Elastic Cloud Server

FAQs

Date 2019-12-02
Contents

1 Questions Summary ......................................................................................................................................... 8

2 Product Consultation ..................................................................................................................................... 9
  2.1 Limits............................................................................................................................................................. 9
  2.1.1 What Restrictions Apply to ECSs? ............................................................................................................. 9
  2.1.2 What Can I Do with ECSs? ....................................................................................................................... 9
  2.1.3 Can ECSs Automatically Recover After the Physical Host Accommodating the ECSs Becomes Faulty? ....... 9
  2.2 License Agreements........................................................................................................................................ 10
  2.2.1 How Can I Use BYOL? ............................................................................................................................. 10

3 Region and AZ ................................................................................................................................................ 11
  3.1 What Is AZ and How Can I Select One? ......................................................................................................... 11
  3.2 How Can I Select a Region? .......................................................................................................................... 11
  3.3 Are Products Different in Different Regions? ................................................................................................. 11
  3.4 Is Data Transmission Between AZs Charged? ................................................................................................. 12
  3.5 Can I Change the Region for a Purchased ECS? ............................................................................................. 12
  3.6 Does ELB Take Effect on the ECSs Deployed in Different Regions? ............................................................... 12
  3.7 Is Application Disaster Recovery Available in Different Regions? ................................................................. 12
  3.8 Does the Public Cloud Provide the Application DR Service? ......................................................................... 12
  3.9 Can Components Contained in an Application Be Distributed to Different Regions? ..................................... 12

4 Billing ............................................................................................................................................................. 13
  4.1 Billing Modes ................................................................................................................................................ 13
  4.1.1 What Are ECS Billing Modes? .................................................................................................................. 13
  4.1.2 What Is Pay-per-Use Billing Mode for ECSs? ............................................................................................. 13
  4.1.3 Is a Pay-per-Use ECS Billed After Being Stopped? ...................................................................................... 13
  4.1.4 What Is the Deduction Cycle for ECSs Charged in Metered Mode? ......................................................... 13
  4.1.5 How Can ECS Billing Be Stopped? ............................................................................................................ 14
  4.2 Renewal and Unsubscription ......................................................................................................................... 14
  4.2.1 How Can I Renew ECSs? .......................................................................................................................... 14
  4.2.2 Is Refund Supported? .............................................................................................................................. 14
  4.2.3 Can I Receive a Reminder If My Account Balance Is Insufficient? ............................................................ 15
  4.2.4 Can I Receive a Reminder of Account Balance Changes? ........................................................................ 15

5 Creation and Deletion .................................................................................................................................... 16
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 ECS Creation</td>
</tr>
<tr>
<td>5.1.1 What Should I Do If I Cannot Find My ECS on the Management Console?</td>
</tr>
<tr>
<td>5.1.2 What Should I Do If the ECS Resources to Be Purchased Are Sold Out?</td>
</tr>
<tr>
<td>5.1.3 Why Does the Failures Area Show an ECS Creation Failure But the ECS List Displays the Created ECS?</td>
</tr>
<tr>
<td>5.1.4 When Does an ECS Become Provisioned?</td>
</tr>
<tr>
<td>5.1.5 Why Cannot I View the ECSs Being Created Immediately After I Pay for Them?</td>
</tr>
<tr>
<td>5.1.6 What Should I Do If It Is Slow to Create ECSs Using a Full-ECS Image?</td>
</tr>
<tr>
<td>5.1.7 How Long Does It Take to Obtain an ECS?</td>
</tr>
<tr>
<td>5.2 ECS Deletion</td>
</tr>
<tr>
<td>5.2.1 What Functions Does the Delete Button Provide?</td>
</tr>
<tr>
<td>5.2.2 What Is a Deleted ECS?</td>
</tr>
<tr>
<td>5.2.3 Can a Deleted ECS Be Provisioned Again?</td>
</tr>
<tr>
<td>5.2.4 Can a Deleted ECS Be Restored?</td>
</tr>
<tr>
<td>5.2.5 What Should I Do If an ECS Remains in the Restarting or Stopping State for a Long Time?</td>
</tr>
<tr>
<td>6 Login and Connection</td>
</tr>
<tr>
<td>6.1 Login Preparations</td>
</tr>
<tr>
<td>6.1.1 What Should Be Prepared for Logging In to an ECS?</td>
</tr>
<tr>
<td>6.1.2 What Are the Username and Password for Remote Logins?</td>
</tr>
<tr>
<td>6.1.3 What Is the Username to Log In to an ECS?</td>
</tr>
<tr>
<td>6.1.4 What Should I Do If My Remote Login Password Was Forgotten?</td>
</tr>
<tr>
<td>6.1.5 Why Cannot I Use the Account Used to Create a GPU-accelerated ECS to Log In to the ECS Through SSH?</td>
</tr>
<tr>
<td>6.1.6 What Should I Do If Starting an ECS Remains in &quot;Waiting for cloudResetPwdAgent&quot; State?</td>
</tr>
<tr>
<td>6.2 Logs Through the Management Console</td>
</tr>
<tr>
<td>6.2.1 What Should I Do If Garbled Characters Are Displayed When I Log In to My ECS Using VNC?</td>
</tr>
<tr>
<td>6.2.2 What Should I Do If the Page Does not Respond After I Log In to an ECS Using VNC and Do Not Perform Any Operation for a Long Period of Time?</td>
</tr>
<tr>
<td>6.2.3 What Should I Do If I Cannot View Data After Logging In to an ECS Using VNC?</td>
</tr>
<tr>
<td>6.2.4 Why Does a Blank Screen Appear While the System Displays a Message Indicating Successful Authentication After I Attempted to Log In to an ECS Using VNC?</td>
</tr>
<tr>
<td>6.2.5 What Should I Do If Error Code 1006 or 1000 Is Displayed When I Log In to an ECS Through the Management Console?</td>
</tr>
<tr>
<td>6.2.6 Why No Audio File Can Be Properly Played on My Windows ECS Logged In Using VNC?</td>
</tr>
<tr>
<td>6.2.7 How Can I Change the Resolution of a Windows ECS?</td>
</tr>
<tr>
<td>6.3 Remote Logins</td>
</tr>
<tr>
<td>6.3.1 What Should I Do If I Cannot Use MSTSC to Log In to an ECS Running the Windows Server 2012 OS?</td>
</tr>
<tr>
<td>6.3.2 What Should I Do If I Cannot Log In to My Windows ECS?</td>
</tr>
<tr>
<td>6.3.3 What Should I Do If I Cannot Log In to My Linux ECS?</td>
</tr>
<tr>
<td>6.3.4 Why Cannot I Use a Non-Default SSH Port to Log In to My Linux ECS?</td>
</tr>
<tr>
<td>6.3.5 What Should I Do If I Cannot Log In to an ECS with Cloud-Init Enabled?</td>
</tr>
<tr>
<td>6.3.6 What Browser Version Is Required to Remotely Log In to an ECS?</td>
</tr>
<tr>
<td>6.3.7 What Should I Do If I Cannot Access a Windows Server 2012 OS After Uninstalling Some Software?</td>
</tr>
</tbody>
</table>
6.3.8 How Can I Log In to an ECS After Its System Disk Is Exchanged with That Attached to Another ECS Running the Same OS? .................................................. 44
6.3.9 Why Does the System Display a Message Indicating that the Password for Logging In to a Windows ECS Cannot Be Viewed? ........................................ 46
6.4 Remote Login Errors on Windows .......................................................... 47
6.4.1 What Should I Do If an Authentication Failure Occurs After I Attempt to Remotely Log In to a Windows ECS? .................................................. 47
6.4.2 What Should I Do If the System Displays a Message Indicating Invalid Credentials? .......................................................... 49
6.4.3 What Should I Do If the System Displays Error Code 0x112f When I Log In to a Windows ECS? .................................................. 55
6.4.4 What Should I Do If an Internal Error Occurs When I Log In to My Windows ECS? .................................................. 56
6.4.5 What Should I Do If BSOD Occurs When I Log In to a Windows Server 2012 ECS Using Remote Desktop Connection? .................................................. 56

7 ECS Management .................................................................................. 58
7.1 Changing Hostnames .......................................................................... 58
7.1.1 How Can a Changed Static Hostname Take Effect Permanently? ............... 58
7.1.2 Is an ECS Hostname with Suffix .novalocal Normal? .............................. 59
7.1.3 What Should I Do If the Hostname of My ECS Is Restored After the ECS Is Restarted? .................................................. 60
7.2 Modifying Specifications ...................................................................... 60
7.2.1 How Can I Modify Specifications of ECSs Charged in Yearly/Monthly Mode? .................................................................................................. 60
7.2.2 How Can I Modify Specifications of ECSs Charged in Pay-Per-Use Mode? .................................................................................................. 60
7.2.3 What Should I Do If the Data Disk of a Windows ECS Becomes Offline After the ECS Specifications Are Modified? .................................................. 61
7.2.4 What Should I Do If the Disk of a Linux ECS Becomes Offline After the ECS Specifications Are Modified? .................................................. 64
7.3 Usage Errors ...................................................................................... 65
7.3.1 How Do I Handle Error Messages Displayed on the Management Console? .......................................................................................... 65
7.3.2 How Can I Recover a Windows ECS with an Abnormal Virtualization Driver? .......................................................................................... 68
7.3.3 What Should I Do If I Cannot Activate a Windows ECS? .......................... 71
7.3.4 What Should I Do If Emails Configured on an ECS Cannot Be Sent? ........ 73
7.3.5 Why Is My Windows ECS Muted? ......................................................... 75
7.3.6 How Do I Change an ECS SID? .......................................................... 78

8 OS Management ................................................................................... 80
8.1 Changing OSs ................................................................................... 80
8.1.1 Are OSs Charged? .......................................................................... 80
8.1.2 Does OS Changing Incur Fees? ......................................................... 80
8.1.3 Can I Install or Upgrade the OS by Myself? ...................................... 80
8.1.4 Can the OS of an ECS Be Changed? ............................................... 80
8.1.5 How Long Does It Take to Change an ECS OS? ................................ 80
8.2 Reinstalling OSs ................................................................................ 81
8.2.1 Does OS Reinstallation Incur Fees? ................................................... 81
8.2.2 Can I Select Another OS During ECS OS Reinstallation? ....................... 81
8.2.3 How Long Does It Take to Reinstall an ECS OS? ............................... 81
8.3 GUI Installation FAQs ...................................................................... 81
8.3.1 Do ECSs Support GUI? ................................................................. 81
9 File Uploading ................................................................. 93
  9.1 Does an ECS Support FTP-based Uploading by Default? ........... 93
  9.2 How Can I Upload a File to a Windows ECS? ..................... 93
  9.3 How Can I Transfer Data Between a Local Host and a Windows ECS? .................................................. 96
  9.4 How Can I Use WinSCP to Upload a File to a Linux ECS? ....... 100
  9.5 What Should I Do If the Connection Between the Client and the Server Times Out When I Upload a File Using FTP? ............... 102
  9.6 What Should I Do If Writing Data Failed When I Upload a File Using FTP? ................................................................. 102
  9.7 What Should I Do If an ECS with FTP Deployed Cannot Be Accessed Through Internet? ..................................................... 103

10 Application Migration ......................................................... 106
  10.1 Can I Transfer ECS Ownership Between Accounts? ............... 106

11 Image Source Management .................................................. 107
  11.1 How Can I Use the Automated Tool to Configure an HUAWEI CLOUD Image Source (x86_64)? ...................... 107
  11.2 How Can I Use an openSUSE Image Source (x86_64) Provided by HUAWEI CLOUD? .................................................. 108
  11.3 How Can I Use a CentOS Image Source (x86_64) Provided by HUAWEI CLOUD? .................................................. 109
  11.4 How Can I Use a Ubuntu Image Source (x86_64) Provided by HUAWEI CLOUD? .................................................. 110
  11.5 How Can I Use a EulerOS Image Source (x86_64 or ARM) Provided by HUAWEI CLOUD? ................................................ 111

12 Disk Management ............................................................... 113
  12.1 Disk Partitions and Virtual Memory ................................... 113
  12.1.1 How Can I Adjust System Disk Partitions? ................. 113
  12.1.2 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Windows ECS? ................. 118
  12.1.3 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Linux ECS? .................. 121
  12.1.4 How Can I Enable Virtual Memory on a Windows ECS? ................................................................. 123
  12.1.5 Why Is the Memory of an ECS Obtained by Running the free Command Inconsistent with the Actual Memory? ................................................................. 125
  12.2 Disk Capacity Expansion .................................................. 127
  12.2.1 How Can I Add the Empty Partition of an Expanded System Disk to the End Root Partition Online? ........... 127
  12.2.2 How Can I Add the Empty Partition of an Expanded System Disk to the Non-end Root Partition Online? .... 128
  12.3 Disk Attachment ......................................................... 131
  12.3.1 Can Multiple Disks Be Attached to an ECS? .................. 131
  12.3.2 What Are the Restrictions on Attaching an EVS Disk to an ECS? ................................................................. 132
  12.3.3 Which ECSs Can Be Attached with SCSI EVS Disks? ......... 132
12.3.4 What Is the Mapping Between Device Names and Disks? .................................................. 133
12.3.5 What Should I Do If a Linux ECS with a SCSI Disk Attached Fails to Restart? .................. 135
12.3.6 How Can I Check Whether the ECSs Attached with the Same Shared SCSI Disk Are in the Same ECS Group? ................................................................. 136
12.4 Others.................................................................................................................................. 138
12.4.1 Who Can Use the Encryption Feature? ............................................................................. 138
12.4.2 How Can I Add an ECS with Local Disks Attached to an ECS Group? ......................... 140
12.4.3 What Should I Do If a Disk Is Offline? .............................................................................. 140
12.4.4 How Can I Obtain Data Disk Information If Tools Are Deleted? .................................. 141

13 Passwords and Key Pairs ........................................................................................................ 143
13.1 Passwords ............................................................................................................................ 143
13.1.1 How Can I Change the Password for Logging In to a Linux ECS? ................................. 143
13.1.2 What Is the Default Password for Logging In to a Linux ECS? ................................... 143
13.1.3 How Can I Set the Validity Period of the Image Password? ........................................ 144
13.1.4 Changing the Login Password on an ECS .................................................................. 145
13.1.5 Resetting the Password for Logging In to a Windows ECS ....................................... 146
13.1.6 Resetting the Password for Logging In to a Linux ECS .............................................. 149
13.1.7 What Should I Do If the System Displays a Message Indicating that the Password Is Incorrect When I Remotely Log In to My ECS? ................................. 151
13.1.8 What Should I Do If I Cannot Log In to My ECS Using the Initial Password After I Use It for a Period of Time? ............................................................ 152
13.1.9 What Should I Do If I Cannot Log In to My ECS Using the Reset Password? ............... 152
13.1.10 What Should I Do If a Service Port Is Used by a One-Click Password Reset Plug-in? .... 155
13.2 Key Pairs .............................................................................................................................. 158
13.2.1 How Can I Obtain the Key Pair Used by an ECS? ......................................................... 158
13.2.2 How Can I Use a Key Pair? ............................................................................................. 158
13.2.3 What Should I Do If a Key Pair Cannot Be Imported? ................................................ 159
13.2.4 Why Was My Login to a Linux ECS Using a Key File Unsuccessful? ......................... 160
13.2.5 What Should I Do If I Cannot Download a Key Pair? .................................................. 161
13.2.6 What Should I Do If a Key Pair Created Using puttygen.exe Cannot Be Imported to the Management Console? ......................................................... 162
13.2.7 What Is the cloudbase-init Account in Windows ECSs? ................................................ 164
13.2.8 What Should I Do If Cloud-Init Does Not Work After Python Is Upgraded? ............... 165

14 Network Configurations ......................................................................................................... 167
14.1 EIP FAQs ............................................................................................................................. 167
14.1.1 Can Multiple EIPs Be Bound to an ECS? ....................................................................... 167
14.1.2 Can an ECS Without an EIP Access the Internet? ....................................................... 168
14.1.3 Why Cannot an EIP Be Pinged? ..................................................................................... 168
14.1.4 Why Can I Remotely Access an ECS But Cannot Ping It? .......................................... 171
14.1.5 What Do I Do If Outbound Access Through TCP Port 25 Is Restricted? .................... 172
14.2 DNS and NTP Configurations ........................................................................................... 172
14.2.1 How Can I Configure the NTP and DNS Servers for an ECS? .................................. 172
14.2.2 Does HUAWEI CLOUD Provide the NTP Server and How Can I Install It? ......................................................... 176
14.2.3 Configuring DNS .................................................................................................................................................... 180
14.3 NICs......................................................................................................................................................................... 184
14.3.1 Will NICs Added to an ECS Start Automatically? .................................................................................................. 184
14.3.2 How Can I Check Whether the Network Communication Between Two ECSs Equipped with an InfiniBand NIC 
Driver Is Normal? ....................................................................................................................................................... 184
14.3.3 How Can I Manually Configure an IP Address for an InfiniBand NIC? .............................................................. 185
14.3.4 How Can I Handle the Issue that a Windows 7 ECS Equipped with an Intel 82599 NIC Reports an Error in 
SR-IOV Scenarios? ....................................................................................................................................................... 186
14.4 Routing ................................................................................................................................................................. 187
14.4.1 How Can I Add a Static Route to a CentOS 6.5 OS? .............................................................................................. 187
14.5 Website or Application Access Failures .................................................................................................................. 188
14.5.1 What Should I Do If My Windows ECS Cannot Access the Internet? ................................................................. 188
14.5.2 Troubleshooting a Website Access Error Occurred on an ECS ............................................................................ 189
14.5.3 Troubleshooting Slow Access of a Website Outside the Chinese Mainland over an ECS ................................. 193
14.6 Others...................................................................................................................................................................... 196
14.6.1 How Can I Obtain the MAC Address of My ECS? ................................................................................................ 196
14.6.2 How Can I Test Network Performance? ................................................................................................................ 196
14.6.3 How Can I View and Modify Kernel Parameters of a Linux ECS? ...................................................................... 204
14.6.4 Can the ECSs of Different Accounts Communicate over the Intranet? ............................................................... 209
14.6.5 Are ECSs I Purchased Deployed in the Same Subnet? ......................................................................................... 209

15 Security Configurations ............................................................................................................................................. 210
15.1 How Does an ECS Defend Against DDoS Attacks? ................................................................................................. 210
15.2 How Can I Disable Operation Protection? ................................................................................................................ 210

16 Resource Monitoring ................................................................................................................................................ 212
16.1 How Can I Create an Agency for Monitoring My ECS? ........................................................................................... 212
16.2 Troubleshooting High Bandwidth or CPU Usage of a Windows ECS ..................................................................... 212
16.3 Troubleshooting High Bandwidth or CPU Usage of a Linux ECS ............................................................................ 217

17 Database Applications ................................................................................................................................................. 221
17.1 Can a Database Be Deployed on an ECS? ................................................................................................................ 221
17.2 Does an ECS Support Oracle Databases? ................................................................................................................ 221

18 Change History .......................................................................................................................................................... 222
1 Questions Summary

Remote Logins
- 6.3.2 What Should I Do If I Cannot Log In to My Windows ECS?
- 6.3.3 What Should I Do If I Cannot Log In to My Linux ECS?
- 6.1.2 What Are the Username and Password for Remote Logins?
- Troubleshooting Multi-User Logins
- Applying for a License for Authenticating Multi-User Sessions and Activating the ECS

Website or Application Access Failures
- Troubleshooting a Website Access Error Occurred on an ECS
- Troubleshooting an Unreachable ECS Port
- 14.5.3 Troubleshooting Slow Access of a Website Outside the Chinese Mainland over an ECS

Internet Access Failures
- 14.5.1 What Should I Do If My Windows ECS Cannot Access the Internet?
- 14.5.3 Troubleshooting Slow Access of a Website Outside the Chinese Mainland over an ECS
- Troubleshooting a Ping Failure or Packet Loss Using a Link Test

ECS Failures or Slow ECS Responses
- 16.2 Troubleshooting High Bandwidth or CPU Usage of a Windows ECS
- 16.3 Troubleshooting High Bandwidth or CPU Usage of a Linux ECS
- How Do I Check Whether the Bandwidth Exceeds the Limit?
- Troubleshooting High Bandwidth Usage on an ECS

Ping Failures
- 14.1.3 Why Cannot an EIP Be Pinged?
- 14.1.4 Why Can I Remotely Access an ECS But Cannot Ping It?
- Troubleshooting a Ping Failure or Packet Loss Using a Link Test
2.1 Limits

2.1.1 What Restrictions Apply to ECSs?

- You are advised not to upgrade ECS kernel or OS versions. If you want to upgrade the main OS version, for example, from CentOS 7.2 to Cent OS 7.3, use the provided OS changing function.
- You are advised not to uninstall the performance optimization software pre-installed on your ECSs.
- You are advised not to change the MAC addresses of your ECS NICs.

