of the ECS is 192.168.0.1, add the following statement:
   ```bash
   192.168.0.1 hostname
   ```
5. Press `Esc` to exit editing mode.
6. Run the following command to save the configuration and exit:
   ```bash
   :wq
   ```

**NOTE**

To update the hostname of a Ubuntu or Debian ECS, set the value of parameter `manage_etc_hosts` in the `/etc/cloud/cloud.cfg` file to `false` and update the new hostname in the `/etc/hosts` file. When editing the `/etc/hosts` file, do not delete the statement in the line where `127.0.0.1` is located. Otherwise, switching from a non-root user to user `root` will time out.
4 Managing Disk Space

4.1 Troubleshooting the Creation of a Swap Partition or File on Linux

Scenarios

This section uses an ECS running CentOS 6.8 as an example to describe how to create a swap partition.

Constraints

A file of a specified size is to be created. Therefore, ensure that the available system disk capacity meets the task requirement.

Scenario 1: Creating a Swap Partition on a Block Storage Device

1. Run the following command to create a partition of 2 GB, for example:

   # fdisk /dev/vdb

   Information similar to the following is displayed:

   Command (m for help): n
   Partition type:
   p primary (0 primary, 0 extended, 4 free)
   e extended
   Select (default p):
   Using default response p
   Partition number (1-4, default 1):
   First sector (2048-20971519, default 2048):
   Using default value 2048
   Last sector, +sectors or +size(K,M,G) (2048-20971519, default 20971519): +2G
   Partition 1 of type Linux and of size 2 GiB is set
   Command (m for help): p

   Disk /dev/vdb: 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: 0x1f02f438
Managing Disk Space

### Issue 01 (2020-07-23)

#### Scenario 2: Creating a Swap Partition Using a Block Storage Device Simulated by a File

**NOTE**

The performance of the block storage device simulated by a file is not as good as that of the passthrough block storage device.

1. Run the following command to create a swap file of 1 GB, for example:
   ```shell
   # dd if=/dev/zero of=/swapfile bs=1M count=1000
   ```
2. Run the following command to modify the file:
   ```shell
   # chmod 600 /swapfile
   ```
3. Run the following command to modify the file attribute:
   ```shell
   # mkswap /swapfile
   ```
4. Run the following command to enable swap:
   ```shell
   # swapon /swapfile
   ```
5. Enable automatic swap partition mounting upon system startup and write the mounting information to `/etc/fstab`.
   ```shell
   # echo "UUID=1ee90e3c-1538-453b-9240-ad430f835f6f swap swap defaults 0 0" >>/etc/fstab
   ```
6. Run the following command to mount the swap partition:
   ```shell
   # mount -a
   ```
5 Multi-user Login Issues

5.1 Troubleshooting Multi-User Logins for an ECS Running Windows Server 2012

Scenarios

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

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

**NOTE**
- The configuration in this section enables concurrent logins by multiple users or multiple concurrent logins using one account. However, a remote desktop license is valid for only 120 days. After the license expires, multi-user logins will be unavailable. For details about how to activate a remote desktop license, see [Applying for a License for Authenticating Multi-User Sessions and Activating the ECS](#).

Procedure

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

Configuring Remote Desktop Session Host and Remote Desktop Licensing

1. Log in to the Windows ECS.
2. On the OS, click ![Server Manager](#) to open Server Manager. Click Add roles and features.
Figure 5-1 Adding roles and features

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

Figure 5-2 Selecting an installation type

4. Choose Server Selection, select Select a server from the server pool, and click Next.

5. Choose Server Roles, select Remote Desktop Services, and click Next.
6. On the Features page, retain default settings and click Next twice.

Figure 5-4 Features

7. On the Role Services page, select Remote Desktop Session Host and Remote Desktop Licensing. In the displayed dialog box, click Add Features and then Next.
8. Confirm installation selections and click **Install**.
9. After the installation is complete, restart the destination server as prompted and click Close.