2.1.2 What Can I Do with ECSs?

You can use ECSs just like traditional physical servers. On an ECS, you can deploy any service application, such as the email system, web system, and Enterprise Resource Planning (ERP) system. After creating an ECS, you can use it like using your local computer or physical server.

2.1.3 Can ECSs Automatically Recover After the Physical Host Accommodating the ECSs Becomes Faulty?

Yes.

ECSs run on physical hosts. Although the cloud platform offers multiple mechanisms to ensure system reliability, error tolerance, and high availability, host hardware might be damaged or power failure might occur. If physical hosts cannot be powered on or restarted due to damage, CPU and memory data will lose and live migration cannot be used to recovery ECSs.

The cloud platform provides automatic recovery by default to restart ECSs through cold migration, ensuring high availability and dynamic ECS migration. Once a physical host accommodating ECSs breaks down, the ECSs automatically migrate to a functional physical host. This minimizes user service interruption. The ECSs will restart during the migration.

NOTE
- Automatic recovery does not ensure user data consistency.
- An ECS can be automatically recovered only if the physical host on which it is deployed becomes faulty. This function does not take effect if the fault is caused by the ECS itself.
• An ECS can be automatically recovered only after the physical host on which it is deployed is shut down. If the physical host is not shut down due to a fault, for example, a memory fault, automatic recovery fails to take effect.
• An ECS can be automatically recovered only once within 12 hours if the host on which it is deployed becomes faulty.
• ECS automatic recovery may fail in the following scenarios:
  • No physical host is available for migration due to a system fault.
  • The target physical host does not have sufficient temporary capacity.
  • An ECS with any of the following resources cannot be automatically recovered:
    • Local disk
    • Passthrough FPGA card
    • Passthrough InfiniBand NIC

2.2 License Agreements

2.2.1 How Can I Use BYOL?

What Is BYOL?

Bring your own license (BYOL) allows you to use your existing OS license. In such a case, you do not need to apply for a license again. In BYOL license type, you do not pay for the license fee when purchasing an ECS.

How to Use BYOL?

If you select the BYOL license type, you are required to manage licenses by yourself. The public cloud platform provides functions for you to maintain license compliance during the license lifecycle. If you have obtained an OS license, you do not need to apply for a license any more.

NOTICE

BYOL can be used on a Windows ECS that is created on a DeH.
BYOL can be used on a Windows ECS that is created in a Dedicated Computing Cluster (DCC). No physical host is specified in a DCC for running a purchased ECS. Therefore, BYOL must be enabled on all physical hosts in the DCC.
3 Region and AZ

3.1 What Is AZ and How Can I Select One?

AZ

An AZ is a physical region where resources use independent power sources and networks. An AZ is generally an independent physical equipment room, ensuring independence of the AZ.

Each region contains multiple AZs. If one AZ becomes faulty, the other AZs in the same region can still properly provide services.

AZs in the same region can communicate with each other over an intranet.

Selecting an AZ

You can purchase ECSs in different AZs as required. The failure of an AZ does not affect the running of ECSs in other AZs. Follow the rules when selecting AZs:

- If only one AZ is available in a region, there is only one AZ in the region.
- The AZ of a purchased ECS cannot be changed.
- The AZs in one region can communicate with each other over an intranet.

3.2 How Can I Select a Region?

A region is a geographic area. Huawei has deployed data centers in multiple regions to provide services nationwide.

It is recommended that you select the nearest region. For example, if you or your customers are located in Beijing, select a CN North region for low network latency and high service access rate.

3.3 Are Products Different in Different Regions?

Yes. The products are different currently.

Huawei deploys mature products and services in each region and new products in certain regions for trial release.
3.4 Is Data Transmission Between AZs Charged?

Data transmission between AZs in the same region is free of charge. However, data transmission between AZs in different regions is charged.

3.5 Can I Change the Region for a Purchased ECS?

No.

Select the region closest to your service and purchase ECSs.

3.6 Does ELB Take Effect on the ECSs Deployed in Different Regions?

No. You are advised to use the dedicated ELB service for the ECSs in each region.

3.7 Is Application Disaster Recovery Available in Different Regions?

Yes.

You can deploy active and standby application nodes in different regions. If the active application node is faulty, the standby application node can still provide services for you.

3.8 Does the Public Cloud Provide the Application DR Service?

Standard application disaster recovery solution is unavailable now. If you have the requirement, contact us. We will customize an application disaster recovery solution based on your application scenarios.

3.9 Can Components Contained in an Application Be Distributed to Different Regions?

Yes. However, such a deployment mode is not recommended.

You are advised to deploy the components contained in an application in the same region. In this manner, these components can communicate with each other over an intranet, reducing bandwidth costs introduced by public networks and ensuring communication quality between the components.
4.1 Billing Modes

4.1.1 What Are ECS Billing Modes?
ECSs can be billed in yearly/monthly or pay-per-use payments. Choose a billing mode best suit you.

4.1.2 What Is Pay-per-Use Billing Mode for ECSs?
In pay-per-use billing mode, fees are billed by hour. If the service duration is less than one hour, fees are charged based on the service duration.

4.1.3 Is a Pay-per-Use ECS Billed After Being Stopped?
After such an ECS is stopped, basic resources including vCPUs, memory, and images are not billed, but system disks are billed based on the capacity you use. If other products, such as EVS disks, EIP, and bandwidth are bound to the ECS, these products are billed separately (yearly/monthly or pay-per-use).

**NOTICE**

If a pay-per-use ECS is stopped and then restarted, the startup may fail due to insufficient resources. In such an event, wait several minutes before attempting another restart or change the ECS flavor.

If the ECS that you use contains local disks (for example, of disk-intensive, H2, P1, or P2 type) or FPGAs (for example, of FP1 or FP1c type), the fees are still billed after the ECS is stopped. To stop billing such an ECS, delete it.

4.1.4 What Is the Deduction Cycle for ECSs Charged in Metered Mode?
Each ECS is charged per hour and postpaid.
4.1.5 How Can ECS Billing Be Stopped?

If a pay-per-use product, such as an ECS or EVS disk is not required any more, delete it to stop billing.

However, this function does not apply to the ECSs using local storage (such as disk-intensive, H2, P1, and P2 ECSs) or FPGAs (such as FP1 or FP1C ECSs). Charges will continue to be incurred for the ECSs even after they are stopped. To stop billing such an ECS, delete it.

A product billed in yearly/monthly mode, such as an ECS or EVS disk, is paid when you purchase it. The billing automatically stops when the payment cycle expires. If you stop using the product before the payment cycle expires, the system does not refund.

This section uses a pay-per-use ECS to describe the impact on billing after the ECS is deleted. Table 4-1 lists the information of the ECS.

Table 4-1 Information of a pay-per-use ECS

<table>
<thead>
<tr>
<th>Resources Used by the ECS</th>
<th>Description</th>
<th>Billing Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic resources</td>
<td>vCPUs, memory, and image</td>
<td>Pay-per-use</td>
</tr>
<tr>
<td>EVS disk</td>
<td>System disk</td>
<td>Pay-per-use</td>
</tr>
<tr>
<td></td>
<td>Data disk</td>
<td>Pay-per-use</td>
</tr>
<tr>
<td>EIP</td>
<td>N/A</td>
<td>Pay-per-use</td>
</tr>
</tbody>
</table>

The ECS is billed as follows after being deleted:

- Basic resources: not billed any more
- EVS disk
  - System disk: not billed any more
  - Data disk: not billed any more if you select Delete the data disks attached to the following ECSs when deleting the ECS. Otherwise, the data disk is still billed.
- EIP: not billed any more if you select Release the EIPs bound to the following ECSs when deleting the ECS. Otherwise, the EIP is still billed.

4.2 Renewal and Unsubscription

4.2.1 How Can I Renew ECSs?

On the Elastic Cloud Server page, click More in the Operation column and select Renew to renew the subscription.

4.2.2 Is Refund Supported?

Automatic refund is not supported.
4.2.3 Can I Receive a Reminder If My Account Balance Is Insufficient?

You can set the account balance threshold on the recharging page. After the account balance is less than the threshold, the system will send you a reminder.

4.2.4 Can I Receive a Reminder of Account Balance Changes?

The system sends you a reminder of the account balance changes using emails or short messages. The reminder message contains account balance adjustment, online recharging, and successful recharging.
5.1 ECS Creation

5.1.1 What Should I Do If I Cannot Find My ECS on the Management Console?

Symptom

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

Possible Causes

The ECS is not in the current region.

Solution

Method 1

1. Log in to the HUAWEI CLOUD management console.
2. Verify the region in which your ECS locates. Then, your ECS is displayed.
Method 2
1. Log in to the HUAWEI CLOUD management console.
2. On the management console homepage, click View Resources in All Regions under My Resources.

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

Each HUAWEI CLOUD region has two or three AZs. If the desired resources are sold out in the current AZ, change the AZ and try again.

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

Symptom

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

**Root Cause**

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

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

### 5.1.4 When Does an ECS Become Provisioned?

ECSs charged in yearly/monthly mode: After you pay for the ECSs and the system successfully deducts incurred fees from your account balance, your ECSs are automatically provisioned.

ECSs charged in metered mode: The ECSs are automatically provisioned after they are created.

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

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

### 5.1.6 What Should I Do If It Is Slow to Create ECSs Using a Full-ECS Image?

**Symptom**

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

**Cause Analysis**

The original backup format provided by CSBS cannot be used to rapidly create ECSs. Therefore, if your full-ECS image is in the original backup format, this issue occurs.

**NOTE**

CSBS has provided a new backup format. This issue is resolved if you use a full-ECS image created using a CSBS backup in the new format.

**Solution**

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

- **Scenario 1:** The ECS based on which the target CSBS backup is created is still available.
Back up the original ECS on the Cloud Server Backup Service page and use the new backup to create a full-ECS image. The created full-ECS image can be used to rapidly create ECSs.

- For instructions about how to back up an ECS, see Cloud Server Backup Service User Guide.
- For instructions about how create a full-ECS image, see Image Management Service User Guide.

- Scenario 2: The ECS based on which the target CSBS backup is created is unavailable.
  a. Use the full-ECS image to create a new ECS.
  b. Back up the ECS.
     For details, see Cloud Server Backup Service User Guide.
  c. Use the CSBS backup to create a full-ECS image again.
     For details, see Image Management Service User Guide.
     The created full-ECS image can be used to rapidly create ECSs.

5.1.7 How Long Does It Take to Obtain an ECS?

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

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

**NOTE**

If obtaining an ECS takes a long time, contact customer service for technical support.

5.2 ECS Deletion

5.2.1 What Functions Does the Delete Button Provide?

After you click Delete, the selected ECS is deleted. You can choose to delete the EVS disk and EIP of the ECS as well. If you do not delete them, they are reserved. If necessary, you can manually delete them later.

To delete an ECS, perform the following operations:

1. Log in to the management console.
3. Select the ECS to be deleted.
4. In the upper part of the ECS list, click Delete.

5.2.2 What Is a Deleted ECS?

Deleted is an intermediate state of the ECS. Deleted indicates that the ECS has been deleted. ECSs in this state can no longer provide services and are soon removed from the system.
5.2.3 Can a Deleted ECS Be Provisioned Again?

No. A deleted ECS is retained in the ECS list on the management console for only a short period of time. It is then completely removed from the system and cannot be provisioned again. You can purchase the ECSs of the same specifications again.

5.2.4 Can a Deleted ECS Be Restored?

No. The data of a deleted ECS cannot be restored. Therefore, before deleting an ECS, back up or migrate its data.

5.2.5 What Should I Do When an ECS Remains in the Restarting or Stopping State for a Long Time?

If an ECS remains in the Restarting or Stopping state for over 30 minutes after being restarted or stopped, you can forcibly restart or stop the ECS as follows:

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. Select the target ECS and click Restart or Stop.
   A dialog box is displayed to confirm whether you want to restart or stop the ECS.
5. Select Forcibly restart the preceding ECSs or Forcibly stop the preceding ECSs.
6. Click OK.
6 Login and Connection

6.1 Login Preparations

6.1.1 What Should Be Prepared for Logging In to an ECS?

Windows

- Obtain the login password.

  ECSs created using a public image have had one-click password reset plug-ins installed by default. If your password was forgotten or has expired, use the password reset function to obtain a new password for logging in to the ECS.
Figure 6-1 Reset Password

Reset Password

- Ensure that the ECS has an EIP bound (only required for MSTSC logins).
  For details, see Assigning an EIP and Binding It to an ECS.
- Make sure that the remote desktop protocol has been enabled on the ECS (only required for MSTSC logins).
  If MSTSC-based remote desktop connection is used, log in to the ECS using VNC and enable the remote desktop protocol.
  For details, see Login Using MSTSC.

More information:
- If your ECS was created using an external image file and the ECS has not had password reset plug-ins installed, reset the ECS login password by attaching a disk to the ECS. For details, see 13.1.5 Resetting the Password for Logging In to a Windows ECS.
- If your ECS is authenticated using a key pair, parse the private key file to a password before logging in to the ECS.
  a. Locate the target ECS.
  b. In the Operation column, click More and select Get Password.
  c. Copy the content of the private key file and paste it into the text box. Click Get Password to obtain a random password.
Elastic Cloud Server
FAQs

6 Login and Connection

Figure 6-2 Get Password

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

Use private key KeyPair-a2cf.pem stored in your local directory to retrieve the password.

Select Private Key

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

---BEGIN RSA PRIVATE KEY----MIIEowIBAAKCAQEAm4Wk/Xngh3FDMnof

Get Password

Username Administrator
Password y2mQneT09AHqMI1cppFk

Cancel

Linux

- Obtain the login password.

ECSs created using a public image have had one-click password reset plug-ins installed by default. If your password was forgotten or has expired, use the password reset function to obtain a new password for logging in to the ECS.
### Figure 6-3 Reset Password

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECS Name</td>
<td>ecs-3f93</td>
</tr>
<tr>
<td>Username</td>
<td>root</td>
</tr>
<tr>
<td>New Password</td>
<td>**       **</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>**       **</td>
</tr>
</tbody>
</table>

- Ensure that the ECS has an EIP bound (only required for SSH logins). SSH logins apply to only Linux ECSs. You can use a remote login tool, such as PuTTY, to log in to your ECS. In such a case, the ECS must have an EIP bound.
  - Verify that the ECS has an EIP bound.
    - For details, see Assigning an EIP and Binding It to an ECS.
  - Check whether the EIP bound to the ECS can be pinged.
    - If a public IP address is used, see Why Cannot an EIP Be Pinged? for troubleshooting.
    - If a private IP address is used, see What Do I Do If Two ECSs in the Same VPC Cannot Communicate with Each Other or Packet Loss Occurs During the Communication Between the Two ECSs? for troubleshooting.

**More information:**
- If your ECS was created using an external image file and the ECS has not had password reset plug-ins installed, reset the ECS login password by attaching a disk to the ECS. For details, see 13.1.6 Resetting the Password for Logging In to a Linux ECS.
- **If your ECS is authenticated using a key pair, parse the private key file to a password before logging in to the ECS.**
  
  For a Linux ECS authenticated using a key pair:
  - For the first login, use an SSH key. For details, see Login Using an SSH Key.
  - For a non-first login, if you want to use the remote login function (VNC) provided by the management console, log in to the ECS using the SSH key and set the password.
For a key-pair-authenticated ECS, obtaining its login password using a private key file failed.

The password fails to inject using Cloud-Init. For details, see What Should I Do If I Cannot Log In to an ECS with Cloud-Init Enabled?

6.1.2 What Are the Username and Password for Remote Logins?

Username for logging in to an ECS:

- For Windows: Administrator
- For Linux: root

If your login password is forgotten, see Resetting the ECS Password on the Management Console.

6.1.3 What Is the Username to Log In to an ECS?

For a Linux ECS, the login username is root. For a Windows ECS, the login username is Administrator. The login password is the one you set during ECS creation.

6.1.4 What Should I Do If My Remote Login Password Was Forgotten?

If you did not set a password when creating an ECS, or the password is forgotten or expired, reset the password by following the instructions provided in Resetting the ECS Password on the Management Console.

NOTE
Keep your password secure.

6.1.5 Why Cannot I Use the Account Used to Create a GPU-accelerated ECS to Log In to the ECS Through SSH?

Solution

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

1. On the Elastic Cloud Server page, locate the target ECS and click Remote Login in the Operation column.
2. On the login page, enter user root and its password.

NOTE
The password is the one you set during ECS creation.
3. In the `/etc/ssh/` directory, modify the three configuration items in the `sshd_config` file, as shown in the following figure.

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

   ```bash
   service sshd restart
   ```

5. Log in to the ECS through SSH.

6. If the fault persists, contact customer service.
6.1.6 What Should I Do If Starting an ECS Remains in "Waiting for cloudResetPwdAgent" State?

**Symptom**

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

**Figure 6-4 Starting cloudResetPwdAgent**

![Starting cloudResetPwdAgent](image)

**Possible Causes**

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

**Solution**

1. Log in to the ECS as user **root**.
2. Run the following command to modify the `/etc/cloud/cloud.cfg` configuration file:
   ```bash
   vi /etc/cloud/cloud.cfg
   ```
3. Add the following statement to the configuration file:
   ```
   manage_etc_hosts: true
   ```

**Figure 6-5 Editing the configuration file**

![Editing the configuration file](image)
6.2 Logins Through the Management Console

6.2.1 What Should I Do If Garbled Characters Are Displayed When I Log In to My ECS Using VNC?

Symptom

After I attempted to log in to my Linux ECS using VNC, garbled characters are displayed, as shown in Figure 6-6.

Possible Causes

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

Solution

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

```
reset
```

NOTE

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

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

If your computer is running Windows 7 and you logged in to the ECS using Internet Explorer 10 or 11, click `AltGr` twice on the VNC page to activate the page.
6.2.3 What Should I Do If I Cannot View Data After Logging In to an ECS Using VNC?

After you log in to an ECS using VNC and view data, for example, play videos or run the `cat` command to view large files, VNC may become unavailable due to the high memory usage of the browser. In such a case, use another browser and log in to the ECS again.

6.2.4 Why Does a Blank Screen Appear While the System Displays a Message Indicating Successful Authentication After I Attempted to Log In to an ECS Using VNC?

Another user has logged in to this ECS using VNC.

Only one user can log in to an ECS using VNC at a time. If multiple users attempt to log in to an ECS at the same time, only the first user can log in to it. For other users, the system displays a message indicating that the user is authenticated, but the screen turns blank. If this occurs, wait until the other user logs out of the ECS.

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

Symptom

When I attempted to remotely log in to an ECS using VNC, the system displayed error code 1006.

Possible Causes

- The ECS is running improperly.
- Another user has logged in to the ECS.
- The ECS has been automatically logged out due to operation timeout.