**Figure 5-8 Installation progress**
Enabling Multi-User Logins

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

   **Figure 5-9 gpedit.msc**

   ![gpedit.msc](image)

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

   Open: `gpedit.msc`

   This task will be created with administrative privileges.

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

   **Figure 5-10 Configuring Connections**

   ![Connections](image)

3. Right-click **Allow users to connect remotely by using Remote Desktop Services** and choose **Edit**. Then, set the status to **Enabled**.
### Figure 5-11 Allowing users to connect remotely by using Remote Desktop Services

<table>
<thead>
<tr>
<th>Allow users to connect remotely by using Remote Desktop Services</th>
<th>Previous Setting</th>
<th>Next Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] Not Configured</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ ] Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ ] Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Options:**

- **Comment:**
- **Supported on:** At least Windows Server 2003 operating systems or Windows XP Professional

**Help:**

- This policy setting allows you to configure remote access to computers by using Remote Desktop Services.
- If you enable this policy setting, users who are members of the Remote Desktop Users group on the target computer can connect remotely to the target computer by using Remote Desktop Services.
- If you disable this policy setting, users cannot connect remotely to the target computer by using Remote Desktop Services. The target computer will maintain any current connections, but will not accept any new incoming connections.
- If you do not configure this policy setting, Remote Desktop Services uses the Remote Desktop setting on the target computer to determine whether the remote connection is allowed. This setting is found on the Remote tab in the System properties sheet. By default, remote connections are not allowed.
- Note: You can limit which clients are able to connect remotely by using Remote Desktop Services by configuring the policy.

4. **Set Limit number of connections** to **Enabled** and set the number based on site requirements.
5. Set **Restrict Remote Desktop Services users to a single Remote Desktop Services session** to **Enabled** or **Disabled** as required. In this example, **Enabled** is selected.
   - **Enabled**: allows concurrent logins by multiple users, but not allowing multiple logins using one account.
     For example, users A, B, and C can concurrently log in to an ECS using account A, B, and C, respectively. However, users A, B, and C cannot use the same account to log in to the ECS.
   - **Disabled**: allows multiple users to concurrently log in to an ECS using one account.
     For example, users A, B, and C can use the same account to concurrently log in to an ECS.

---

**Figure 5-12 Setting limit number of connections**

Set **Restrict Remote Desktop Services users to a single Remote Desktop Services session** to **Enabled** or **Disabled** as required. In this example, **Enabled** is selected.

- **Enabled**: allows concurrent logins by multiple users, but not allowing multiple logins using one account.
  
  For example, users A, B, and C can concurrently log in to an ECS using account A, B, and C, respectively. However, users A, B, and C cannot use the same account to log in to the ECS.

- **Disabled**: allows multiple users to concurrently log in to an ECS using one account.
  
  For example, users A, B, and C can use the same account to concurrently log in to an ECS.
6. Run `cmd` and then `gpupdate /force` to forcibly start Local Group Policy Editor and restart the ECS.

Adding a New User to the Remote Desktop Users Group

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

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

2. Select Users, right-click the blank area, and choose New User from the shortcut menu.
3. Set user information and click Create.

5. In the Select Users dialog box, click Advanced.
Figure 5-18 Selecting users (Advanced)

6. Click **Find Now**, select the user for remote login in the search results, and click **OK**.
Figure 5-19 Selecting users (Find Now)
7. Click **OK** to add the user to the Remote Desktop Users group.
5.2 Troubleshooting a Browser Launch Error Occurred in Multi-User Login

Symptom

Solution
This section uses Internet Explorer as an example.

1. Right-click the browser icon and choose Create shortcut.
2. Right-click the created shortcut and choose Properties.

Follow-up Operations
For instructions about how to activate Remote Desktop Licensing, see Applying for a License for Authenticating Multi-User Sessions and Activating the ECS.
3. On the **Shortcut** tab, add the following content to the end of **Target**.

   \[ --user-data-dir="c:\MyInternetExplorerData" \]

   **NOTE**

   - There is a space between `.exe` and `--user`.
   - `c:\MyInternetExplorerData` indicates the directory where the Internet Explorer data files are stored. You can set it to any valid directory. If this directory does not exist, the browser automatically creates one.

   **Figure 5-22** Internet Explorer properties

   ![Internet Explorer properties]

   4. Save the modification and multiple users can use the browser at the same time.
5.3 Applying for a License for Authenticating Multi-User Sessions and Activating the ECS

Scenarios

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

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

Procedure

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

Applying for a License for Authenticating Multi-User Sessions

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

Figure 5-23 Selecting RD Licensing Manager

4. Right-click the unactivated server and choose Properties from the shortcut menu.
5. In the Properties dialog box, set Connection Method to Web Browser. Record the product ID which will be required for obtaining a server license.

**NOTICE**

If the destination server is not displayed in RD Licensing Manager, choose Action > Connect, and enter the server IP address.
Figure 5-25 Web browser for connection

6. Set parameters and click OK.

**Figure 5-27 Activating the license server**

8. Set parameters and click Next. Confirm the product information and click Next.
9. Record the license server ID and click Yes.

**Figure 5-29** Obtaining the license server ID

10. If the license server ID is not available, set **License Program** to **Enterprise agreement** and click **Next**.
11. Set parameters.
   - **Product Type**: specifies the license server type, for example, *Windows Server 2012 Remote Desktop Services Per User client access license*.
   - **Quantity**: the maximum number of users allowed for remote desktop connections, for example, 999.
   - **Agreement Number**: a 7-digit license registration number purchased at the official Microsoft website.

   **NOTE**

   HUAWEI CLOUD does not provide licenses for remote desktop connections. Purchase such a license at the official Microsoft website.

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

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

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

---

*Figure 5-32 Obtaining a license key pack ID*

*Figure 5-33 Activating the ECS*
3. Set Connection method to Web Browser and click **Next**.

![Figure 5-35 Web browser for connection](image)

4. Enter the license server ID and click **Next**.
   
The license server ID is the ID obtained in step 9.
5. Select **Start Install Licenses Wizard now** and click **Next**.
6. Enter the license key pack ID and click **Next**.
The key pack ID is obtained in step **12**.
Figure 5-38 Entering the key pack ID

To install your licenses, you must obtain a license key pack ID from the Remote Desktop Licensing Web Site located at:

https://activate.microsoft.com

To obtain a license key pack ID, you will need the license code information that you received from your license program (for example, retail product packaging, Enterprise Agreement, or Select License).

You will also need your license server ID. Your license server ID is:

After you have obtained the license key pack ID from the Remote Desktop Licensing Web Site, type the ID in the following boxes.

![License Activation](image)

Please write down this ID. Having this information with you will facilitate communications with the Microsoft Clearinghouse should you need assistance with recovering licenses.

7. Click Finish.

Configuring the Licensing Server for Remote Desktop Session Host

1. Log in to the Windows ECS.

2. On the OS, click to open Server Manager. Click Tools > Terminal Services > RD Licensing Diagnoser and check the ECS authorization status.

As shown in the following figure, the system displays a message indicating that the licensing mode for the Remote Desktop Session Host Server is not configured.
3. In the **Run** dialog box, enter `gpedit.msc` and click **OK** to start Local Group Policy Editor.

4. Choose **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Licensing.**
5. Set **Use the specified Remote Desktop license servers** to **Enabled**, enter the private IP address or hostname of the ECS under **License servers to use**, and click **OK**.
6. **Set the Remote Desktop licensing mode** to **Enabled**, and set the licensing mode to **Per User**.

**NOTE**

If a message is displayed indicating that there is a problem with remote desktop license, set the licensing mode to **Per Device**.
7. Run `cmd` and then `gpupdate /force` to forcibly start Local Group Policy Editor and restart the ECS.
6 Troubleshooting Remote Login Errors On a Windows ECS

6.1 What Should I Do If 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 6-1, 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. For details, see Unable to RDP to Virtual Machine: CredSSP Encryption Oracle Remediation. Rectify the fault by following the instructions provided in official Microsoft document.