Troubleshooting

1. Log in to the ECS again using VNC.
   - If the login is successful, no further action is required.
   - If the fault persists, go to 2.
2. Check whether the ECS is running properly.
   Error code 1006 is displayed if the ECS is stopped, deleted, migrated, or restarted, or an operation timed out on the ECS.
3. Check whether another user has logged in to the ECS.
   If yes, you can log in to the ECS only after that user logs out.
6.2.6 Why No Audio File Can Be Properly Played on My Windows ECS Logged In Using VNC?

Symptom

Audio files can be properly played on my Windows ECS that is logged in using MSTSC. However, when I logged in to the ECS using VNC, playing the audio files failed.

Possible Causes

VNC does not support audio playing.

Solution

Use a local computer to play the audio files. The following operations use a local computer running Windows 7 as an example.

1. Start the local computer.

   ☐ NOTE

   This operation is not to log in to the Windows ECS.

2. Press Win+R to start the Open text box.

3. Enter mstsc and click OK.

   The Remote Desktop Connection window is displayed.

   Figure 6-8 Remote Desktop Connection

   ![Remote Desktop Connection](image)

4. Click Options in the lower left corner and click the Local Resources tab.
5. In the **Remote audio** pane, click **Settings**.

**Figure 6-10** Setting remote audio playback

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

### 6.2.7 How Can I Change the Resolution of a Windows ECS?

**Scenarios**

The resolution of a Windows ECS that is remotely logged in must be changed.
Solution 1: Using VNC

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

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

   ![Display settings](image)

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

   **NOTE**

   If the remote desktop is not fully displayed, set **Change the size of text, apps, and other items** to 100%.
4. In the **Resolution** drop-down list, select the desired resolution.

**Figure 6-13 Setting a resolution**

5. Click **Apply**.

**Solution 2: Using MSTSC**

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

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

**Figure 6-14 Remote Desktop Connection**

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

**Figure 6-15 Display**

5. Use MSTSC to log in to the ECS.
6.3 Remote Logins

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

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

Possible Causes
The local computer used by the user is running the Windows 10 OS.
Due to limitations, the Windows 10 OS does not support remote logins to an ECS running the Windows Server 2012 OS using the initial password.

Solutions
- Solution 1
  Use a local computer running the Windows 7 OS to remotely log in to the ECS running the Windows Server 2012 OS.
- Solution 2
  Retain the original local computer and change the initial login password.
  a. Use VNC to log in to the ECS running the Windows Server 2012 OS for the first time.
  b. Change the login password as prompted.
  c. Use the changed password and MSTSC to log in to the ECS again.
- Solution 3:
  Retain the original local computer and initial login password.
  a. Choose Start. In the Search programs and files text box, enter mstsc and press Enter.
     The Remote Desktop Connection page is displayed.
  b. Enter the EIP and click Connect. Then, use username administrator and the login password configured during ECS creation for connection.
     The connection fails, and the system displays the message "You must change your password before logging on for the first time. Please update your password or contact your system administrator or technical support."
  c. Click Options in the lower left corner of the Remote Desktop Connection page.
  d. On the General tab, click Save As in the Connection settings pane and save the remote desktop file in .rdp format.
  e. Use Notepad++ to open the .rdp file.
  f. Add the following statement to the last line of the .rdp file and save the file.
     enablecredsspssupport:i:0
6.3.2 What Should I Do If I Cannot Log In to My Windows ECS?

**Symptom**

An ECS cannot be logged in due to some reasons, for example, the network malfunctions, the local port for accessing the remote desktop is denied on the firewall, or the CPU is overloaded on the ECS.

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

**Attempting Login Using VNC on the Management Console**

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

*NOTE*

Click here to learn the preparations for logging in to an ECS.

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

**Figure 6-16 Remote Login**

![Remote Login](image)

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

**Figure 6-17 Ctrl+Alt+Del**

![Ctrl+Alt+Del](image)

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

If you can log in to the ECS using VNC but cannot log in to the ECS using a remote desktop connection, locate the fault as follows:

1. Checking Whether the Network Is Functional
2. Checking Whether the Firewall Is Correctly Configured
3. Checking Whether the Remote Access Port Is Correctly Configured
4. Checking Whether the CPU Is Overloaded
5. Checking Whether an Error Occurs During a Remote Login

Checking Whether the Network Is Functional

Check whether the EIP bound to the ECS can be pinged.

If the EIP cannot be pinged, resolve this issue by following the instructions provided in Why Cannot an EIP Be Pinged?

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

Checking Whether the Firewall Is Correctly Configured

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

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

---

**NOTICE**

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 Whether the Remote Access Port Is Correctly Configured

1. Check whether port 3389 on the ECS is accessible.
   - If the port is inaccessible, check whether this port is allowed in the security group.
     - Learn how to modify a security group rule.

   2. Check whether the remote access port on the ECS has been changed.
      a. Choose Start > Run, enter cmd, and press Enter. In the CLI, enter regedit to open Registry Editor.
      b. In HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalSer
3. Check whether the number of connections to the ECS is limited.
   Check the internal remote desktop configuration of the ECS.
   a. Choose Start > Run, enter cmd, and press Enter. In the CLI, enter gedit.msc to open Local Group Policy Editor.
   b. Choose Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections. Then, in the Limit number of connections dialog box, check whether the number is limited.

   ![Image](image1.png)

   **NOTE**

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

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

**Checking Whether the CPU Is Overloaded**

If the login failure is caused by high CPU usage, perform the following operations to reduce the CPU usage:

```plaintext
ver\WinStations\RDP Tcp\Port Number, check whether the port is the default one, port 3389. If not, change the port to the configured one for remote logins.
```

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

   ![Image](image1.png)

   **NOTE**

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

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

**Checking Whether the CPU Is Overloaded**

If the login failure is caused by high CPU usage, perform the following operations to reduce the CPU usage:

```plaintext
ver\WinStations\RDP Tcp\Port Number, check whether the port is the default one, port 3389. If not, change the port to the configured one for remote logins.
```
Stop certain processes that are not used temporarily and try again.
Verify that the Windows Update process is not running on the backend.
Restart the ECS.
Reinstall the ECS OS. Back up important data before the reinstallation.
If the ECS OS cannot be reinstalled due to important data, replace the disk attached to the ECS. To do so, back up data on the original disk, detach the disk from the ECS, attach the new disk to the ECS, and copy data to the new disk.

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

Checking Whether an Error Occurs During a Remote Login

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

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

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

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.

6.3.3 What Should I Do If I Cannot Log In to My Linux ECS?

Symptom

An ECS cannot be logged in due to some reasons, for example, the network malfunctions, the local port for accessing the remote desktop is denied on the firewall, or the CPU is overloaded on the ECS.

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

Attempting Login Using VNC on the Management Console

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

#ab NOTEB
Click here to learn the preparations for logging in to an ECS.
1. Log in to the management console.
3. In the Operation column of the target ECS, click Remote Login.
4. (Optional) When the system displays "Press CTRL+ALT+DELETE to log on", click Ctrl+Alt+Del in the upper part of the remote login page to log in to the ECS.

**NOTE**

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

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

**Fault Locating**

If you can log in to the ECS using VNC but cannot log in to the ECS using a remote desktop connection, locate the fault as follows:

1. **Checking Whether the Network Is Functional**
2. **Checking Whether the Security Group Is Correctly Configured**
3. **Checking Whether the Remote Access Port Is Correctly Configured**
4. **Checking Whether the CPU Is Overloaded**
5. **Checking Whether an OS Fault Has Occurred**

**Checking Whether the Network Is Functional**

Check whether the EIP bound to the ECS can be pinged.

If the EIP cannot be pinged, resolve this issue by following the instructions provided in Why Cannot an EIP Be Pinged?

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

**Checking Whether the Security Group Is Correctly Configured**

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

Run the following command:

```
telnet Private IP address of the peer ECS
```

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

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

After performing the preceding operations, try to remotely log in to the ECS again.
Checking Whether the Remote Access Port Is Correctly Configured

Check the internal configuration of the affected ECS.

1. Verify that the sshd process is running.
2. Check whether the local computer is restricted on the ECS.
   a. Log in to the ECS and run the following command to check the configuration:

   ```
   vi /etc/hosts.deny
   ```
   b. If the IP address of the local computer is detected, the IP address is denied. In such a case, delete the IP address from the file.
3. Switch to the file in `/etc/ssh/ssh_config` on the local computer and view the default login port. Then, check whether the SSH-enabled port in the file in `/etc/ssh/sshd_config` on the ECS has been changed (the default port number is 22).

   ```
   Port 22
   AddressFamily any
   ```

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

Checking Whether the CPU Is Overloaded

If the login failure is caused by high CPU usage, perform the following operations to reduce the CPU usage:

- Stop certain processes that are not used temporarily and try again.
- Restart the ECS.
- Reinstall the ECS OS. Back up important data before the reinstall.
- If the ECS OS cannot be reinstalled due to important data, replace the disk attached to the ECS. To do so, back up data on the original disk, detach the disk from the ECS, attach the new disk to the ECS, and copy data to the new disk.

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

Checking Whether an OS Fault Has Occurred

- Password injection failure
  Failing to obtain a password is generally due to a Cloud-Init-based password injection failure. See What Should I Do If I Cannot Log In to an ECS with Cloud-Init Enabled? for troubleshooting.
- File system damaged after a forcible stop
  There is a low probability that the file system is damaged. As a result, the ECS fails to be restarted. See What Should I Do If the Forcibly Stopped Linux ECS Fails to Start Due to File System Damage? for troubleshooting.

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

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

Possible Causes

After the default SSH port on a Linux ECS is changed, if the new port is not correctly configured in the SSH configuration file or firewall security policy, the new port cannot be used to log in to the ECS.

Solution

1. Check whether the new port is correctly configured in the security group. If the changed SSH port is 12345, ensure that this port is allowed in the inbound direction when other parameters are set to Any in the outbound direction.

2. Check whether port 12345 is allowed on the iptables firewall.

3. Log in to the ECS and check the SSH configuration file.
   a. Run the following command to check whether port 12345 has been configured:
      ```bash
      vi /etc/ssh/sshd_config
      ```
   b. If the port has not been configured, replace #Port 22 with Port 12345.
   c. Run the following command to restart SSH:
      ```bash
      service sshd restart
      ```

6.3.5 What Should I Do If I Cannot Log In to an ECS with Cloud-Init Enabled?

Symptom

For a key-pair-authenticated ECS, obtaining its login password using a private key file failed.

Possible Causes

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

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

Solution

If logging in to an ECS with Cloud-Init enabled failed, perform the following operations to locate the fault:
1. Ensure that Cloud-Init has been correctly configured on the image based on which the ECS was created.
   Cloud-Init has been correctly configured for all public images. Skip this step for public images. Check the Cloud-Init configuration on non-public images.
2. Ensure that the key pair for logging in to the ECS is correct.
3. Ensure that DHCP is enabled in the VPC to which the ECS belongs.
4. Ensure that the ECS has an EIP bound.
5. View security group rules in the outbound direction and ensure that port 80 is accessible.

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

When you use a browser to remotely log in to an ECS, ensure that the browser version meets the requirements listed in Table 6-1.

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>31.0-75.0</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>27.0-62.0</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>10.0-11.0</td>
</tr>
</tbody>
</table>

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

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

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

Handling Method
To handle this issue, perform the following operations to change the core mode back to full:
1. Log in to the ECS.
2. In the upper right corner, click Send CtrlAltDel and start the task manager.
3. Choose File > Run new task.
   The Create new task page is displayed.
4. In the Open text box, type cmd and press Enter.
5. Run the following command to change the system mode from core to full:
   ```
   ```
6. After about 10 minutes, the system displays a message, asking you whether to restart the system. In such an event, press Y to restart the system.
   You can access the desktop after logging in to the ECS again.

### 6.3.8 How Can I Log In to an ECS After Its System Disk Is Exchanged with That Attached to Another ECS Running the Same OS?

#### Symptom

Two pay-per-use ECSs run the same OS, for example, both run Windows or Linux. The system disks attached to the two stopped ECSs are exchanged. After the exchanging, the login passwords or keys of the ECSs may change. In such a case, how can I log in to the ECSs?

#### NOTE

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

1. Log in to the Windows ECS.
2. Run the following command to release the IP address:
   ```
   ipconfig /release
   ```
   This operation will interrupt network connections and affect the use of the ECS. After the ECS is restarted, network connections will automatically recover.

#### Windows

Login methods vary according to the login authentication used on the ECSs. For example, there are three Windows ECSs with parameters configured in Table 6-2.
Table 6-2 Parameter configurations

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

- Scenario 1: System disk vol_01 is detached from ecs_01 offline and then attached to ecs_02 as the system disk. How can I log in to ecs_02?
  After ecs_02 starts up, use its initial password Ecs@02 to log in to the ECS.

- Scenario 2: System disk vol_01 is detached from ecs_01 offline and then attached to ecs_03 as the system disk. How can I log in to ecs_03?
  The random password for logging in to ecs_03 must be resolved again. The procedure is as follows:
  a. Delete the initial password for logging in to ecs_03.
     - Locate the row containing ecs_03, click More in the Operation column, and select Delete Password from the drop-down list. Then, click OK.
  b. Start ecs_03.
     - Locate the row containing ecs_03, click More in the Operation column, and select Start from the drop-down list. Then, in the Start ECS dialog box, click OK.
  c. Obtain the password for logging in to ecs_03.
     i. Locate the row containing ecs_03, click More in the Operation column, and select Get Password from the drop-down list.
     ii. Click Select File and upload private key file Keypair_03 of ecs_03.
     iii. Click Get Password to obtain a new random password.
  d. Use the random password obtained in step c to log in to ecs_03 with the system disk replaced.

**Linux**

Login methods vary according to the login authentication used on the ECSs. For example, there are three Linux ECSs with parameters configured in Table 6-2.
### Parameter configurations

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

- **Scenario 1:** System disk vol_01 is detached from ecs_01 offline and then attached to ecs_02 as the system disk. How can I log in to ecs_02?
  
  Use either of the following methods to log in to ecs_02:
  
  - Use private key file Keypair_01 (if available) of ecs_01.
  
  - Use the original password Ecs@02 of ecs_02.

- **Scenario 2:** System disk vol_01 is detached from ecs_01 offline and then attached to ecs_03 as the system disk. How can I log in to ecs_03?
  
  Use one of the following methods to log in to ecs_03:
  
  - Use the password Ecs@01 (if available) of ecs_01.
  
  - Use private key file Keypair_01 (if available) of ecs_01.
  
  - Use private key file Keypair_03 of ecs_03.

### Why Does the System Display a Message Indicating that the Password for Logging In to a Windows ECS Cannot Be Viewed?

#### Symptom

Password authentication is required to log in to a Windows ECS. Therefore, a key file is required to obtain the initial password for logging in to the ECS. However, after Get Password is clicked, the system displays a message indicating that the password could not be viewed. ECS login was therefore unsuccessful.

#### Possible Causes

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

- **Cause 1:** The image used to create the Windows ECS is a private image, on which Cloudbase-Init has not been installed.

- **Cause 2:** Cloudbase-Init has been installed on the image, but the key pair had not been obtained when the Windows ECS was created.

#### Solution

- If the issue is a result of cause 1, proceed as follows:
If a private image is created without Cloudbase-Init installed, the ECS configuration cannot be customized. As a result, you can log in to the ECS only using the original image password.

The original image password is the OS password configured when the private image was created. If the original image password has been forgotten, use the password reset function available on the Elastic Cloud Server page to reset the password.

- If the issue is a result of cause 2, proceed as follows:
  a. Locate the row containing the target ECS, click More in the Operation column, and select Restart.
  b. Click More in the Operation column and select Get Password to check whether the password can be obtained.
     - If the password can be obtained, no further action is required.
     - If no, contact technical support.

### 6.4 Remote Login Errors on Windows

#### 6.4.1 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 6-20, 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 6-20 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).
5. Click OK.

6.4.2 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**.

   ![ gpedit.msc dialog box with instructions to enter gpedit.msc and press OK ]

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

   ![ Locating the network access policy dialog box ]

4. Select **Classic - local users authenticate as themselves** and click **OK**.
Figure 6-24 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 `gedit.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 6-26 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 6-28 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 6-30 Add a Windows Credential

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.
4. Click Save changes.

6.4.3 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.

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 12.1.4 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.

### 6.4.4 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.

### 6.4.5 What Should I Do If BSOD Occurs When I Log In to a Windows Server 2012 ECS Using Remote Desktop Connection?

**Symptom**
When I attempted to use remote desktop connection to log in to an ECS running Windows Server 2012 R2 from a local computer with redirected drive enabled, blue screen of death (BSOD) occurred.

**Root Cause**
The remote desktop connection with redirected drive enabled loads the desired rdpdr.sys drive, which leads to BSOD and error code 0x18, 0x50, 0xa, 0x27, or 0x133.
Solution

After enabling the remote desktop connection, disable redirect local drives.

1. Start the Run dialog box.
2. Enter mstsc and click OK.
   The Remote Desktop Connection window is displayed.
3. Click Options in the lower left corner and click the Local Resources tab.
4. In the Local devices and resources pane, click More.
5. Deselect Drives.
6. Click OK.

Figure 6-33 Disabling redirect local drives
7 ECS Management

7.1 Changing Hostnames

7.1.1 How Can a Changed Static Hostname Take Effect Permanently?

Symptom

The static hostname of a Linux ECS is user defined and injected using Cloud-Init during the ECS creation. Although the hostname can be changed by running the `hostname` command, the changed hostname is restored after the ECS is restarted.

Changing the Hostname on the ECS

To make the hostname changed by running the `hostname` command take effect even after the ECS is stopped or restarted, save the changed hostname into configuration files.

The changed hostname is assumed to be `new_hostname`.

**Step 1** Modify the `/etc/hostname` configuration file.

1. Run the following command to edit the configuration file:
   ```bash
   sudo vim /etc/hostname
   ```
2. Change the hostname to the new one.
3. Run the following command to save and exit the configuration file:
   ```bash
   :wq
   ```

**Step 2** Modify the `/etc/sysconfig/network` configuration file.

1. Run the following command to edit the configuration file:
   ```bash
   sudo vim /etc/sysconfig/network
   ```
2. Change the HOSTNAME value to the new hostname.
   ```bash
   HOSTNAME=Changed hostname
   ```

**NOTE**

If there is no HOSTNAME in the configuration file, manually add this parameter and set it to the changed hostname.

An example is provided as follows:
### Hostname Change

1. Run the following command to save and exit the configuration file:
   ```bash
   :wq
   ```

#### Step 3 Modify the `/etc/cloud/cloud.cfg` configuration file.

1. Run the following command to edit the configuration file:
   ```bash
   sudo vim /etc/cloud/cloud.cfg
   ```
2. Use either of the following methods to modify the configuration file:
   - **Method 1:** Change the `preserve_hostname` parameter value or add the `preserve_hostname` parameter to the configuration file.
     If `preserve_hostname: false` is already available in the `/etc/cloud/cloud.cfg` configuration file, change it to `preserve_hostname: true`. If `preserve_hostname` is unavailable in the `/etc/cloud/cloud.cfg` configuration file, add `preserve_hostname: true` before `cloud_init_modules`.
     If you use method 1, the changed hostname still takes effect after the ECS is stopped or restarted. However, if the ECS is used to create a private image and the image is used to create a new ECS, the hostname of the new ECS is the hostname `(new_hostname)` used by the private image, and user-defined hostnames cannot be injected using Cloud-Init.
   - **Method 2** (recommended): Delete or comment out `-update_hostname`.
     If you use method 2, the changed hostname still takes effect after the ECS is stopped or restarted. If the ECS is used to create a private image and the image is used to create a new ECS, the changed hostname permanently takes effect, and user-defined hostnames (such as `new_new_hostname`) can be injected using Cloud-Init.

#### Step 4 Run the following command to restart the ECS:
   ```bash
   sudo reboot
   ```

#### Step 5 Run the following command to check whether the hostname has been changed:
   ```bash
   sudo hostname
   ```

If the changed hostname is displayed in the command output, the hostname has been changed and the new name permanently takes effect.