Figure 6-1 Failed to set up a remote desktop connection
Solution

Modify the remote desktop connection settings on the Windows ECS. To do so, perform the following operations:

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 navigation pane on the left, 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 6-2 Remote settings

5. Click OK.
6.2 What Should I Do If the Local Computer Cannot Connect to My Windows ECS?

Symptom

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

Figure 6-3 Cannot connect to the remote computer

Possible Causes

- Port 3389 of the security group on the ECS is disabled. For details, see Checking Whether the Port 3389 Is Correctly Configured.
- 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 Whether the Port 3389 Is Correctly Configured

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

Checking Whether the Firewall Is Correctly Configured

Check whether the firewall on the ECS is enabled.

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

![Windows Firewall](image)

**Figure 6-4 Windows Firewall**

3. Click **Turn Windows Firewall on or off**. View and set the firewall status.

![Checking firewall status](image)

**Figure 6-5 Checking firewall status**

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

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

**NOTE**

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

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

**Checking Remote Desktop Connection Settings**

Modify the remote desktop connection settings of the Windows ECS: Select **Allow connections from computers running any version of remote desktop (less secure)**. To do so, perform the following operations:

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)**.
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.
Checking Remote Desktop Session Host Configuration

1. Open the cmd window and enter `gpedit.msc`.
2. Click OK to start Local Group Policy Editor.

4. Set Require use of specific security layer for remote (RDP) connections to Enabled and Security layer to RDP.
6.3 What Should I Do If I Do Not Have the Permission to Remotely Log In to a Windows ECS?

**Symptom**

When I connect a remote desktop to a Windows ECS, the system prompts that I need the permission to log in through Remote Desktop Services.

**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 6-12 Allow log on through Remote Desktop Services properties](image)

   b. Locate and double-click **Deny log on through Remote Desktop Services**. If the administrator account exists, delete it.
6.4 What Should I Do If the System Displays No Remote Desktop License Servers Available to Provide a License When I Log In to a Windows ECS?

Symptom

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

Precautions

- This section applies to ECSs running Windows Server 2008 or Windows Server 2012.
- You need to restart the ECS during the operation, which may interrupt services. Back up your data in advance.
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.

Windows Server 2008

1. Log in to the management console.
3. Remotely log in to the Windows ECS.
4. Open Server Manager, right-click Remote Desktop Services under Roles, and choose Remove Roles from the shortcut menu.

   ![Server Manager](image)

5. In the displayed dialog box, deselect Remote Desktop Session Host and click Next till you finish the operation.
6. Click **Delete**.
7. Restart the ECS.

**Windows Server 2012**

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. Remotely log in to the Windows ECS.
4. Open **Server Manager**, choose **Manage > Remove Roles and Features**, and click **Next**.

**Figure 6-14 Deleting roles and features**

5. Select the destination server and click **Next**.
6. Deselect **Remote Desktop Services**.
7. Click **Delete**.
8. Restart the ECS.

### 6.5 What Should I Do If the System Displays Error Code 0x112f When I Log In to a Windows ECS?

**Symptom**

When I log in to a Windows ECS, the system displays error code 0x112f.

**Figure 6-16 Error message (code: 0x112f)**

---

**Possible Causes**

The ECS memory is insufficient.

**Solution**

- Method 1 (recommended)
Modify the ECS specifications to increase the vCPUs and memory size. For instructions about how to modify ECS specifications, see Modifying ECS vCPU and Memory Specifications.

- **Method 2**
  Enable virtual memory on the ECS to obtain its idle memory.
  For instructions 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. Therefore, use this method only when necessary.

### 6.6 What Should I Do If the System Displays 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 I connect to an ECS running Windows Server 2008 using MSTSC.

**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, go to Step 2.

**Step 2** Check whether the firewall is disabled:

For details, see Configuring a Firewall.

If the firewall is enabled, go to Step 3.