---

### 7.1.2 Is an ECS Hostname with Suffix `.novalocal` Normal?

#### Symptom

Hostnames of some ECSs have the suffix `.novalocal`.

For example, the hostname is set to `abc` during ECS creation. Table 7-1 lists the hostnames (obtained by running the `hostname` command) of ECSs created using different images and those displayed after the ECSs are restarted.

<table>
<thead>
<tr>
<th>Image</th>
<th>Hostname Before ECS Restart</th>
<th>Hostname After ECS Restart</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

2019-12-02
<table>
<thead>
<tr>
<th>Image</th>
<th>Hostname Before ECS Restart</th>
<th>Hostname After ECS Restart</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS 6.8</td>
<td>abc</td>
<td>abc.novalocal</td>
</tr>
<tr>
<td>CentOS 7.3</td>
<td>abc.novalocal</td>
<td>abc.novalocal</td>
</tr>
<tr>
<td>Ubuntu 16</td>
<td>abc</td>
<td>abc</td>
</tr>
</tbody>
</table>

Hostnames of ECSs created based on some types of images have the suffix `.novalocal`, while others do not.

**Troubleshooting**

This is a normal phenomenon.

The static hostname of a Linux ECS is user defined and injected using Cloud-Init during the ECS creation. According to the test results, Cloud-Init adapts to OSs differently. As a result, hostnames of some ECSs have suffix `.novalocal`, while others do not.

If you do not need suffix `.novalocal` in obtained hostnames, change the hostnames. For details, see “How Can a Changed Static Hostname Take Effect Permanently?”

**7.1.3 What Should I Do If the Hostname of My ECS Is Restored After the ECS Is Restarted?**

The following uses an ECS running the CentOS 7 OS as an example:

1. Log in to the ECS and view the Cloud-Init configuration file.
2. In the `/etc/cloud/cloud.cfg` file, comment out or delete `update_hostname`.

**NOTE**

- `update_hostname` indicates that the hostname is changed in Cloud-Init each time the ECS is restarted.
- `update_hostname` is commented out in public images by default. For instructions about how to comment out `update_hostname` in private images, see Installing Cloud-Init.

**7.2 Modifying Specifications**

**7.2.1 How Can I Modify Specifications of ECSs Charged in Yearly/Monthly Mode?**

You can modify ECS specifications anytime you want. Before modifying ECS specifications, stop the ECS, select target specifications, pay for extra fees, and restart the ECS to make the modification take effect.

**7.2.2 How Can I Modify Specifications of ECSs Charged in Pay-Per-Use Mode?**

You can modify your ECS specifications at any time without paying for the difference.
Before modifying the specifications, stop the ECS. Then, on the Elastic Cloud Server page, click More in the Operation column and select Modify Specifications. Then, start the ECS.

### 7.2.3 What Should I Do If the Data Disk of a Windows ECS Becomes Offline After the ECS Specifications Are Modified?

#### Scenarios

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

#### Procedure

1. Check whether the number of disks displayed on the Computer page after specifications modification is the same as that before specifications modification.
   - If yes, the disks are properly attached. No further action is required.
   - If no, an error has occurred in disk attachment. In such a case, go to step 2.

For example:

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

**Figure 7-1 Disk attachment before specifications modification**

![Disk attachment before specifications modification](image)

After the specifications are modified, check disk attachment.
Only one system disk is displayed. Data disks failed to attach after the specifications modification.

2. Set the affected disks to be online.
   a. Click Start in the task bar. In the displayed Start menu, right-click Computer and choose Manage from the shortcut menu.
      The Server Manager page is displayed.
   b. In the navigation pane on the left, choose Storage > Disk Management.
      The Disk Management page is displayed.
   c. In the left pane, the disk list is displayed. Right-click the affected disk and choose Online from the shortcut menu to make it online.
3. On the **Computer** page, check whether the number of disks is the same as that before the specifications modification.
   - If the numbers are the same, no further action is required.
   - If the numbers are different, contact customer service.
7.2.4 What Should I Do If the Disk of a Linux ECS Becomes Offline After the ECS Specifications Are Modified?

Scenarios

After Linux ECS specifications are modified, disk attachment may fail. Therefore, check disk attachment after specifications modification. This section describes how to check disk attachment after ECS specifications are modified.

Procedure

1. Log in to the ECS as user root.
2. Run the following command to view the disks attached before specifications modification:
   
   ```
   fdisk -l | grep 'Disk /dev/
   ```

   ![Figure 7-5 Viewing disks attached before specifications modification](image)

   As shown in Figure 7-5, the ECS has three disks attached: /dev/vda, /dev/vdb, and /dev/vdc.

3. Run the following command to view disks attached after specifications modification:
   
   ```
   df -h| grep '/dev/
   ```

   ![Figure 7-6 Viewing disks attached after specifications modification](image)

   As shown in Figure 7-6, only one disk /dev/vda is attached to the ECS.

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

5. Run the `mount` command to attach the affected disks.
   
   For example, run the following command:
   
   ```
   mount /dev/vbd1 /mnt/vbd1
   ```

   In the preceding command, /dev/vbd1 is the disk to be attached, and /mnt/vbd1 is the path for disk attachment.
Ensure that /mnt/vbd1 is empty. Otherwise, the attachment will fail.

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

   fdisk -l | grep 'Disk /dev/

   df -h | grep '/dev/'

   - If the numbers are the same, no further action is required.
   - If the numbers are different, contact customer service.

   **Figure 7-7 Checking the number of disks attached**

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

7.3 Usage Errors

7.3.1 How Do I Handle Error Messages Displayed on the Management Console?

**Symptom**

- An error message was displayed on the management console after you performed ECS-related operations.
- An error code was displayed after you used an ECS API (see Elastic Cloud Server API Reference).

**Background**

After you perform ECS-related operations on the management console, the system displays the request status on the Elastic Cloud Server page. You can determine the request execution status based on the information displayed in the request status.

- If the operation request is executed, the system automatically clears the task prompt.
- If an error occurs during the request execution, the system displays an error code and its description in the taskbar.
Solution

If an error occurs, find the error code and perform the corresponding operations listed in Table 7-2.

Table 7-2 Error codes and solution suggestions

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Message Displayed on the Management Console</th>
<th>Solution Suggestion for Pay-Per-Use ECSs</th>
<th>Solution Suggestion for Yearly/Monthly ECSs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ecs.0000</td>
<td>Request error. Try again later or contact customer service.</td>
<td>Adjust the request structure as directed in Elastic Cloud Server API Reference.</td>
<td>Adjust the request structure as directed in Elastic Cloud Server API Reference.</td>
</tr>
<tr>
<td>Ecs.0001</td>
<td>The maximum number of ECSs or EVS disks has been reached. Contact customer service and request a quota increase.</td>
<td>Contact customer service to apply for an increased ECS quota. <strong>NOTE</strong> When applying for increasing your ECS quota, first determine the number of target ECSs, CPU cores (vCPUs), and memory capacity (RAM) required.</td>
<td>Submit a service ticket to apply for an increased ECS quota. After the submission, contact customer service for troubleshooting. <strong>NOTE</strong> When applying for increasing your ECS quota, first determine the number of target ECSs, CPU cores (vCPUs), and memory capacity (RAM) required.</td>
</tr>
<tr>
<td>Ecs.0005</td>
<td>System error. Try again later or contact customer service.</td>
<td>Adjust the request structure as directed in Elastic Cloud Server API Reference.</td>
<td>Adjust the request structure as directed in Elastic Cloud Server API Reference.</td>
</tr>
<tr>
<td>Ecs.0006</td>
<td>Invalid parameters.</td>
<td>If your selected ECS configuration has not been released, change the configuration and create the ECS again.</td>
<td>If your selected ECS configuration has not been released, change the configuration and create the ECS again.</td>
</tr>
<tr>
<td>Ecs.0010</td>
<td>The private IP address is in use. Select an available IP address and create the ECS again.</td>
<td>Use idle IP addresses to purchase your ECSs.</td>
<td>Contact customer service to cancel the order and use an idle IP address to purchase your ECS.</td>
</tr>
<tr>
<td>Ecs.0011</td>
<td>Invalid password. Change the password to make it meet the password complexity requirements, and perform the</td>
<td>Input a password that meets password complexity requirements.</td>
<td>Contact customer service to cancel the order, input a password that meets password complexity requirements, and perform the request again.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Message Displayed on the Management Console</td>
<td>Solution Suggestion for Pay-Per-Use ECSs</td>
<td>Solution Suggestion for Yearly/Monthly ECSs</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Ecs.0012</td>
<td>The number of IP addresses in the subnet is insufficient. Release IP addresses in the subnet or select another subnet, and create the ECS again.</td>
<td>Obtain more idle IP addresses on the target subnet or use a new subnet for purchasing ECSs.</td>
<td>Obtain more idle IP addresses on the target subnet and contact customer service for troubleshooting. Alternatively, contact customer service to cancel the order and use a new subnet for purchasing ECSs.</td>
</tr>
<tr>
<td>Ecs.0013</td>
<td>Insufficient EIP quota. Contact customer service and request a quota increase.</td>
<td>Contact customer service to apply for an increased EIP quota.</td>
<td>Submit a service ticket to apply for an increased EIP quota and contact customer service for troubleshooting.</td>
</tr>
<tr>
<td>Ecs.0015</td>
<td>This disk type is not supported by the ECS.</td>
<td>Select a supported EVS disk and attach it to the ECS.</td>
<td>Select a supported EVS disk and attach it to the ECS.</td>
</tr>
<tr>
<td>Ecs.0100</td>
<td>The ECS status does not meet requirements. Change to the desired ECS status and try again.</td>
<td>Change to the desired ECS status and try again.</td>
<td>Change the ECS status to the required status and contact customer service for troubleshooting.</td>
</tr>
<tr>
<td>Ecs.0104</td>
<td>Insufficient number of ECS slots for attaching disks.</td>
<td>Detach an EVS disk from the ECS before attaching a new EVS disk.</td>
<td>Detach an EVS disk from the ECS before attaching a new EVS disk.</td>
</tr>
<tr>
<td>Ecs.0105</td>
<td>No system disk found.</td>
<td>Reattach the EVS system disk to the ECS and perform the desired operation again.</td>
<td>Reattach the EVS system disk to the ECS and contact customer service for troubleshooting.</td>
</tr>
<tr>
<td>Ecs.0107</td>
<td>The number of shared disks that can be attached to an ECS exceeds the maximum limit.</td>
<td>Detach an EVS disk from the ECS before attaching a new EVS disk.</td>
<td>Detach an EVS disk from the ECS before attaching a new EVS disk.</td>
</tr>
<tr>
<td>Ecs.0509</td>
<td>This operation is not allowed on a yearly/monthly system disk. Select a pay-per-use system disk and</td>
<td>N/A</td>
<td>Change the ECS billing mode to pay-per-use and perform the desired operation again.</td>
</tr>
</tbody>
</table>
### Error Code Displayed on the Management Console

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Message Displayed on the Management Console</th>
<th>Solution Suggestion for Pay-Per-Use ECSs</th>
<th>Solution Suggestion for Yearly/Monthly ECSs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ecs.051</td>
<td>Yearly/Monthly ECSs do not support OS changing.</td>
<td>N/A</td>
<td>Change the ECS billing mode to pay-per-use and perform the desired operation again.</td>
</tr>
</tbody>
</table>

### 7.3.2 How Can I Recover a Windows ECS with an Abnormal Virtualization Driver?

**Background**

An error occurs in the virtualization driver on a Windows ECS because Tools is not properly running. To ensure proper ECS running, handle this issue by following the instructions provided in this section.

**Issue Description**

The virtualization driver of some ECSs became abnormal, which affected the data security, availability, and system performance of these ECSs.

The impact of this issue is as follows:

1. The file system of these ECSs might be damaged.
   When you stop or restart such ECSs on the management console, the ECSs will be forcibly stopped or restarted due to the lack of the virtualization driver.

2. Services on the ECSs become unavailable.
   The affected ECSs cannot be hot migrated between physical servers. When the physical server accommodating such an ECS becomes faulty or the hardware of the physical server is maintained, the ECS cannot be migrated to another physical server, affecting service high availability.

3. The network and storage performance of the ECSs is deteriorated.
   The virtualization driver improves the network and storage performance of ECSs. Therefore, when the virtualization driver becomes abnormal, the network and storage performance is deteriorated.

**Scenarios**

- **Scenario 1**
  A Windows ECS has no Tools installed.

- **Scenario 2**
  The virtualization driver of an ECS has been uninstalled.
Procedure

Perform the following operations to install Tools on the Windows ECS:

1. Obtain the Tools installation package **pvdriver-windows.zip**.
   To download the installation package, log in at
2. Decompress the software package and double-click **setup.exe** to start the installation.

**Figure 7-8** Installing the virtualization driver

3. Click **Next** and select "I accept the terms in the License Agreement".
4. Click **Install** to start the installation.
5. Click **Finish** to complete the installation.

**Figure 7-10** Installation completed
6. Restart the ECS.

**Figure 7-11** Determining whether to restart the ECS

7. View the virtualization driver status in the bottom right corner of the ECS desktop. The yellow icon indicates that the virtualization driver is running properly.

**Figure 7-12** Proper running status of the virtualization driver

### 7.3.3 What Should I Do If I Cannot Activate a Windows ECS?

**Symptom**

A Windows ECS is automatically activated within two hours after it is purchased. However, it is still not activated after two hours.

**Prerequisites**

The IP address of the HUAWEI CLOUD DNS server has been configured.

**Handling Method**

1. Manually activate the Windows ECS.
   
   To do so, perform the following operations:
   
   a. Choose **Start > Run**. In the **Run** text box, type **cmd**.
   b. Run the following command to check whether the IP address of the KMS server is correct:

   ```
   slmgr -dli
   ```
If the obtained IP address is the same as that shown in the red box of Figure 7-13, the IP address of the KMS server is correct.

If the obtained IP address is different from that shown in the red box of Figure 7-13, the IP address of the KMS server is incorrect. In this case, run the following command to register the ECS with the KMS server:

```
slmgr -skms 100.125.1.2
```

If the system displays an error, indicating that the link to the server is inaccessible, check whether the IP address of the HUAWEI CLOUD DNS server has been configured.

c. Run the following command to check whether the ECS has been activated:

```
slmgr -ato
```

If error 0xC004F074 occurs, activating the ECS failed. In this event, go to step 2.

2. Identify the cause of the ECS activation failure.

a. Check whether the private IP address of the ECS is correct.

i. Run the following command to obtain the private IP address:

```
ipconfig
```

ii. Check whether this IP address is the same as the private IP address displayed on the management console.

- If yes, go to step 2.b.
- If no, go to step 2.a.iii.
iii. Run the following command to release the private IP address:

```
ipconfig /release
```

iv. Run the following command to assign an IP address to the ECS again:

```
ipconfig /renew
```

v. Run the following command to check whether the ECS has been activated:

```
slmgr -ato
```

b. Verify that the time in the ECS is the same as the standard time. If the time is significantly different, the ECS cannot be activated.

c. Run the following command on the ECS to check whether the link between the ECS and the activated server port is reachable:

```
telnet 100.125.1.2 1688
```

Check whether all ports and protocols are bypassed in the outbound direction of the security group.

d. Run the following command to check whether the ECS has been activated:

```
slmgr -ato
```

The system displays a message indicating that the ECS has been activated.

### 7.3.4 What Should I Do If Emails Configured on an ECS Cannot Be Sent?

**Solution**

- For the emails sent using the browser:
  
  When you use a browser to log in to your mailbox, HTTP is used, and the default port number is 80. However, SMTP is used between email servers.
  
  If you use a browser to send emails, enable port 80 for TCP in the outbound direction.

  a. On the page providing details about the target ECS, find the security group and click the security group ID.

  ![Security Group Page]

  b. On the **Security Group** page, click the **Outbound** tab and then **Add Rule**.

  c. In the dialog box that is displayed, set **Protocol/Application** to TCP and **Port** to 80. Then, click **OK**.
For the emails sent and received by an email client:
If you use an email client, SMTP is used to send emails and the port number is 25; POP3 is used to receive emails and the port number is 110.
For details, see steps a to c.

-note
Add an inbound rule with Protocol/Application set to TCP and Port to 110. Add an outbound rule with Protocol/Application set to TCP and Port to 25.

Related Operations (Requesting for Permitting TCP Port 25 for Outbound Transmission)

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

1. On the Create Service Ticket page, choose Products > Elastic Cloud Server. For details about how to submit a service ticket, see Submitting a Service Ticket.
2. Click Open Port 25 under Select Subtype and click Create Service Ticket.

Figure 7-14 Creating a service ticket

3. On the displayed page, enter the required information as prompted.
7.3.5 Why Is My Windows ECS Muted?

Symptom

No audio file can be played on a Windows ECS that is remotely accessed using MSTSC. How can I play an audio file on such an ECS?

Constraints

This section applies to ECSs running Windows Server 2008 R2 or Windows Server 2016.

Possible Causes

The audio function is disabled on Windows ECSs by default. As a result, audio files cannot be played on them. To enable the audio function, perform the operations described in this section.

Step 1: Enable Windows Audio

Enable Windows audio and set it to run automatically.

1. Start the Run dialog box.
2. Enter services.msc to access the service management console.
3. Find Windows Audio and set it as follows:
   - Startup type: Automatic
   - Service status: Start

The following figure uses Windows Server 2012 as an example.

4. Disable the remote connection.

Step 2: Enable Audio and Video Playback

The method of enabling audio and video playback varies depending on the ECS OS.

Windows Server 2008

Step 1 Enable RDP-TCP Audio and video playback and Audio recording.

1. Log in to the Remote Desktop Session Host Configuration management console.
   a. Choose Start > Control Panel.
   b. In the upper right corner of the page, choose Category for View by.
c. Choose **System and Security > Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration**.

2. Deselect **Audio and video playback** and **Audio recording**.
   
   In the **Connections** pane, double-click **RDP-Tcp**. In the **RDP-Tcp Properties** dialog box, click the **Client Settings** tab and deselect **Audio and video playback** and **Audio recording**.

![Remote Desktop Session Host Configuration](image)

Figure 7-15 Remote Desktop Session Host Configuration

3. Click **OK** to enable the audio function.

   **Step 2** Click **Send CtrlAltDel** to restart the ECS and log in to it.

   **Step 3** Enable the audio service.

   ![Enabling the audio service](image)

   **Figure 7-16** Enabling the audio service

   **Step 4** Play an audio file to verify the service.

   ----End

**Windows Server 2012**

**Step 1** Start the **Run** dialog box.

**Step 2** Run the **gpedit.msc** command to start **Local Group Policy Editor**.
Step 3  Choose **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection**. Then, enable **Allow audio and video playback redirection**.

Step 4  Select **Enabled** and click **Apply**.

![Configuration settings screenshot](image)

Retain the default settings of MSTSC.

Step 5  Run the following command to update the group policy:

```
gpupdate
```

----
End

**Step 3: Configure Remote Audio Settings**

Start the local remote desktop software MSTSC, choose **Options > Local Resources**, and click **Settings in Remote audio**. Then, select **Play on this computer** in **Remote audio playback** and click **OK**.
Log in to the ECS using MSTSC and check whether audio can be played properly.

7.3.6 How Do I Change an ECS SID?

Microsoft identifies computers and users by security identifier (SID). The ECSs created using an image have the same SID. If such ECSs are required to join in a Windows domain, they must use different SIDs.

This section describes how to use SIDCHG to change an ECS SID.

To change SIDs in a batch, use a private image and follow the operations provided in "Running Sysprep". For details, see Image Management Service User Guide.

---

**NOTICE**

Changing an ECS SID may lead to data loss or system damage. Therefore, back up data before changing the SID.

---

**Procedure**

1. Click **SIDCHG** to download it.

   **NOTE**
   
   For the server edition, download the 64-bit version.

   **Figure 7-17 Downloading SIDCHG**

   ![SIDCHG 2.0](image)

   SIDCHG 2.0
   
   SIDCHG and SIDCHG64 (64-bit Windows)
   
   These are directly executables of SIDCHG SID Change Utility. There is no installation program.

   It is important to not interrupt SID change in process. Additionally, on Windows 10, Do not Log in into the computer during SID change! Logging in will affect Start Menu and modern Windows interfaces and apps.

2. Run the following command to change the ECS SID:

   `sidchg64-2.0n.exe /R`
In the preceding command, /R indicates that the ECS automatically restarts after its SID is changed, and /S indicates that the ECS does not automatically restart.

3. Enter the trial key or license as prompted and press Enter.

Click here to obtain the latest trial key and learn how to use SIDCHG.

4. When the system displays a message asking you whether to continue, press y.

5. Log in to the ECS again.

6. After the ECS is restarted, run the cmd command to open the CLI and run whoami /user to verify that the SID has been changed.
8 OS Management

8.1 Changing OSs

8.1.1 Are OSs Charged?

The Linux and Windows OSs provided by the public cloud are free of charge.

8.1.2 Does OS Changing Incur Fees?

No. The OS changing on the public cloud is free of charge. After the OS changing, the system will re-charge you according to your select product.

8.1.3 Can I Install or Upgrade the OS by Myself?

ECSs must use the provided OSs or the OSs developed based on the provided OSs. You can patch the OS but you are not allowed to upgrade it or add more OSs.

**NOTE**

If you are required to upgrade the main OS version, for example, from CentOS 7.2 to CentOS 7.3, use the provided OS switchover function.

8.1.4 Can the OS of an ECS Be Changed?

Yes. An ECS OS can be changed.

For instructions about how to change an ECS OS, see Changing the OS.

8.1.5 How Long Does It Take to Change an ECS OS?

Stop the ECS, click More in the Operation column, and select Change OS from the drop-down list. The process takes about 10 to 20 minutes.

During this process, the ECS is in Changing OS state.
8.2 Reinstalling OSs

8.2.1 Does OS Reinstallation Incur Fees?

Reinstalling an OS for an ECS allows you to use the original image to reinstall the ECS and does not incur fees.

8.2.2 Can I Select Another OS During ECS OS Reinstallation?

No. You can use only the original image of the ECS to reinstall the OS. To use a new system image, see Changing the OS.

8.2.3 How Long Does It Take to Reinstall an ECS OS?

Stop the ECS, click More in the Operation column, and select Reinstall OS in the drop-down list. The process takes about 5 to 7 minutes.

During this process, the ECS is in Reinstalling OS state.

8.3 GUI Installation FAQs

8.3.1 Do ECSs Support GUI?

Windows ECSs are managed through a GUI but Linux ECSs are managed through the CLI. You can configure a GUI if required.
8.3.2 How Can I Install GUI on an ECS Running CentOS 6?

Scenarios
The ECSs running CentOS 6 series do not have GUI installed by default. If GUI is required, perform the operations described in this section to install it.

Procedure
1. Run the following command to obtain the installation component provided by the OS:
   
   `# yum groupinstall "Desktop"

2. Run the following command to set the default startup level to 5 (GUI):
   
   `# sed -i 's/id:3:initdefault:/id:5:initdefault:/' /etc/inittab`

3. Access GUI and run the following command:
   
   `# startx`

8.3.3 How Can I Install GUI on an ECS Running CentOS 7 or EulerOS?

Scenarios
- This document applies to CentOS 7 series as well as EulerOS 2.2 and earlier versions.
- EulerOS 2.3 and later versions do not support GUI.
- The ECSs created using a CentOS 7 public image do not have GUI installed by default. If GUI is required, perform the operations described in this section to install it.

Constraints
To ensure proper system running, ensure that the idle system memory is at least 2 GB.

Procedure
1. Run the following command to install the GUI desktop component:
   
   `# yum groupinstall "Server with GUI"

2. After the installation is complete, run the following command to set the default startup level to `graphical.target`
   
   `# systemctl set-default graphical.target`

3. Run the following command to start `graphical.target`
   
   `# systemctl start graphical.target`

4. Set the language, time zone, username, and password as prompted.

8.3.4 How Can I Install GUI on an ECS Running Ubuntu?

Scenarios
The ECSs running Ubuntu series do not have GUI installed by default. If GUI is required, perform the operations described in this section to install it.
Constraints

- The operations described in this section apply to ECSs running Ubuntu 14 or 16 only.
- The target ECS must have an EIP bound or have an intranet image source configured.

Procedure

1. Log into the ECS and install the GUI desktop component.
   a. Run the following command to update the software library:
      ```bash
      # apt-get update
      ```
   b. Run the following command to install the Ubuntu GUI desktop component:
      ```bash
      # apt-get install ubuntu-desktop
      ```
      During the installation process, you are required to manually confirm the operation twice. Press y.

2. Enable GUI.
   After the ECS is restarted, the GUI remote desktop can be used. Only the guest account can be used for remote logins, and it does not require a login password.
   To allow other users to log in to the ECS, go to step 3, in which user root is used as an example.

3. Set remote logins as user root. (The following operations also apply to other users.)
   a. Run the following command to modify the 50-ubuntu.conf configuration file:
      ```bash
      # vi /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf
      ```
      The modified data is as follows:
      ```plaintext
      [Seat:*]
      user-session=ubuntu
      greeter-show-manual-login=true
      allow-guest=false
      ```
   b. Run the following command to edit the root/.profile file:
      ```bash
      # vi /root/.profile
      ```
      Change `mesg n || true` at the end of the file to `tty -s && mesg n || true`.
      The modified file data is as follows:
      ```bash
      # ~/.profile: executed by Bourne-compatible login shells.
      if [ "BASH" ]; then
        if [ -f ~/.bashrc ]; then
          . ~/.bashrc
        fi
      fi
      tty -s && mesg n || true
      ```
   c. Restart the ECS. Then, you can log in to the GUI as user root.

---

**NOTICE**

The following operations can only be performed by user root. Use a remote login tool, such as PuTTY.

   a. Run the following command to modify the 50-ubuntu.conf configuration file:
      ```bash
      # vi /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf
      ```
      The modified data is as follows:
      ```plaintext
      [Seat:*]
      user-session=ubuntu
      greeter-show-manual-login=true
      allow-guest=false
      ```
   b. Run the following command to edit the root/.profile file:
      ```bash
      # vi /root/.profile
      ```
      Change `mesg n || true` at the end of the file to `tty -s && mesg n || true`. The modified file data is as follows:
      ```bash
      # ~/.profile: executed by Bourne-compatible login shells.
      if [ "BASH" ]; then
        if [ -f ~/.bashrc ]; then
          . ~/.bashrc
        fi
      fi
      tty -s && mesg n || true
      ```
   c. Restart the ECS. Then, you can log in to the GUI as user root.
8.4 OS Faults

8.4.1 How Can I Upgrade the Kernel of a Linux ECS?

Upgrade Notes

If tools have been installed on the Linux ECS, you must uninstall the tools before upgrading the ECS kernel. Otherwise, the following issues may occur after the kernel is upgraded:

- The Linux ECS cannot identify the NIC, leading to network access failure.
- The Linux ECS cannot identify data disks. As a result, starting system mount points fails, and the ECS cannot start.

Background

PVOPS is the Xen driver delivered with Linux distributions.

Procedure

1. Log in to the ECS.
2. Check whether the Tools have been installed on the Linux ECS, taking the SUSE Linux Enterprise Server 11 SP1 as an example.
   a. Run the following command on any directory to view the ECS driver:

   
   ```bash
   lsmod | grep xen
   ```

   Figure 8-3 Viewing the ECS driver

   ```
   [linux-7.0.8-desktop #] lsmod | grep xen
   xen_vbd 23692 3
cdrom 40507 2 sr_mod,xen_vbd
   xen_vmdq 4295 0
   xen_vnif 30374 0
   xen_balloon 14025 1 xen_vnif
   xen_hcall 1867 0
   xen_platform_pci 94654 5 xen_vbd,xen_vmdq,xen_vnif,xen_balloon,xen_hcall,[permanent]
   ```

   b. Run the following command to view the driver path, taking a disk driver as an example:

   ```bash
   modinfo xen_vbd
   ```

   Figure 8-4 Viewing the driver path

   ```
   [linux-7.0.8-desktop #] modinfo xen_vbd
   filename: /lib/modules/2.6.32.12-0.7-default/updates/pvdriver/xen_vbd/xen_vbd.ko
   license: Dual BSD/GPL
   alias: xen_vbd
   architecture: x86_64
   dependencies: xen-platform-pci,cadmum
   vefmagic: 2.6.32.12-0.7-default SMP mod_unload modversions
   ```

   c. Check whether `pvdriver` is contained in the driver path.
      - If so, the tools have been installed in the ECS. Then, go to step 3.
      - If no, go to step 4.

3. Uninstall the tools.
a. Run the following command to switch to user root:

```
su root
```

b. Run the following command to uninstall Tools in the root directory:

```
/ect/.uvp-monitor/uninstall
```

**NOTE**

After Tools is uninstalled, ECS monitoring metrics may be lost and monitoring data cannot be collected. To resolve this issue, you can compile and install the UVP Tools. For details, see https://github.com/UVP-Tools/UVP-Tools/.

4. Upgrade the kernel using the method determined by yourself.

5. Check whether the Linux ECS driver supports PVOPS. Use any one of the following methods:
   - Method 1:
     Determine based on the ECS OS.
     - All Linux distribution OSs are delivered with a Xen open-source driver, which supports PVOPS.
     - The SUSE Linux Enterprise Server 11 SP3 provided by the OS competence center is not delivered with any Xen open-source driver and does not support PVOPS.
   - Method 2:
     Check whether the ECS driver has a Xen driver module. If so, the ECS driver supports PVOPS. To obtain the data, run the following command in any directory:

     ```
     lsmod | grep xen
     ```

   **Figure 8-5** Viewing the ECS driver

   ```
   [root@localhost ~]# lsmod | grep xen
   xen_vif        59585  0 [permanent]
   xen_vbd        50857  0
   xen_balloon    45641  1 xen_vif,[permanent]
   xen_platform_pci 118125  3 xen_vif,xen_vbd,xen_balloon,[permanent]
   ```

   **NOTE**

   The name of a Xen driver module varies depending on the Linux distribution OS. You only need to check whether the driver has a driver module with the **XEN** field.
   - Method 3:
     Run the `cat /boot/config* | grep -i xen` command in any directory and check whether the **XEN** field is contained in the command output. If so, the ECS driver supports PVOPS.
Figure 8-6 Viewing the XEN field

```
root@ubuntu:/home# cat /boot/config* | grep -i xen
CONFIG_XEN=y
CONFIG_XEN_DOMO=y
CONFIG_XEN_PVH=y
CONFIG_XEN_MAX_DOMAIN_MEMORY=500
CONFIG_XEN_SAVE_RESTORE=y
# CONFIG_XEN_DEBUG_FS is not set
CONFIG_XEN_PVH=y
CONFIG_PCI_XEN=y
```

6. Upgrade the kernel based on the result obtained in step 5.
   - If the Linux ECS driver supports PVOPS, go to step 8.
   - If the Linux ECS driver does not support PVOPS, go to step 7.

7. Install the open-source component xen-kmp so that the ECS driver supports PVOPS. For instructions about how to use PVOPS, see “Optimizing a Linux Private Image” in Image Management Service User Guide.

8. (Optional) Configure required parameters based on the defect list for certain Linux distribution OSs.
   To obtain the defect list, go to following URL:
   https://github.com/UVP-Tools/UVP-Tools/tree/master/docs

8.4.2 Why Cannot My ECS OS Start Properly?

1. Check the image based on which the ECS was created. If the image is a public one, this issue is not caused by private image sources.

Figure 8-7 Image type

2. Click **Apply for Server** and check whether the same ECS can be created. If not, this image may have been canceled.
3. Change the ECS OS to one that is available on the management console.

### 8.4.3 How Can I Fix the Meltdown and Spectre Security Vulnerabilities on Intel Processor Chips?

#### Symptom

On January 3, 2018 (Beijing time), severe security vulnerabilities Meltdown and Spectre were found on Intel processor chips. The details are as follows:

**Vulnerability name:** Severe chip-level vulnerabilities on Intel processor chips  
**Vulnerability IDs:** CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754  
**Severity:** High risk  
**Vulnerability description:** High-risk CPU kernel vulnerabilities Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5715 and CVE-2017-5753) exposed. Attackers can use these vulnerabilities to bypass the memory security isolation mechanism and access the core data of the OS and other programs without authorization, leading to sensitive information disclosure.

#### Impact

These vulnerabilities will not cause attacks between ECSs but may introduce attacks between:

- Applications on an ECS  
- Accounts for logging in to an ECS

If your ECSs are created using a public image, the cloud platform will automatically fix the vulnerabilities, which will not affect your services.

If your ECSs are created using a private image, determine whether to install a patch described in this section in the private image based on the impact of the vulnerabilities.

#### Background

For details about the official patches released for affected OSs, see [Security Notices](#).

#### Prerequisites

Tests have been fully verified and ECS data has been backed up.

#### Installing a Patch on Windows ECSs

**Step 1** Log in to the ECS.
Step 2  Use either of the following methods to install the patch:

- Method 1: Use Windows Update to install the patch.
  a. Open Windows Update and click **Check for Updates**.
  b. Download and install the required patch.
- Method 2: Manually download and install the patch.
  Download the official patch and install it. For details, see **Background**.

Step 3  Restart the ECS for the patch to take effect.

Step 4  Check whether the patch has been installed.

1. Check whether the ECS is running properly.
2. Check whether the requirements specified in the **Verification** column of **Background** are met.

----End

**Installing a Patch on Linux ECSs**

Step 1  Log in to the ECS.

Step 2  Check whether Tools have been installed on the ECS, taking the SUSE Linux Enterprise Server 11 SP1 as an example.

1. Run the following command on any directory to view the ECS driver:
   ```bash
   lsmod | grep xen
   
   **Figure 8-9** Viewing the ECS driver
   ```

2. Run the following command to view the driver path, taking a disk driver as an example:
   ```bash
   modinfo xen_vbd
   
   **Figure 8-10** Viewing the driver path
   ```

3. Check whether **pvdriver** is contained in the driver path.
   - If so, Tools have been installed in the ECS. Then, go to **Step 3**.
   - If no, go to **Step 4**.

Step 3  Uninstall Tools.
1. Run the following command to switch to user root:
   `su root`

2. Run the following command to uninstall Tools in the root directory:
   `/etc/uvp-monitor/uninstall`

3. Run the following command to restart the ECS:
   `reboot`

**Step 4** Install the patch to upgrade the kernel. For details, see Background.

☐ NOTE
After updating the kernel, run the `reboot` command to restart the ECS.

**Step 5** Check whether the patch has been installed.

1. Check whether the ECS is running properly.
2. Check whether the requirements specified in the Verification column of Background are met.

☐ NOTE
After the patch is installed, the driver delivered with the OS is used on the ECS. In this event, the memory usage and disk usage of Linux ECSs will not be monitored. The other features and functions are not affected. If the memory usage and disk usage must be monitored, contact customer service.

----End

**Checking Whether Security Vulnerabilities Have Been Fixed on Linux**

1. Click `spectre-meltdown-checker` to obtain `spectre-meltdown-checker.sh`.
2. Upload the script to the ECS.
3. Run the following commands on the ECS and check whether the Meltdown or Spectre vulnerability has been fixed based on the script prompt:
   ```
   chmod +x spectre-meltdown-checker.sh
   sudo bash spectre-meltdown-checker.sh
   ```
   Figure 8-11 shows the command output.

**Figure 8-11** Command output after the script is executed

```
```

**OK** indicates that the vulnerability has been fixed, and **KO** indicates that the vulnerability has not been fixed. The information shown in Figure 8-11 indicates that the CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754 vulnerabilities have been fixed.

**Enabling or Disabling the Security Vulnerability Patch on Linux**

CPU speculative execution optimizes performance. Therefore, fixing the Meltdown or Spectre vulnerability may deteriorate performance under specific workloads.

If the impact on the system performance is unacceptable or a better protection solution is available, you can disable certain or all security protection policies.
Determine the optimal security policy based on application scenarios:

- **Meltdown vulnerability**
  Page Table Isolation (PTI) takes effect on the kernel. This function is suitable for CVE-2017-5754.

- **Spectre vulnerability**
  Indirect Branch Restricted Speculation (IBRS) takes effect on specified registers (MSR) in SPEC_CTRL model. Working with retpoline, IBRS controls Indirect Branch Prediction Barriers (IBPBs) on specified registers (MSR) in PRED_CMD model. This function is suitable for CVE-2017-5715.

☐ **NOTE**

The CVE-2017-5753 vulnerability is fixed by a kernel patch and cannot be disabled. No obvious impact was detected for the patch in Red Hat performance tests.

- **Disabling the Meltdown Vulnerability Patch**
  To prevent the enabling of PTI from deteriorating the system performance, or a better protection solution is available, perform the following operations to disable the patch:
  a. Modify kernel parameters based on OSs:
     - CentOS, EulerOS, Ubuntu, Fedora, and Red Hat: Add the kernel parameter `nopti`.
     - Debian and OpenSUSE: Add the kernel parameter `pti=off`.
  b. Restart the ECS.

- **Disabling the Spectre Vulnerability Patch**
  To prevent the Spectre vulnerability fixing from deteriorating the system performance, or a better protection solution is available, perform the following operations to disable the patch:
  a. Modify kernel parameters based on OSs:
     - CentOS, EulerOS, Fedora, Debian, Red Hat, and OpenSUSE: Add the kernel parameter `spectre_v2=off`.
     - Ubuntu: Add the kernel parameter `nospectre_v2=off`.
  b. Restart the ECS.

If you are using one of the following OSs, visit their official website for more details.

Red Hat: [https://access.redhat.com/articles/3311301?spm=a2c4g.11186623.2.20.42b49d4aJuKYx2](https://access.redhat.com/articles/3311301?spm=a2c4g.11186623.2.20.42b49d4aJuKYx2)

SUSE: [https://www.suse.com/support/kb/doc/?spm=a2c4g.11186623.2.21.42b49d4avOXw7d&id=7022512](https://www.suse.com/support/kb/doc/?spm=a2c4g.11186623.2.21.42b49d4avOXw7d&id=7022512)


### 8.4.4 How Can I Enable SELinux on an ECS Running CentOS?

**Symptom**

SELinux is disabled on ECSs running CentOS 7.5 by default. After I enable SELinux by running `/etc/selinux/config` and enter the login password, the login failed.

This section describes how to resolve this issue based on enabled SELinux.
Solution

The operations described in this section are performed on ECSs running CentOS 7.5.

1. Run the following command to change `SELINUX=disabled` in the SELinux configuration file to `SELINUX=enforcing`:
   ```
   vim /etc/selinux/config
   ```

2. Run the following command to automatically enable SELINUX on the file system upon ECS restarting:
   ```
   touch /.autorelabel
   ```

3. Run the following command to restart the ECS to make the configuration take effect:
   ```
   reboot
   ```

**NOTE**

After the preceding command is executed, the system automatically restarts twice.

**8.4.5 What Should I Do If the Forcibly Stopped Linux ECS Fails to Start Due to File System Damage?**

**Symptom**

After a Linux ECS is forcibly stopped, there is a low probability that the file system is damaged. As a result, the ECS fails to be restarted.

**Figure 8-12 Failure to start an ECS**
Possible Causes

As shown in Figure 8-12, the ECS cannot be started because the file system is damaged. Forcibly stopping or restarting an ECS is highly risky because this operation may cause inconsistent metadata of the file system, leading to the file system damage.

Solution

Use the disk repair tool (fsck) delivered with the Linux OS to rectify the fault.

The following uses Figure 8-12 as an example, in which the affected disk partition is /dev/xvdb1.

1. Enter user root password as prompted.
2. Run the following command to check whether the affected disk partition has been mounted:
   
   `mount | grep xvdb1`
   
   - If yes, go to step 3.
   - If no, go to 4.