**Step 3** Log in to the ECS using VNC and view the port information.
1. Open the cmd window and run the following command:
   `netstat -ano |findstr: 3389`

   **Figure 6-18** Checking port 3389

   ![Figure 6-18](image.png)

   As shown in **Figure 6-18**, 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 6-19** Checking System process

   ![Figure 6-19](image.png)

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 for verification.

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.

**Figure 6-20 Remote Desktop Services**

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

7. Click **OK**.

8. After the configuration is complete, open the **cmd** window.

9. Run the following command to update the group policy:

   `gpupdate`
6.7 What Should I Do If the System Displays Error Code 122.112... When I Log In to a Windows ECS?

Symptom

The system displays error 122.112... when I locally connect to an ECS running Windows Server 2012 using RDC. The server 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.

3. In the **Event Level** pane, select **Critical**, **Warning**, **Verbose**, and **Error**.
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 flavor of the purchased Windows ECS is 1U1GB. If it is, change the flavor or stop unnecessary processes.

----End

### 6.8 What Should I Do If the System Displays Invalid Certificate or Associated Chain When I Log In to a Windows ECS from a Mac?

**Symptom**
Due to the particularity of the Mac system, I need to perform related internal configurations on Mac and the Windows ECS to ensure successful remote connection. When I 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.

### Possible Causes

The policy group of the ECS is incorrectly configured.

### 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 6-27 Invalid certificate or associated chain**

**Figure 6-28 Clicking Preferences**
2. Select **Security** and modify the parameter settings according the following figure.

**Figure 6-29 Setting security**

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 6-30 Remote Desktop Session Host**

8. Modify the following parameters as prompted:
   - Enable **Require use of specific security layer for remote (RDP) connections**.
- Disable **Require user authentication for remote connections by using Network Level Authentication.**
6.9 What Should I Do If the System Displays a Message Indicating Invalid Credentials?

**Symptom**

When a local PC running Windows attempts 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 press **OK** to start **Local Group Policy Editor**.

**Figure 6-33** `gpedit.msc`

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

**Figure 6-34** Locating the network access policy

4. Select **Classic - local users authenticate as themselves** and click **OK**.
Figure 6-35 Changing the network access policy

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 press OK to start Local Group Policy Editor.
4. Double-click **Allow Delegating Saved Credentials with NTLM-only Server Authentication** and click **OK**.

**Figure 6-37 Allow Delegating Saved Credentials with NTLM-only Server Authentication**

5. Select **Enabled** and enter `TERMSRV/*` in the **Show Contents** text box. `TERMSRV/*` indicates the terminal server running on all computers.
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 6-39 Updating the group policy**

---

**Step 3: Set the Credentials of the Local Server**

1. Open the control panel on the local server and choose Credential Manager > Windows Credentials.
2. Check whether the credential of the target ECS is contained in the Windows credentials. If no, add a credential.

**Figure 6-41 Add a Windows Credential**

![Add a Windows Credential](image)

**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.**
6.10 What Should I Do If an Internal Error Occurs When I Log In to My Windows ECS?

Symptom

When I attempted to log in to my 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.
3. Restart the local server.
If you still cannot log in to the ECS using the preceding methods, check whether the local network is accessible. If not, change the network (for example, switch to a mobile hotspot) and check whether you can remotely log in to the ECS.

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

6.11 Troubleshooting Disconnected Session Because of a Protocol Error

Symptom

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

Figure 6-43 Protocol error

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 6-44 Opening the registry editor

2. Choose `HKEY_LOCAL_MACHINE > SYSTEM > ControlSet001 > Control > Terminal Server > RCM.`
3. Delete Certificate.

Figure 6-45 Deleting Certificate

4. Restart the ECS.
6. Right-click **RDP-Tcp** and choose **Properties**. In the displayed dialog box, click **General** and set **Security layer** to **RDP Security Layer**.
6.12 Troubleshooting an Identity Error of the Remote Computer

**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.
Possible Causes

Security software has been installed on the ECS, which prevents logins from unknown IP addresses.