3. Run the following command to unmount the affected disk partition:
   
   `umount /dev/xvdb1`

4. Run the following command to rectify the fault for the file system of the affected disk partition:
   
   `fsck -y /dev/xvdb1`

5. Run the following command to restart the ECS to make the configuration take effect:
   
   `reboot`

☐ NOTE

If the fault persists, contact the customer service personnel for technical support.
9 File Uploading

9.1 Does an ECS Support FTP-based Uploading by Default?

No. To support FTP-based uploading, you are required to install and configure FTP.

9.2 How Can I Upload a File to a Windows ECS?

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

Prerequisites

The Windows ECS can access the Internet.

Solution

1. On the local Windows computer, click Start. In the Search programs and files text box, enter mstsc.
   
   The Remote Desktop Connection window is displayed.

2. Click Options.
3. On the **General** tab, enter the EIP bound to the ECS and username **Administrator** for logging in to the ECS.

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

6. In the Drives pane, select the local disk where the file to be uploaded to the Windows ECS is located.
7. Click **OK** and log in to the Windows ECS.
8. Choose **Start > Computer**.
   The local disk is displayed on the Windows ECS.
9. Double-click the local disk to access it and copy the file to be uploaded to the Windows ECS.

### 9.3 How Can I Transfer Data Between a Local Host and a Windows ECS?

#### Method 1: Install a Data Transfer Tool

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

#### Method 2: Configure Local Disk Mapping

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

1. Log in to the local host.
2. Press **Win+R** to open the **Open** text box.
3. Enter **mstsc** to start the remote desktop connection.
4. In the **Remote Desktop Connection** window, click 🎯 in the lower left corner.
5. Click the **Local Resources** tab and then **More** in the **Local devices and resources** pane.
6. Select Drives and Other supported Plug and Play (PnP) devices and click OK to map all disks on the local host to the Windows ECS.
   If only certain disks on the local host need to be mapped to the Windows ECS, expand Drives and select the desired ones.
7. Open the Remote Desktop Connection window again and enter the EIP bound to the Windows ECS in the Computer text box.

Figure 9-4 Connecting a remote desktop to the Windows ECS

8. Click Connect.
   Log in to the Windows ECS.

9. Check the disks of the Windows ECS. If the disk information of the local host is displayed, data can be transmitted between your local host and the Windows ECS.
Method 3: Use a Shared Folder

1. Log in to the ECS.
2. Create a folder, for example, test on the ECS.
3. Right-click the folder and choose Properties from the shortcut menu.
4. Click the Sharing tab and click Share.
5. Add target users for data sharing as prompted and set Permission Level for the users.
   You can add multiple users to share the folder with them. Alternatively, you can expand the drop-down list and select Everyone to share the folder with any user.
6. Click Share.
   The system displays a message, indicating that the test folder is shared with the added users.
7. In the displayed dialog box, copy the path in which the shared folder is stored and click Done.
   Close the dialog box.
8. On the local host, press Win+R to open the Run dialog box.
9. Paste the path copied in step 7 and click OK.
   The shared folder is opened. Then, you can copy the data in the shared folder to the local host.

9.4 How Can I Use WinSCP to Upload a File to a Linux ECS?

WinSCP is generally used to upload files to Linux ECSs. This section describes how to upload a file from a local Windows computer to a Linux ECS using WinSCP.
The operations described in this section are performed in CentOS 7.2 as an example.

**Prerequisites**

The Linux ECS can access the Internet.

**Solution**

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

![WinSCP interface](image)

Set parameters as follows:

- **File protocol**: Either SFTP or SCP will do.
- **Host name**: Enter the EIP bound to the ECS. Log in to the management console to obtain the EIP.
- **Port number**: 22 by default.
- **User name**: Enter the username for logging in to the ECS.
  - If the ECS is logged in using an SSH key pair,
    - The username is **core** for a CoreOS public image.
    - The username is **root** for a non-CoreOS public image.
  - If the ECS is logged in using a password, the username is **root** for a public image.
- **Password**: the password set when you purchased the ECS or converted using a key.

4. Click **Login**.
5. After the login, drag a file from the local computer on the left to the remotely logged in ECS on the right for uploading.
9.5 What Should I Do If the Connection Between the Client and the Server Times Out When I Upload a File Using FTP?

Symptom
When I attempted to access the server from the client to upload a file using FTP, the connection timed out.

Constraints
The operations described in this section apply to FTP on Windows ECSs only.

Possible Causes
Data is intercepted by the firewall or security group on the server.

Solution
1. Check the firewall settings on the server.
2. Disable the firewall or add desired rules to the security group.

9.6 What Should I Do If Writing Data Failed When I Upload a File Using FTP?

Symptom
When I attempted to upload a file using FTP, writing data failed. As a result, the file transfer failed.

Constraints
The operations described in this section apply to FTP on Windows ECSs only.

Possible Causes
When NA T is enabled on the FTP server, the FTP client must connect to the FTP server in passive mode. In such a case, the public IP address (EIP) of the server cannot be accessed from the router. Therefore, you need to add the EIP to the public IP address list on the server. Additionally, set the port range to limit the number of ports with data forwarded by the router.

Solution
The public IP address must be associated with the private IP address using NAT. Therefore, the server must be configured accordingly.
1. Configure the public IP address of the server.
   Choose Edit > Settings.
2. Choose **Passive mode settings**, set the port range (for example, 50000-50100) for transmitting data, and enter the target public IP address.

3. Click **OK**.

4. Allow traffic on TCP ports 50000-50100 and 21 in the security group in the inbound direction.

5. Test the connection on the client.

**9.7 What Should I Do If an ECS with FTP Deployed Cannot Be Accessed Through Internet?**

**Symptom**

- A Windows ECS with FTP deployed cannot be accessed using an EIP.
- The FTP client cannot access the FTP server, and the connection timed out.
- Uploading a file is slow.
Possible Causes

- The security group to which the target ECS is added blocks external network connections.
- The firewall of the ECS blocks the FTP process.

Enabling FTP Firewall Support

To allow a HUAWEI CLOUD server to access the FTP server deployed on an ECS using a public IP address (EIP), the FTP server must work in passive mode. In such a case, enable FTP firewall support.

1. Double-click FTP Firewall Support.

2. Set parameters and click Apply.
   - **Data Channel Port Range**: specifies the range of ports used for passive connections. The port range is 1025-65535. Configure this parameter based on site requirements.
   - **External IP Address of Firewall**: Enter the public IP address of the ECS.
Setting the Security Group and Firewall

After deploying FTP, add a rule to the target security group to allow access to the FTP port in the inbound direction.

After enabling FTP firewall support, allow access to the ports used by the FTP site and the data channel ports used by the FTP firewall in the security group.

By default, the firewall allows access to TCP port 21 for FTP. If another port is used, add an inbound rule that allows access to that port on the firewall.

1. Log in to the management console.
2. Click in the upper left corner and select 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. Click the security group ID.
   The system automatically switches to the Security Group page.
7. On the Inbound Rules tab, click Add Rule and configure the access rule for the inbound direction.
   Set Source to the IP address segment containing the IP addresses allowed to access the ECS over the Internet.

   The valid port range that can be specified in Enabling FTP Firewall Support is 1025-65535. For example, the configured data port range is 5000-6000.

   ![Add Inbound Rule](image)

   □ NOTE
   The default source IP address 0.0.0.0/0 indicates that all IP addresses can access ECSs in the security group.
10.1 Can I Transfer ECS Ownership Between Accounts?

No. This function is not supported.
11 Image Source Management

11.1 How Can I Use the Automated Tool to Configure an HUAWEI CLOUD Image Source (x86_64)?

Scenarios

When updating the OS or software of an ECS, you can access the ECS to the Internet and use an external image source. However, if your ECS cannot access the Internet, or the external image source cannot provide services stably, you can use the one-click script configuration function provided by HUAWEI CLOUD to configure and update the image source.

Constraints

- Make sure that the intranet DNS server provided by HUAWEI CLOUD has been configured. For instructions about how to obtain an intranet DNS server, see What Are the Private DNS Server Addresses Provided by the DNS Service?
- The operations described in this section apply to ECSs deployed on x86_64 servers.
- The operations described in this section apply to ECSs deployed on x86_64 servers.
- Only the following OSs are supported: EulerOS, CentOS, Debian, Ubuntu, and openSUSE.

Procedure

1. Log in to the ECS.
2. Run the following command to configure the image source with a few clicks:

```
wget http://mirrors.myhuaweicloud.com/repo/mirrors_source.sh && sh mirrors_source.sh
```

NOTE

If executing the command failed, manually configure the image source by following the instructions provided in the configuration guide for other HUAWEI CLOUD image sources or contact customer service.
11.2 How Can I Use an openSUSE Image Source (x86_64) Provided by HUAWEI CLOUD?

Scenarios

When updating the OS or software of an ECS, you can access the ECS to the Internet and use an external openSUSE image source. However, if your ECS cannot access the Internet, or the external openSUSE image source cannot provide services stably, you can use the openSUSE image source provided by HUAWEI CLOUD.

Constraints

- Make sure that the intranet DNS server provided by HUAWEI CLOUD has been configured. For instructions about how to obtain an intranet DNS server, see What Are the Private DNS Server Addresses Provided by the DNS Service?
- The operations described in this section apply to ECSs deployed on x86_64 servers.
- The operations described in this section apply to ECSs deployed on x86_64 servers.
- HUAWEI CLOUD does not provide the image source of the SUSE Linux Enterprise Server (SLES) enterprise edition.

Procedure

1. Log in to the ECS.
2. Run the following commands to back up the .repo file:
   ```
   mkdir /etc/zypp/repos.d/repo_bak
   mv /etc/zypp/repos.d/*.repo /etc/zypp/repos.d/repo_bak/
   ```
3. Run the command listed in Table 11-1 to configure the zypper source for the target OpenSUSE version.

Table 11-1 Configuring the zypper source

<table>
<thead>
<tr>
<th>Version</th>
<th>Command</th>
</tr>
</thead>
</table>
| OpenSUSE 13.2 | `zypper addrepo -f cg
`zypper addrepo -f cg
`zypper addrepo -f cg
`zypper addrepo -f cg
| OpenSUSE 42.2 | `sudo zypper ar -f cg
http://mirrors.myhuaweicloud.com/opensuse/distribution/leap/42.2/repo/oss HWCloud:42.2:OSS`
`sudo zypper ar -f cg` |
## 11.3 How Can I Use a CentOS Image Source (x86_64) Provided by HUAWEI CLOUD?

### Scenarios

When updating the OS or software of an ECS, you can access the ECS to the Internet and use an external CentOS image source. However, if your ECS cannot access the Internet, or the external CentOS image source cannot provide services stably, you can use the CentOS image source provided by HUAWEI CLOUD.

### Constraints

- Make sure that the intranet DNS server provided by HUAWEI CLOUD has been configured. For instructions about how to obtain an intranet DNS server, see What Are the Private DNS Server Addresses Provided by the DNS Service?
- The operations described in this section apply to ECSs deployed on x86_64 servers.

### Procedure

1. Log in to the ECS as user root.
2. Run the following command to back up the CentOS-Base.repo file:
   ```bash
   mkdir -p /etc/yum.repos.d/repo_bak/
   mv /etc/yum.repos.d/*_repo /etc/yum.repos.d/repo_bak/
   ```
3. Select a suitable curl command according to the CentOS image source version, run the command to download the CentOS-Base.repo file, and save the file into `/etc/yum.repos.d/`:
   ```bash
   curl -o /etc/yum.repos.d/CentOS-Base.repo
   http://mirrors.myhuaweicloud.com/repo/CentOS-Base-6.repo
   ``
curl -o /etc/yum.repos.d/CentOS-Base.repo
http://mirrors.myhuaweicloud.com/repo/CentOS-Base-7.repo

4. Run the following command to generate a cache:

   `yum makecache`

   **NOTE**
   - After the command is executed, if the system displays the message "Another app is currently holding the yum lock", run the `rm -rf /var/run/yum.pid` command to delete the `yum.pid` file. Then, run the `yum makecache` command again to generate the cache.
   - If the system displays the message "Error: Cannot retrieve metalink for repository: epel. Please verify its path and try again" after you run the `yum makecache` command, you must run the `yum --disablerepo=epel -y update ca-certificates` command to update the certificate for temporarily disabling the epel source.

### 11.4 How Can I Use a Ubuntu Image Source (x86_64) Provided by HUAWEI CLOUD?

#### Scenarios

When you are required to update the OS or software of an ECS, you can access the ECS to the Internet and use an external Ubuntu image source. However, if your ECS cannot access the Internet, or the external Ubuntu image source cannot provide services stably, you can use the Ubuntu image source provided by HUAWEI CLOUD.

#### Constraints

- Make sure that the intranet DNS server provided by HUAWEI CLOUD has been configured. For instructions about how to obtain an intranet DNS server, see [What Are the Private DNS Server Addresses Provided by the DNS Service?](#)
- The operations described in this section apply to ECSs deployed on x86_64 servers.
- The operations described in this section apply to ECSs deployed on x86_64 servers.

#### Procedure

1. Log in to the ECS.
2. Run the following command to back up the `sources.list` file:

   ```
   mv /etc/apt/sources.list /etc/apt/sources.list.bak
   ```

3. Select a suitable `wget` command according to the Ubuntu image source version, run the command to download the `sources.list` file, and save the file into `/etc/apt/`:

   ```
   Table 11-2 lists the mapping between Ubuntu versions and version names.
   ```

<table>
<thead>
<tr>
<th>Version</th>
<th>Version Name</th>
<th>apt Source Configuration File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu 18.04</td>
<td>(Bionic Beaver)</td>
<td>sources.list.bionic</td>
</tr>
<tr>
<td>Ubuntu 17.10</td>
<td>(Artful Aardvark)</td>
<td>sources.list.artful</td>
</tr>
<tr>
<td>Ubuntu 17.04</td>
<td>(Zesty Zapus)</td>
<td>sources.list.zesty</td>
</tr>
</tbody>
</table>
### Version Name and apt Source Configuration File

<table>
<thead>
<tr>
<th>Version</th>
<th>Version Name</th>
<th>apt Source Configuration File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu 16.10</td>
<td>(YakketyYak)</td>
<td>sources.list.yakkety</td>
</tr>
<tr>
<td>Ubuntu 16.04 LTS</td>
<td>(Xenial Xerus)</td>
<td>sources.list.xenial</td>
</tr>
<tr>
<td>Ubuntu 14.04 LTS</td>
<td>(Trusty Tahr)</td>
<td>sources.list.trusty</td>
</tr>
<tr>
<td>Ubuntu 12.04 LTS</td>
<td>(Precise Pangolin)</td>
<td>sources.list.precise</td>
</tr>
</tbody>
</table>

Take Ubuntu 14.04 as an example. Its apt source configuration file is `sources.list.trusty`. The configurations are as follows:

```
wget -O /etc/apt/sources.list http://mirrors.myhuaweicloud.com/repo/sources.list.trusty
```

4. Run the following command to update the software library:

```
apt-get update
```

## 11.5 How Can I Use a EulerOS Image Source (x86_64 or ARM) Provided by HUAWEI CLOUD?

### Scenarios

When updating the OS or software of an ECS, you can access the ECS to the Internet and use an external EulerOS image source. However, if your ECS cannot access the Internet, or the external EulerOS image source cannot provide services stably, you can use the EulerOS image source provided by HUAWEI CLOUD.

### Constraints

- Make sure that the intranet DNS server provided by HUAWEI CLOUD has been configured. For instructions about how to obtain an intranet DNS server, see What Are the Private DNS Server Addresses Provided by the DNS Service?
- The operations described in this section apply to ECSs deployed on x86_64 servers.
- The operations described in this section apply to ECSs deployed on x86_64 or ARM (Huawei Kunpeng) servers.

### Procedure

1. Log in to the ECS.
2. Run the following commands to back up the Euler repo file:
   ```
   mkdir -p /etc/yum.repos.d/repo_bak/
   mv /etc/yum.repos.d/*_repo /etc/yum.repos.d/repo_bak/
   ```
3. Select a suitable curl command to download the `Euler-Base.repo` file of the desired version and save the file into `/etc/yum.repos.d/`:
   - x86_64 (only EulerOS 2.2 is supported)
     ```
     curl -o /etc/yum.repos.d/EulerOS-base.repo http://mirrors.myhuaweicloud.com/repo/EulerOS_2_x_base.repo
     ```
For example, if EulerOS 2.2 is used, change x in `EulerOS_2_x_base.repo` to 2 in the following command:

```
curl -o /etc/yum.repos.d/EulerOS-base.repo http://mirrors.myhuaweicloud.com/repo/EulerOS_2_2_base.repo
```

ARM (only EulerOS 2.8 is supported)

```
curl -o /etc/yum.repos.d/EulerOS-base.repo http://mirrors.myhuaweicloud.com/repo/EulerOS_2_8_base.repo
```

4. Run the following command to generate a cache:

```
yum makecache
```

⚠️ NOTE

After the command is executed, if the system displays the message "Another app is currently holding the yum lock", run the `rm -rf /var/run/yum.pid` command to delete the `yum.pid` file. Then, run the `yum makecache` command again to generate the cache.
12 Disk Management

12.1 Disk Partitions and Virtual Memory

12.1.1 How Can I Adjust System Disk Partitions?

Scenarios

If the capacity of system disk partitions is inconsistent with the actual system disk capacity after an ECS is created, you can manually adjust the partitions to expand the system disk.

There are two ways to expand a system disk:

- Take the empty partition as a new partition and attach this partition to a directory in the root partition after formatting it. You can perform the operations in this section.
- Add the empty partition to the root partition to be expanded. For detailed operations, see the following:
  - How can I add the empty partition of a system disk to be expanded to the end root partition online?
  - How can I add the empty partition of a system disk to be expanded to the non-end root partition online?

Procedure

Take an ECS running CentOS 7.3 64bit as an example. The system disk capacity is 60 GB when the ECS is created. However, the capacity of system disk partitions is only 40 GB.

To use the 20 GB capacity, performing the following operations to adjust system disk partitions:

Step 1  View disk partitions.

1. Log in to the ECS as user root.
2. Run the following command to view details about the ECS disk:
   
   `fdisk -l`

   In the following command output, `/dev/xvda` or `/dev/vda` indicates the system disk.
Step 2  Create a partition for the expanded system disk capacity.

1. Run the following command to switch to the fdisk mode (taking /dev/xvda as an example):

   \texttt{fdisk /dev/xvda}

   Information similar to the following is displayed:

   \begin{verbatim}
   [root@ecs-8d6c ]# fdisk /dev/xvda
   Welcome to fdisk (util-linux 2.23.2).
   Changes will remain in memory only, until you decide to write them.
   Be careful before using the write command.

   Command (m for help):
   \end{verbatim}

2. Enter \texttt{n} and press \texttt{Enter} to create a new partition.

   Because the system disk has two existing partitions, the system automatically creates the third one.

   Information similar to the following is displayed:

   \begin{verbatim}
   1 1049MB 41.0GB 40.9GB primary ext4 boot
   2 41.0GB 42.9GB 2000MB primary linux-swap(v1)
   \end{verbatim}
3. Enter the new partition's start cylinder number and press **Enter**.

The start cylinder number must be greater than the end cylinder numbers of existing partitions. In this example, use the default value for the new partition's start cylinder number and press **Enter**. Information similar to the following is displayed.

```
First sector (03006808-125829119, default 03006808):
Using default value 03006808
Last sector, +sectors or +size(K,M,G) (03006808-125829119, default 125829119):
Using default value 125829119
Partition 3 of type Linux and of size 20 GiB is set
```

4. Enter the new partition's end cylinder number and press **Enter**.

In this example, use the default value for the new partition's end cylinder number and press **Enter**. Information similar to the following is displayed.