Solution

- Uninstall the security software.
- Open the security software and enable the default login mode.

6.13 Troubleshooting the Connection Error of Two Computers in the Allotted Time

Symptom

An error message is displayed indicating that the computer cannot connect to the remote computer in the amount of time allotted.
Solution

Run `cmd` and then `netsh winsock reset`, restart the ECS as prompted, and try connecting again.

6.14 Troubleshooting a Denied Connection Because of Unauthorized User Account

Symptom

An error message is displayed indicating that the connection is 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 the remote desktop permissions.

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**.
3. Check whether there are user groups or users that have been granted the remote login permission.
   If not, add required users or groups.
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 that encounters a login error.
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.
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.
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
   ```

### 6.15 Troubleshooting a Lost Connection Because of Another User's Login

**Symptom**

An error message is displayed indicating that your remote desktop session has ended because another user has connected to the remote computer.
Windows Server 2008

1. Choose **Start > Administrative Tools > Remote Desktop Services > 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**.
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.**

3. Double-click **Restrict Remote Desktop Services users to a single Remote Desktop Services session**, change the value to **Disabled**, and click **OK.**
4. Run `gpupdate/force` to update the group policy.

**Figure 6-60 Updating the group policy**
7

Passwords and Key Pairs

7.1 Troubleshooting Password Reset for User root in the Single-User Mode on a Linux ECS

Scenarios

- The one-click password reset function on the management console does not take effect.
- The password reset plug-in is not installed and the password of user root is lost.

Constraints

Resetting the password of user root requires to restart the ECS and switch to the single-user mode. Therefore, identify the risks and back up your data.

CentOS 7 or EulerOS Series

1. On the ECS management console, restart the ECS and click Remote Login.
2. Press the up arrow key to prevent automatic system startup. When the kernels are displayed, press e to enter the editing mode.

![Figure 7-1 Entering the kernel editing mode](image)

- **NOTE**

  The Euler image encrypts the GRUB file by default. When you edit the kernel parameters, you need to contact customer service to obtain username and password.

3. Locate the row containing linux16 and perform the following operations:
   a. Delete the parameters not needed. Retain console=ttys0 console=ttys0 for BMS.
   b. Change ro to rw for mounting the root partition with read-write permissions.
   c. Add rd.break and press Ctrl+X.
4. Run the following command to go to the /sysroot directory:
   # chroot /sysroot
5. Reset the password of user root:
   # passwd root
6. (Optional) Run the following command to enable SELinux if required:
   # touch /.autorelabel
7. Exit the current root directory:
   # exit
8. Restart the ECS.
   # reboot

**CentOS 6 or Red Hat 6 Series**

1. On the ECS management console, restart the ECS and click **Remote Login**.
   When booting the system, press **Esc** to stop the countdown and enter a GRUB menu.
2. Move the cursor to the first default kernel and press `e` to edit the commands before booting.

Figure 7-4 GRUB menu

![GRUB menu](image)

3. Move the cursor to the row containing `kernel` and press `e`.
### Figure 7-6 Selecting the row that contains `kernel`

![GNU GRUB version 0.97 (639K lower / 1839356X upper memory)](image)

Use the 1 and 4 keys to select which entry is highlighted. Press ‘b’ to boot, ‘e’ to edit the selected command in the boot sequence, ‘c’ for a command-line, ‘o’ to open a new line after ‘0’ for before the selected line, ‘d’ to remove the selected line, or escape to go back to the main menu.

4. Move the cursor to the row that contains **quiet**, enter a space and **1** after **quiet**, and press **Enter**.

### Figure 7-7 Editing in the row that contains `quiet`

![Minimal BASH-like line editing is supported. For the first word, TAB lists possible command completions. Anywhere else TAB lists the possible completions of a device/filename. ESC at any time cancels. ENTER at any time accepts your changes.](image)

5. Press **b** to boot the kernel and change to runlevel 1 (single-user mode).
6. When the prompt '#' is displayed, run the following command to reset the password:

   ```bash
   # passwd root
   ``

7. Restart the ECS.

   ```bash
   # reboot
   ```

---

**Debian or Ubuntu Series**

1. On the ECS management console, restart the ECS and click **Remote Login**. Press **Esc** to stop the countdown and enter a GRUB menu.
2. Press e to enter the GRUB2 editing mode.
3. Locate the row that contains `linux`, delete the parameters not needed, and change `ro` to `rw` (mount the root partition in read-write mode), and add `init=/bin/bash` to the end of the row.