```
Last sector, +sectors or +size(K,M,G) (03006808-125829119, default 125829119):
Using default value 125829119
Partition 3 of type Linux and of size 20 GiB is set
```

5. Enter **p** and press **Enter** to view the created partition.

Information similar to the following is displayed.

```
Command (m for help): p
Disk /dev/xvda: 64.4 GB, 64424509440 bytes, 125829120 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
LBA size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 8d6d0d86e5

Device Boot Start   End   Blocks  Id  System
/dev/xvda1   2048  7999543  39999246  03  Linux
/dev/xvda2  7999544  83886879 19527688  82  Linux swap / Solaris
/dev/xvda3  83886880 125829119 20971520  03  Linux
```

6. Enter **w** and press **Enter**. The system saves and exits the partition.

The system automatically writes the partition result into the partition list. Then, the partition is created.

Information similar to the following is displayed.

```
The system automatically writes the partition result into the partition list. Then, the partition is created.
Command (m for help): w
The partition table has been altered!
Calling ioctl() to re-read partition table.
```

```
WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at the next reboot or if you run partprobe(8) or kpartx(8)
Syncing disks.
```

```
Root Docs: Edle: ~ # fdisk /dev/xvda1
Welcome to fdisk (util-linux 2.23.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): n
Partition type:
  p  primary (2 primary, 0 extended, 2 free)
  e  extended
Select (default p): e
Using default response e
Partition number (2,4, default 3): 3
First sector (03006808-125829119, default 03006808):
Using default value 03006808
Last sector, +sectors or +size(K,M,G) (03006808-125829119, default 125829119):
Using default value 125829119
Partition 3 of type Linux and of size 20 GiB is set
```

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

```
WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

```
Root Docs: Edle: ~ # fdisk /dev/xvda
Welcome to fdisk (util-linux 2.23.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): n
Partition type:
  p  primary (2 primary, 0 extended, 2 free)
  e  extended
Select (default p): e
Using default response e
Partition number (2,4, default 3): 3
First sector (03006808-125829119, default 03006808):
Using default value 03006808
Last sector, +sectors or +size(K,M,G) (03006808-125829119, default 125829119):
Using default value 125829119
Partition 3 of type Linux and of size 20 GiB is set
```
7. Run the following command to view disk partitions:

```
parted -l /dev/xvda
```

### Step 3
Run the following command to synchronize the modifications in the partition list with the OS:

```
partprobe
```

### Step 4
Configure the type of the new partition file system.

1. Run the following command to view the type of the file system:

```
df -TH
```

### Information similar to the following is displayed:

```
[root@ecs-86dc ~]# df -TH
Filesystem  Type  Size  Used  Avail  Use%  Mounted on
/dev/xvda1  ext4  41G   1.3G  37G   3%   /
devtmpfs  devtmpfs  943M   0  943M   0%  /dev
tmpfs  tmpfs  952M   0  952M   0%  /dev/shm
tmpfs  tmpfs  952M  0.0M  952M   0%  /run
tmpfs  tmpfs  191M   0  191M   0%  /run/user/0
```

2. Run the following command to format the partition (taking the **ext4** type as an example):

```
mkfs -t ext4 /dev/xvda3
```

### NOTE
Formatting the partition requires a period of time. During this time, observe the system running status and do not exit the system.

```
[root@ecs-86dc ~]# mkfs -t ext4 /dev/xvda3
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
1790544 inodes, 7156992 blocks
357849 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2155872256
219 block groups
32768 blocks per group, 32768 fragments per group
8176 inodes per group
Superblock backups stored on blocks:
```

Elastic Cloud Server
FAQs
12 Disk Management

2019-12-02
Step 5 Mount the new partition to the target directory.

If the new partition is mounted to a directory that is not empty, the subdirectories and files in the directory will be hidden. Therefore, you are advised to mount the new partition to an empty directory or a newly created directory. If the new partition must be mounted to a directory that is not empty, move the subdirectories and files in the directory to another directory temporarily. After the partition is mounted, move the subdirectories and files back.

Take the newly created directory `/root/new` as an example.

1. Run the following command to create the `/root/new` directory:
   ```bash
   mkdir /root/new
   ```

2. Run the following command to mount the new partition to the `/root/new` directory:
   ```bash
   mount /dev/xvda3 /root/new
   ```

   Information similar to the following is displayed:
   ```bash
   [root@ecs-86dc ~]# mount /dev/xvda3 /root/new
   ```

3. Run the following command to view the mounted file systems:
   ```bash
   df -TH
   ```

   Information similar to the following is displayed:
   ```bash
   Filesystem     Type      Size  Used  Avail Use% Mounted on
   /dev/xvda1     ext4      41G   13G  28G  32% /dev
   devtmpfs       devtmpfs  913M   0   913M   0% /dev/shm
   tmpfs          tmpfs     952M   0   952M   0% /run
   tmpfs          tmpfs     952M 8.8M  944M   1% /run
   /dev/xvda3     ext4     220G 17M  203G  1% /root/new
   tmpfs          tmpfs    191M   0  191M   0% /run/user/8
   [root@ecs-86dc ~]#
   ```

Step 6 Determine whether to set automatic mounting upon system startup for the new disk.

If you do not set automatic mounting upon system startup, you must mount the new partition to the specified directory again after the ECS is restarted.

- If automatic mounting is required, go to Step 7.
- If automatic mounting is not required, no further action is required.

Step 7 Set automatic mounting upon system startup for the new disk.

---

**NOTICE**

Do not set automatic mounting upon system startup for unformatted disks, which will cause ECS startup failures.
1. Run the following command to obtain the file system type and UUID:

```
blkid
```

According to the preceding figure, the UUID of the new partition is 96e5e028-b0fb-4547-a82a-35ace1086c4f.

2. Run the following command to open the `fstab` file using the vi editor:

```
vi /etc/fstab
```

3. Press `i` to enter editing mode.

4. Move the cursor to the end of the file and press Enter. Then add the following information:

```
UUID=96e5e028-b0fb-4547-a82a-35ace1086c4f /root/new ext4 defaults 0 0
```

5. Press `Esc`, run the following command, and press Enter. The system saves the configurations and exits the vi editor.

```
:wq
```

**NOTE**

If a new disk for which automatic mounting upon system startup has been set must be detached, you must delete the automatic mounting configuration before detaching the disk. Otherwise, starting the ECS will fail after the disk is detached. To delete the automatic mounting configuration, perform the following operations:

1. Run the following command to open the `fstab` file using the vi editor:

```
vi /etc/fstab
```

2. Press `i` to enter editing mode.

3. Delete the following statement:

```
UUID=96e5e028-b0fb-4547-a82a-35ace1086c4f /root/new ext4 defaults 0 0
```

4. Press `Esc`, run the following command, and press Enter. The system saves the configurations and exits the vi editor.

```
:wq
```

----

**12.1.2 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Windows ECS?**

This section uses an ECS running Windows Server 2008 R2 64bit as an example to describe how to obtain the mapping between disk partitions and disk devices.

1. Log in to the Windows ECS.
2. Click Start in the lower left corner of the desktop.
4. In the navigation pane on the left, choose Storage > Disk Management.
5. Taking disk 1 marked in Figure 12-1 as an example, view the disk device for disk 1.
   a. Right-click the gray area where disk 1 is located, as shown in the red box in Figure 12-1.
   b. Click Properties.
      The SCSI Disk Device Properties dialog box is displayed, as shown in Figure 12-2.
c. Click the Details tab and set Property to Parent.

Figure 12-3 Disk device details

- Record the digits following & in the parameter value, for example, 51776, which is the master and slave device number corresponding to the disk partition.
- Obtain the disk device according to the information listed in Table 12-1.
  The disk device corresponding to 51776 is xvde. The disk device used by disk 1 is xvde.
### Table 12-1 Mapping between disk partitions and disk devices

<table>
<thead>
<tr>
<th>Master and Slave Device Number for a Disk Partition</th>
<th>Disk Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>51712</td>
<td>xvda</td>
</tr>
<tr>
<td>51728</td>
<td>xvdb</td>
</tr>
<tr>
<td>51744</td>
<td>xvdc</td>
</tr>
<tr>
<td>51760</td>
<td>xvdd</td>
</tr>
<tr>
<td>51776</td>
<td>xvde</td>
</tr>
<tr>
<td>51792</td>
<td>xvdf</td>
</tr>
<tr>
<td>51808</td>
<td>xvdg</td>
</tr>
<tr>
<td>51824</td>
<td>xvdh</td>
</tr>
<tr>
<td>51840</td>
<td>xvdi</td>
</tr>
<tr>
<td>51856</td>
<td>xvdj</td>
</tr>
<tr>
<td>51872</td>
<td>xdk</td>
</tr>
<tr>
<td>51888</td>
<td>xdl</td>
</tr>
<tr>
<td>51904</td>
<td>xdm</td>
</tr>
<tr>
<td>51920</td>
<td>xdn</td>
</tr>
<tr>
<td>51936</td>
<td>xdo</td>
</tr>
<tr>
<td>51952</td>
<td>xdp</td>
</tr>
<tr>
<td>268439552</td>
<td>xdq</td>
</tr>
<tr>
<td>268439808</td>
<td>xdr</td>
</tr>
<tr>
<td>268440064</td>
<td>xds</td>
</tr>
<tr>
<td>268440320</td>
<td>xdt</td>
</tr>
<tr>
<td>268440576</td>
<td>xdu</td>
</tr>
<tr>
<td>268440832</td>
<td>xdv</td>
</tr>
<tr>
<td>268441088</td>
<td>xdw</td>
</tr>
<tr>
<td>268441344</td>
<td>xdx</td>
</tr>
</tbody>
</table>

### 12.1.3 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Linux ECS?

For a Linux ECS, its disk partitions correspond to disk devices. This section uses a Linux ECS running Red Hat Enterprise Linux 7 as an example to describe how to obtain the mapping between disk partitions and disk devices.
1. Log in to the Linux ECS as user root.

2. Right-click in the blank area of the desktop and choose Open Terminal from the shortcut menu.

3. Run the following command to view disk partitions and disk devices:

   `fdisk -l`

<table>
<thead>
<tr>
<th>Disk Partition</th>
<th>Disk Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>xvda</td>
<td>xvda</td>
</tr>
<tr>
<td>xvdb</td>
<td>xvdb</td>
</tr>
<tr>
<td>xvdc</td>
<td>xvdc</td>
</tr>
<tr>
<td>xvdd</td>
<td>xvdd</td>
</tr>
<tr>
<td>xvde</td>
<td>xvde</td>
</tr>
<tr>
<td>xvdf</td>
<td>xvdf</td>
</tr>
</tbody>
</table>

Table 12-2 lists the mapping between disk partitions and disk devices.
12.1.4 How Can I Enable Virtual Memory on a Windows ECS?

Enabling ECS virtual memory will deteriorate disk I/O performance. Therefore, the Windows ECSs provided by the platform do not have virtual memory enabled by default. If the memory size of an ECS is insufficient, you are advised to increase its memory size by modifying the ECS specifications. Perform the operations described in this section to enable virtual memory if required.

- **NOTE**
  
  If the memory usage is excessively high and the I/O performance is not as good as expected, you are not suggested to enable virtual memory. The reason is as follows: The excessively high memory usage limits the system performance improvement. Furthermore, frequent memory switching requires massive additional I/O operations, which will further deteriorate the I/O performance and the overall system performance.

The operations described in this section are provided for the ECSs running Windows Server 2008 or later.

1. Right-click **Computer** and choose **Properties** from the shortcut menu.
2. In the navigation pane on the left, choose **Advanced system settings**.
The **System Properties** dialog box is displayed.

3. Click the **Advanced** tab and then **Settings** in the **Performance** pane.

The **Performance Options** dialog box is displayed.

**Figure 12-4** Performance Options

![Performance Options dialog box]

4. Click the **Advanced** tab and then **Background Services** in the **Processor scheduling** pane.

5. Click **Change** in the **Virtual memory** pane.

The **Virtual Memory** dialog box is displayed.

6. Configure virtual memory based on service requirements.
   - **Automatically manage paging file size for all drives**: Deselect the check box.
   - **Drive**: Select the drive where the virtual memory file is stored.
     
     You are advised not to select the system disk to store the virtual memory.
   - **Custom size**: Select **Custom size** and set **Initial size** and **Maximum size**.
     
     Considering **Memory.dmp** caused by blue screen of death (BSOD), you are advised to set **Initial size** to 16 and **Maximum size** to 4096.
7. Click Set and then OK to complete the configuration.
8. Restart the ECS for the configuration to take effect.

12.1.5 Why Is the Memory of an ECS Obtained by Running the free Command Inconsistent with the Actual Memory?

**Symptom**

After an ECS is created, run the `free -m` command to view the ECS memory. The query result is less than the memory configured during ECS creation.

An example is provided as follows:

For example, you set memory to 4,194,304 KB (4096 MB) when creating the ECS. After the ECS is created, run the `free -m` command to view its memory. The command output is as follows:

```
[root@localhost ~]# free -m
           total used free shared buff/cache available
Mem: 3790 167 3474 8 147 3414
Swap: 1022 0 1022
```

The memory in the command output is 3790 MB, which is less than the configured 4096 MB.

Run the `dmidecode -t memory` command to check the actual memory configured for the ECS. The command output is as follows:
[root@localhost ~]# dmidecode -t memory
# dmidecode 3.0
Getting SMBIOS data from sysfs.
SMBIOS 2.8 present.
Handle 0x1000, DMI type 16, 23 bytes
Physical Memory Array
Location: Other
Use: System Memory
Error Correction Type: Multi-bit ECC
Maximum Capacity: 4 GB
Error Information Handle: Not Provided
Number Of Devices: 1

Handle 0x1100, DMI type 17, 40 bytes
Memory Device
Array Handle: 0x1000
Error Information Handle: Not Provided
Total Width: Unknown
Data Width: Unknown
Size: 4096 MB
Form Factor: DIMM
Set: None
Locator: DIMM 0
Bank Locator: Not Specified
Type: RAM
Type Detail: Other
Speed: Unknown
Manufacturer: QEMU
Serial Number: Not Specified
Asset Tag: Not Specified
Part Number: Not Specified
Rank: Unknown
Configured Clock Speed: Unknown
Minimum Voltage: Unknown
Maximum Voltage: Unknown
Configured Voltage: Unknown

The memory in the command output is the same as that configured during ECS creation.

**Possible Causes**

When the OS is started, related devices are initialized, which occupies memory. In addition, when the kernel is started, it also occupies memory. The memory occupied by kdump can be set. Unless otherwise specified, do not change the memory size occupied by kdump.

The command output of `free -m` shows the available memory of the ECS, and that of `dmidecode -t memory` shows the hardware memory.

Therefore, the memory obtained by running the `free -m` command is less than the memory configured for the ECS. This is a normal phenomenon.

**NOTE**

Physical servers also have this issue.
12.2 Disk Capacity Expansion

12.2.1 How Can I Add the Empty Partition of an Expanded System Disk to the End Root Partition Online?

Scenarios

If the capacity of system disk partitions is inconsistent with the actual system disk capacity after an ECS is created, you can add the empty partition to the root partition of the system disk.

This section describes how to add the empty partition to the end root partition online.

Procedure

In the following operations, the ECS that runs CentOS 6.5 64bit and has a 50 GB system disk is used as an example. The system disk has two partitions, /dev/xvda1: swap and /dev/xvda2: root, and the root partition is the end partition.

1. Run the following command to view disk partitions:
   ```bash
   parted -l /dev/xvda
   ```

2. Run the following command to obtain the file system type and UUID:
   ```bash
   blkid
   ```

3. Run the following command to install the growpart tool:
   ```bash
   yum install cloud-utils-growpart
   ```

4. Run the following command to expand the root partition (the second partition) using growpart:
   ```bash
   growpart /dev/xvda 2
   ```

5. Run the following command to verify that online capacity expansion is successful:
   ```bash
   parted -l /dev/xvda
   ```
Disk /dev/xvda: 53.7GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number Start End Size Type File system Flags
1 1049kB 4296MB 4295MB primary linux-swap(v1)
2 4296MB 53.7GB 49.4GB primary ext4 boot

6. Run the following command to expand the capacity of the file system:
   \texttt{resize2fs -f \$Partition name}
   
   Suppose the partition name is /dev/xvda2, run the following command:

   [root@sluo-ecs-a611 ~]# resize2fs -f /dev/xvda2
   resize2fs 1.42.9 (28-Dec-2013)
   Filesystem at /dev/xvda2 is mounted on /; on-line resizing required
   old_desc_blocks = 3, new_desc_blocks = 3
   ....
   [root@sluo-ecs-a611 ~] # df -hT  //Check file system capacity expansion

12.2.2 How Can I Add the Empty Partition of an Expanded System Disk to the Non-end Root Partition Online?

Scenarios

If the capacity of system disk partitions is inconsistent with the actual system disk capacity after an ECS is created, you can add the empty partition to the root partition of the system disk.

This section describes how to add the empty partition to the non-end root partition online.

Procedure

In the following operations, the ECS that runs CentOS 6.5 64bit and has a 100 GB system disk is used as an example. The system disk has two partitions, /dev/xvda1: root and /dev/xvda2: swap, and the root partition is not the end partition.

1. Run the following command to view disk partitions:
   \texttt{parted -l /dev/xvda}

   [root@sluo-ecs-a611 ~]# parted -l /dev/xvda
   Model: Xen Virtual Block Device (xvd)
   Disk /dev/xvda: 107GB
   Sector size (logical/physical): 512B/512B
   Partition Table: msdos
   Disk Flags:

   Number Start End Size Type File system Flags
   1 1049kB 41.0GB 40.9GB primary ext4 boot
   2 41.0GB 42.9GB 2000MB primary linux-swap(v1)

   The first is the root partition, and the second is the swap partition.

2. View and edit the fstab partition table to delete the swap partition attaching information.
   a. Run the following command to view the fstab partition table:
      \texttt{tail -n 3 /etc/fstab}
Run the following command to edit the fstab partition table and delete the swap partition attaching information.

```
vi /etc/fstab
tail -n 3 /etc/fstab
```

Run the following command to disable the swap partition:

```
swapoff -a
```

Delete the swap partition.

Run the following command to view the partition:

```
parted /dev/xvda
```

Press p.
Model: Xen Virtual Block Device (xvd)
Disk /dev/xvda: 107GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

<table>
<thead>
<tr>
<th>Number</th>
<th>Start</th>
<th>End</th>
<th>Size</th>
<th>Type</th>
<th>File system</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1049kB</td>
<td>41.0GB</td>
<td>40.9GB</td>
<td>primary</td>
<td>ext4</td>
<td>boot</td>
</tr>
<tr>
<td>2</td>
<td>41.0GB</td>
<td>42.9GB</td>
<td>2000MB</td>
<td>primary</td>
<td>linux-swaps(v1)</td>
<td></td>
</tr>
</tbody>
</table>

c. Run the following command to delete the partition:

```
rm 2
```

(d parted) rm2

d. Press p.

(parted) p

Model: Xen Virtual Block Device (xvd)
Disk /dev/xvda: 107GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

<table>
<thead>
<tr>
<th>Number</th>
<th>Start</th>
<th>End</th>
<th>Size</th>
<th>Type</th>
<th>File system</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1049kB</td>
<td>41.0GB</td>
<td>40.9GB</td>
<td>primary</td>
<td>ext4</td>
</tr>
</tbody>
</table>

e. Run the following command to edit the fstab partition table:

```
quit
```

(parted) quit

Information: You may need to update /etc/fstab.