**Figure 7-9 Modifying ro parameter**

4. Press Ctrl+X to enter the rescue mode.
5. Reset the password of user `root`:
   ```bash
   # passwd root
   ```
6. Restart the ECS.
   ```bash
   # reboot
   ```

**SUSE 11 Series**

1. On the ECS management console, restart the ECS and click Remote Login. Press the up arrow key to stop the countdown and enter a GRUB menu.
2. Delete the parameter of Boot Options and add `init=/bin/bash`.
3. Press **Enter** to switch to the single-user mode.
4. Reset the password of user **root**:
   ```bash
   # passwd root
   ```
5. Restart the ECS.
   ```bash
   # reboot
   ```

**SUSE 12 Series**

1. On the ECS management console, restart the ECS and click **Remote Login**. Press **Esc** to stop the countdown and enter a GRUB menu.

**Figure 7-11 GRUB menu**

2. Press **e** to enter the GRUB2 editing mode.
3. Move the cursor to the end of the row containing **linux** and add **init=/bin/bash** to the end of the row.
4. Press **Ctrl+X** to enter the rescue mode.
5. Reset the password of user **root**:
   
   ```
   # passwd root
   ```
6. Restart the ECS.
   
   ```
   # reboot
   ```
8 Configuring a Firewall

8.1 Disabling a Windows ECS Firewall and Adding a Port Exception on a Windows ECS Firewall

Scenarios

This section describes how to disable a Windows ECS firewall and add a port exception on a Windows ECS firewall.

The following operations are performed on an ECS running Windows Server 2012.

| 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.

Enabling or Disabling a Firewall

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.

![Windows Firewall Control Panel]

3. Click Turn Windows Firewall on or off.
View and set the firewall status.

![Windows Firewall interface]

Adding a Port Exception on a Firewall

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. In the navigation pane on the **Windows Firewall** page, choose **Advanced settings > Inbound Rules**.

You can view details about the programs and ports that can be connected to the ECS.
4. Click **New Rule** in the **Actions** column.

Enable ports as prompted. This section uses port 3333 as an example. To permit port 3333, perform the following operations:

Select **Port**.

Select a protocol type and set the port.
Set a connection rule.

- **TCP**

Set the application scenarios of the rule.
5. Verify that the traffic to the port is permitted on the firewall.
   Click the newly added rule to view its details and set other information, such as computer connection, allowed IP connection, and protocol type.
8.2 Disabling a Linux ECS Firewall and Adding a Port Exception on a Linux ECS Firewall

Scenarios

This section describes how to disable a Linux ECS firewall and add a port exception on a Linux ECS firewall.

⚠️ 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.

Disabling a Firewall

Run the following command to disable the firewall based on the ECS OS:

- CentOS 6
  ```
  service iptables stop
  ```
- CentOS 7
  ```
  systemctl stop firewalld.service
  ```
- Ubuntu
  ```
  ufw disable
  ```
- Debian
  ```
  /etc/init.d/iptables stop
  ```

Adding a Port Exception on a Firewall

- CentOS 6
  a. For example, to add TCP port 23, run the following command:
     ```
     iptables -A INPUT -m state --state NEW -m tcp --dport 23 -j ACCEPT
     ```
  b. Save the configuration.
     ```
     service iptables save
     ```
  c. (Optional) Configure the firewall to automatically start upon ECS startup.
     ```
     chkconfig iptables on
     ```

□ NOTE

- To disable automatic firewall startup, run the following command:
  ```
  chkconfig iptables off
  ```
- When the firewall is started on CentOS 6, the “iptables no config file” error may be displayed because the `iptables` configuration file is not detected. To handle this issue, perform the following operations:
  - Add a new rule.
    ```
    iptables -P OUTPUT ACCEPT
    ```
  - Save the configuration.
    ```
    service iptables save
    ```
2. Start the firewall again.
   
   ```bash
   service iptables start
   ```

   • CentOS 7
   a. Start the firewall.
   ```bash
   systemctl start firewalld.service
   ```
   Check whether the firewall is enabled.
   ```bash
   firewall-cmd --state
   ```
   Information similar to the following is displayed:
   ```bash
   [root@ecs-centos7 ~]# firewall-cmd --state
   running
   ```
   b. For example, to add TCP port 23, run the following command:
   ```bash
   firewall-cmd --zone=public --add-port=23/tcp --permanent
   ```
   The configuration is correct if the command output is as follows:
   ```bash
   [root@ecs-centos7 ~]# firewall-cmd --zone=public --add-port=23/tcp
   --permanent
   success
   ```
   c. Reload the policy configuration for the new configuration to take effect.
   ```bash
   firewall-cmd --reload
   ```
   d. Run the following command to view all enabled ports:
   ```bash
   firewall-cmd --list-ports
   ```
   ```bash
   [root@ecs-centos7 ~]# firewall-cmd --list-ports
   23/tcp
   ```
   e. (Optional) Configure the firewall to automatically start upon ECS startup.
   ```bash
   systemctl enable firewalld.service
   ```
   Check whether automatic firewall startup is enabled.
   ```bash
   systemctl is-enabled firewalld.service;echo $?
   ```
   The configuration is correct if the command output is as follows:
   ```bash
   [root@ecs-centos7 ~]# systemctl is-enabled firewalld.service;echo $?
   enabled
   0
   ```

   **NOTE**

   To disable automatic firewall startup, run the following command:
   ```bash
   systemctl disable firewalld.service
   ```
9 Installing IIS

9.1 Troubleshooting IIS Installation on a Windows ECS

Scenarios

This section describes how to install IIS on an ECS running Windows Server 2012 R2 Standard.

IMPORTANT
Only the procedure for installing IIS will be described. The procedure for installing applications is subject to actual requirements.

Procedure

1. Open Server Manager.
2. Choose Quick Start > Add roles and features.

Figure 9-1 Adding roles and features

3. In the left navigation pane, choose Installation Type.
4. Select **Role-based or feature-based installation** and click **Next**.
5. Click **Server Selection**.
6. Select **Select a server from the server pool** and select a server from **Server Pool**.

7. Click **Next**.
8. Click **Server Roles**.
9. In the role list, select **Web Server (IIS)**.

**Figure 9-4 Web server (IIS)**

10. In **Add Roles and Features Wizard**, click **Add Features**.

![Image of adding features](image.png)
12. Choose **Web Server Roles (IIS) > Role Services**. Select the required role services. If you are not sure about which role service to install, you are advised to select all items except **FTP Server**.

**Figure 9-7 Selecting role services**

13. Click **Next**, confirm the roles to be installed, and click **Install**.
Helpful Links

For instructions about how to configure a domain name for IIS, see Troubleshooting Domain Name Modification on IIS Manager.

9.2 Troubleshooting Domain Name Modification on IIS Manager

Symptom

A 404 error occurs on the website constructed using IIS.

Possible Causes

IP address of the domain name is not specified on the IIS Manager.

Procedure

This section describes how to edit site binding on the IIS Manager that is deployed on an ECS running Windows Server 2008 R2.

1. Log in to the ECS and choose Start > Administrative Tools > IIS Manager.
2. On the IIS Manager, click Sites.
3. Right-click the website to be modified and choose Edit Bindings.
   Select a domain name and click Edit to add the private IP address of the specified ECS.

![Edit Site Binding](image)