5. Run the following command to view partition after the swap partition is deleted:

```
parted -l /dev/xvda
```

[root@sluo-ecs-a611 ~]# parted -l /dev/xvda

Model: Xen Virtual Block Device (xvd)
Disk /dev/xvda: 107GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

<table>
<thead>
<tr>
<th>Number</th>
<th>Start</th>
<th>End</th>
<th>Size</th>
<th>Type</th>
<th>File system</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1049kB</td>
<td>41.0GB</td>
<td>40.9GB</td>
<td>primary</td>
<td>ext4</td>
</tr>
</tbody>
</table>

6. Run the following command to install the growpart tool:

This tool may be integrated in the `cloud-utils-growpart/cloud-utils/cloud-initramfs-tools/cloud-init` package. Run the `yum install cloud-*` command to ensure it is available.

```
yum install cloud-utils-growpart
```

7. Run the following command to expand the root partition (the first partition) using growpart:

```
growpart /dev/xvda 1
```

[root@sluo-ecs-a611 ~]# growpart /dev/xvda 1

CHANGED: partition=1 start=2048 old: size=79978496 end=79980544 new: size=209710462,end=209712510
8. Run the following command to verify that online capacity expansion is successful:

   ```bash
   [root@sluo-ecs-a611 ~]# parted -l /dev/xvda
   Model: Xen Virtual Block Device (xvd)
   Disk /dev/xvda: 107GB
   Sector size (logical/physical): 512B/512B
   Partition Table: msdos
   Disk Flags:
   
   Number  Start   End    Size   Type     File system  Flags
   1  1049kB  107GB  107GB  primary  ext4         boot
   ```

9. Run the following command to expand the capacity of the file system:

   ```bash
   resize2fs -f $Partition name
   ```

   Suppose the partition name is `/dev/xvda1`, run the following command:

   ```bash
   [root@sluo-ecs-a611 ~]# resize2fs -f /dev/xvda1
   resize2fs 1.42.9 (28-Dec-2013)
   Filesystem on /dev/xvda1 is mounted on /; on-line resizing required
   old_desc_blocks = 3, new_desc_blocks = 3
   ....
   [root@sluo-ecs-a611 ~] # df -hT  //Check file system capacity expansion
   ```

---

**12.3 Disk Attachment**

**12.3.1 Can Multiple Disks Be Attached to an ECS?**

Yes. Disk functions have been upgraded recently. The ECSs created after the disk function upgrade can be attached with up to 60 disks.

- When creating an ECS, you can add 24 disks to it.
- After an ECS is created, up to 60 disks can be attached to it. For details, see Table 12-3.

**Table 12-3 Numbers of disks that can be attached to newly created ECSs**

<table>
<thead>
<tr>
<th>ECS Type</th>
<th>Maximum VBD Disks</th>
<th>Maximum SCSI Disks</th>
<th>Maximum Local Disks</th>
<th>Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xen</td>
<td>60</td>
<td>59</td>
<td>59</td>
<td>VBD disks + SCSI disks + Local disks ≤ 60</td>
</tr>
<tr>
<td>KVM</td>
<td>24</td>
<td>59</td>
<td>59</td>
<td>VBD disks + SCSI disks + Local disks ≤ 60</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SCSI disks + Local disks ≤ 59</td>
</tr>
</tbody>
</table>

**NOTE**

- The system disk of an ECS is of VBD type. Therefore, the maximum number of SCSI and local disks is 59.

The maximum number of disks attached to an ECS that is created before the disk function upgrade remains unchanged, as shown in Table 12-4.
### Table 12-4 Numbers of disks that can be attached to existing ECSs

<table>
<thead>
<tr>
<th>ECS Type</th>
<th>Maximum VBD Disks</th>
<th>Maximum SCSI Disks</th>
<th>Maximum Local Disks</th>
<th>Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xen</td>
<td>60</td>
<td>59</td>
<td>59</td>
<td>VBD disks + SCSI disks + Local disks ≤ 60</td>
</tr>
<tr>
<td>KVM</td>
<td>24</td>
<td>23</td>
<td>59</td>
<td>VBD disks + SCSI disks ≤ 24</td>
</tr>
</tbody>
</table>

#### How Can I Check Whether an ECS Is Created Before or After the Disk Function Upgrade?

1. Log in to management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. Click the name of the target ECS. The page providing details about the ECS is displayed.
4. Click the **Disks** tab.
5. Check the number of disks that can be attached to the ECS to determine the total number of disks.
   - If the total number of disks that can be attached is 24 (including the system disk), the ECS is created before the disk function upgrade.
   - If the total number of disks that can be attached is 60 (including the system disk), the ECS is created after the disk function upgrade.

#### 12.3.2 What Are the Restrictions on Attaching an EVS Disk to an ECS?

- The EVS disk and the target ECS must be located in the same AZ.
- The target ECS must be in **Running** or **Stopped** state.
- A frozen EVS disk cannot be attached to an ECS.
- For yearly/monthly ECSs:
  - If you detach the system disk purchased when creating an ECS and want to continue using it as a system disk, you can only attach it to the original ECS. If you want to use it as a data disk, you can attach it to any ECS.
  - If you detach the non-shared data disk purchased when you create an ECS and want to attach it again, you can only attach it to the original ECS as a data disk.

#### 12.3.3 Which ECSs Can Be Attached with SCSI EVS Disks?

A Xen ECS running one of the following OSs supports the attachment of SCSI EVS disks:

- Windows
- SUSE Enterprise Linux Server 11 SP4 64bit
- SUSE Enterprise Linux Server 12 64bit
- SUSE Enterprise Linux Server 12 SP1 64bit
- SUSE Enterprise Linux Server 12 SP2 64bit

All KVM ECSs support the attachment of SCSI EVS disks.
12.3.4 What Is the Mapping Between Device Names and Disks?

Scenarios

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

Obtaining the Disk ID of an ECS on the Management Console

1. Log in to the management console.
3. Click the target ECS name in the ECS list.
   The page providing details about the ECS is displayed.
4. Click the Disks tab and then to expand the disk information.
5. Check the device type and ID of the disk.

NOTE

If Device Identifier is not displayed on the web page, stop the ECS and restart it.
- If Device Type is VBD, use a serial number or BDF to obtain the disk device name. (Kunpeng ECSs support only serial numbers.)
  To use a serial number, see Using a Serial Number to Obtain a Disk Device Name.
  To use a BDF, see Using a VBD to Obtain a Disk Device Name.
- If Device Type is SCSI, use a WWN to obtain the disk device name. For details, see Using a WWN to Obtain a Disk Device Name.

Using a Serial Number to Obtain a Disk Device Name

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

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

```
# udevadm info --query=all --name=/dev/xxx | grep ID_SERIAL
# ll /dev/disk/by-id/*
```

Or:

```
# udevadm info --query=all --name=/dev/vdb | grep ID_SERIAL
# ll /dev/disk/by-id/*
```

The following information is displayed:

```
[root@ecs-ab63 ~]# udevadm info --query=all --name=/dev/vdb | grep ID_SERIAL
E: ID_SERIAL=62f0d06b-808d-480d-8
[root@ecs-ab63 ~]# ll /dev/disk/by-id/*
กระทา ../vda
```
The displayed information is the disk device name, /dev/vdb in the preceding terminal display.

Using a VBD to Obtain a Disk Device Name
1. Run the following command to use a BDF to obtain the device name:
   ```bash
   ll /sys/bus/pci/devices/BDF disk ID/virtio*/block
   ```
   For example, if the BDF disk ID of the VBD disk is 0000:02:02.0, run the following command to obtain the device name:
   ```bash
   ll /sys/bus/pci/devices/0000:02:02.0/virtio*/block
   ```
   The following information is displayed:
   ```bash
   [root@ecs-ab63 ~]# ll /sys/bus/pci/devices/0000:02:02.0/virtio*/block
   total 0
   drwxr-xr-x 8 root root 0 Dec 30 15:56 vdb
   ```
   The displayed information is the disk device name, /dev/vdb in the preceding terminal display.

Using a WWN to Obtain a Disk Device Name
1. Log in to the ECS as user root.
2. Run the following command to view the disk device name:
   ```bash
   ll /dev/disk/by-id |grep WWN|grep scsi-3
   ```
   For example, if the WWN obtained on the management console is 6888603000008b32fa16688d09368506, run the following command:
   ```bash
   ll /dev/disk/by-id |grep 6888603000008b32fa16688d09368506|grep scsi-3
   ```
   The following information is displayed:
   ```bash
   [root@host-192-168-133-148 block]# ll /dev/disk/by-id/ |grep 6888603000008b32fa16688d09368506 |grep scsi-3
   lrwxrwxrwx 1 root root 9 May 21 20:22 scsi-3 6888603000008b32fa16688d09368506 -> ../../sda
   ```

Obtaining the Disk Device Name of a Xen Instance

**Step 1** Obtain the disk information displayed on the management console.
1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. Click the target ECS name in the ECS list.
   The page providing details about the ECS is displayed.
4. Click the **Disks** tab and then  to expand the disk information.
5. Check the device name, type, and ID of the disk.
   - If the device type is **VBD**, go to Step 2.
   - If the device name is **SCSI**, go to Step 3.
NOTE

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

Step 2 Check the device name of a VBD disk on the ECS.

For a VBD disk, the device name displayed on the management console corresponds to the disk device name viewed on the ECS. For details, see Table 12-5.

Table 12-5 Mapping between disk device names displayed on the management console and those obtained on the ECS

<table>
<thead>
<tr>
<th>Device Name (Management Console)</th>
<th>Device Name (ECS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sd***</td>
<td>/dev/xvd***</td>
</tr>
<tr>
<td>/dev/vd***</td>
<td>/dev/xvd***</td>
</tr>
<tr>
<td>/dev/xvd***</td>
<td>/dev/xvd***</td>
</tr>
</tbody>
</table>

An example is provided as follows:

If the device name displayed on the management console is /dev/sdb, the device name of the device attached to the ECS is /dev/xvdb.

Step 3 Check the device name of a SCSI disk on the ECS.

1. Obtain the disk device ID.
   The device ID of the SCSI disk displays the disk WWN on the ECS.
2. Log in to the ECS as user root.
3. Run the following command to view the disk device name:

   ```
   ll /dev/disk/by-id | grep WWN | grep scsi-3
   
   [root@host-192-168-133-148 block]# ll /dev/disk/by-id/ | grep 68886030000008b32fa16688d09368506 | grep scsi-3
   lrwxrwxrwx 1 root root 9 May 21 20:22 scsi-36888603000008b32fa16688d09368506 -> ../../sda
   
   ---End
   ```

12.3.5 What Should I Do If a Linux ECS with a SCSI Disk Attached Fails to Restart?

Symptom

For a Linux ECS with a SCSI disk attached, if automatic SCSI disk attaching upon ECS startup is enabled in /etc/fstab and the disk drive letter (for example, /dev/sdb) is used, restarting the ECS may fail.

Possible Causes

SCSI disk allocation is determined based on the ID of the slot accommodating the disk as well as the available drive letter in the ECS. Each time when a disk is attached to the ECS, an idle
drive letter is automatically allocated in sequence. When the ECS starts, the disks are loaded in slot sequence. Therefore, a slot ID corresponds to a drive letter.

After the SCSI disk is detached from the running ECS, the slot sequence for disks may be changed, leading to the disk drive letter change after the ECS is restarted. As a result, the slot IDs do not correspond to the drive letters, and restarting the ECS failed.

Solution

1. Log in to the ECS as user root.
2. Run the following command to obtain the SCSI ID according to the drive letter of the SCSI disk:
   ```bash
   ll /dev/disk/by-id/|grep Disk drive letter
   ```
   For example, if the drive letter of the SCSI disk is /dev/sdb, run the following command:
   ```bash
   ll /dev/disk/by-id/|grep sdb
   ```
   CNA64_22:/opt/galax/eucalyptus/ecs_scripts # ll /dev/disk/by-id/|grep sdb
   lrwxrwxrwx 1 root root 9 Dec 6 11:26 scsi-3688860300001436b005014f890338280 -> ../../sdb
   lrwxrwxrwx 1 root root 9 Dec 6 11:26 wwn-0x688860300001436b005014f890338280 -> ../../sdb
   
   3. Change the drive letter (for example, /dev/sdb) of the SCSI disk to the corresponding SCSI ID in the /etc/fstab file.
      ```bash
      /dev/disk/by-id/SCSI ID
      ```
      For example, if the SCSI ID obtained in step 2 is scsi-3688860300001436b005014f890338280, use the following data to replace /dev/sdb:
      ```bash
      /dev/disk/by-id/scsi-3688860300001436b005014f890338280
      ```

12.3.6 How Can I Check Whether the ECSs Attached with the Same Shared SCSI Disk Are in the Same ECS Group?

Scenarios

Shared EVS disks of the SCSI type support SCSI locks. To improve data security, the shared EVS disks of the SCSI type must be attached to the ECSs in the same anti-affinity ECS group. This section describes how to check whether the ECSs attached with the same shared SCSI disk are in the same ECS group.

- For details about ECS groups, see Managing ECS Groups.
- For details about using shared EVS disks, see Shared EVS Disks and Usage Instructions.

Procedure

1. Log in to the management console.
3. Click the target shared SCSI disk to view its details.
4. In the Servers pane on the right side of the page, the ECSs to which the shared SCSI disk is attached are displayed.

In this example, the ECSs to which the shared SCSI disk volume-0001 is attached are ecs-0001 and ecs-0002.
Figure 12-6 Details about the disk

5. Click the names of these ECSs, respectively. On the page providing details about an ECS, you can view the ECS group to which the current ECS belongs. In this example, the ECS group to which ECS ecs-0001 belongs is ecs-group_01.

**NOTE**

If the ECS group is left blank, the ECS has not been added to any ECS group.

Figure 12-7 Details about an ECS (1)

In this example, the ECS group to which ECS ecs-0002 belongs is ecs-group_01.
Figure 12-8 Details about an ECS (02)

It is determined that the shared SCSI disk **volume-0001** is attached to ECSs **ecs-0001** and **ecs-0002**, and both ECSs are in ECS group **ecs-group_01**.

### 12.4 Others

#### 12.4.1 Who Can Use the Encryption Feature?

The rights of users in a user group to use the encryption feature are as follows:

- The user having security administrator rights can grant KMS access rights to EVS for using the encryption feature.
- When a common user who does not have security administrator rights attempts to use the encryption feature, the condition varies depending on whether the user is the first one in the user group to use this feature.
  - If the common user is the first one in the user group to use the encryption feature, the user must contact the user having security administrator rights for rights granting. Then, the common user can use the encryption feature.
  - If the common user is not the first one in the user group to use the encryption feature, the user has permission to use the encryption feature.

The following section uses a user group as an example to describe how to grant KMS access rights to EVS for using the encryption feature.

For example, a user group shown in Figure 12-9 consists of four users, user 1 to user 4. User 1 has security administrator rights. Users 2, 3, and 4 are common users who do not have security administrator rights.
Scenario 1: User 1 Uses the Encryption Feature

In this user group, if user 1 uses the encryption feature for the first time, the procedure is as follows:

1. User 1 creates Xrole to grant KMS access rights to EVS.
   After rights granting, the system automatically creates CMK *evs/default* for encrypting EVS disks.

   **NOTE**

   Encrypting EVS disks relies on KMS. When user 1 uses the encryption feature for the first time, the user must grant the KMS access rights to EVS. Then, all users in the user group can use the encryption feature, without requiring the rights granting any more.

2. User 1 selects a key.
   One of the following keys can be used:
   - Default CMK, *evs/default*
   - CMK, the key that you have created before using the EVS disk encryption feature
   - Newly created key (For instructions about how to create a key, see *Creating a Key Pair in Data Encryption Workshop User Guide*.)

After user 1 uses the encryption feature, all other users in the user group can use this feature, without requiring to contact user 1 for rights granting.

Scenario 2: Common User Uses the Encryption Feature

In this user group, if user 3 uses the encryption feature for the first time, the procedure is as follows:

1. When user 3 uses the encryption feature, the system displays a message indicating that the user has no rights.
2. User 3 asks user 1 to create Xrole to grant KMS access rights to EVS.

After the rights are granted, user 3 and all other users in the user group can use the encryption feature, without requiring to contact user 1 for rights granting.
12.4.2 How Can I Add an ECS with Local Disks Attached to an ECS Group?

An ECS group logically isolates ECSs. The ECSs in an ECS group support anti-affinity and are allocated on different hosts.

An ECS with local disks attached cannot be added to an ECS group after the ECS is created. To use ECS group functions, select a security group during ECS creation.

12.4.3 What Should I Do If a Disk Is Offline?

**Symptom**

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

**Possible Causes**

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

**Table 12-6 SAN policies**

<table>
<thead>
<tr>
<th>SAN Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnlineAll</td>
<td>Indicates that all newly detected disks are automatically brought online.</td>
</tr>
<tr>
<td>OfflineShared</td>
<td>Indicates that all newly detected disks on sharable buses, such as FC or iSCSI, are left offline by default, while disks on non-sharable buses are kept online.</td>
</tr>
<tr>
<td>OfflineInternal</td>
<td>Indicates that all newly detected disks are left offline.</td>
</tr>
</tbody>
</table>
The SAN policy of certain Windows OSs, such as Windows Server 2008/2012 Enterprise Edition and Data Center Edition, is **OfflineShared** by default.

**Solution**

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

1. Log in to the Windows ECS.
2. Press **Win+R** to run **cmd.exe**.
3. Run the following command to access DiskPart:
   ```bash
diskpart
```
4. Run the following command to view the SAN policy on the ECS:
   ```bash
san
```
   - If the SAN policy is **OnlineAll**, run the **exit** command to exit DiskPart.
   - If the SAN policy is not **OnlineAll**, go to step 5.
5. Run the following command to change the SAN policy to **OnlineAll**:
   ```bash
san policy=onlineall
```
6. (Optional) Use the ECS with the SAN policy changed to create a private image to make the configuration take effect permanently. After an ECS is created using this private image, the disks attached to the ECS are online by default. You only need to initialize them.

**12.4.4 How Can I Obtain Data Disk Information If Tools Are Deleted?**

If Tools are uninstalled from a Linux ECS in a non-PVOPS system, data disks cannot be identified. In such a case, you can obtain information about these data disks by creating a new ECS and attaching the data disks of the original ECS to the new ECS. The procedure is as follows:

1. Log in to the management console and create a new ECS.
   
   **NOTE**
   
   The new ECS must be located in the same AZ and have the same parameter settings as the original ECS.

2. (Optional) On the **Elastic Cloud Server** page, locate the row containing the original ECS, click **More** in the **Operation** column, and select **Stop**. On the **Stop ECS** page, select **Forcibly stop the preceding ECSs** and **Yes** and click **OK** to forcibly stop the original ECS.

   Manually refresh the **Elastic Cloud Server** page. The original ECS is stopped once the **Status** changes to **Stopped**.

   **NOTE**

   The ECSs running certain OSs support online data disk detaching. If your OS supports this feature, you can detach data disks from the running ECS.

3. Click **→** to view information about the data disks attached to the original ECS.

   **NOTE**

   If the original ECS has multiple data disks attached, repeat steps 4 to 6 to attach each data disk to the new ECS.

4. Click a data disk.
The Elastic Volume Service page is displayed.

5. Select the data disk to be detached and click Detach in the Operation column. On the Detach Disk page, select the original ECS and click OK to detach the data disk from the original ECS.

Manually refresh the Elastic Volume Service page. The data disk is detached from the original ECS once the Status changes to Available.

6. Select the detached data disk and click Attach in the Operation column. On the Attach Disk page, click the new ECS, select a device name, and click OK to attach the data disk to the new ECS.

Manually refresh the EVS list. The data disk is attached to the new ECS once the Status value changes to In-use. You can then log in to the management console and view information about the data disk of the new ECS.
13 Passwords and Key Pairs

13.1 Passwords

13.1.1 How Can I Change the Password for Logging In to a Linux ECS?

Solution

1. Use the existing key file to log in to the Linux ECS as user root.
2. Run the following command to reset the password of user root:
   ```bash
   passwd
   ```
   To reset the password of another user, replace `passwd` with `passwd username`.
3. Enter the new password as prompted.
   
   New password:
   Retype new password:
   
   If the following information is displayed, the password has been reset:
   ```bash
   passwd: password updated successfully
   ```

13.1.2 What Is the Default Password for Logging In to a Linux ECS?

The default username for logging in to an ECS running Linux, such as CentOS or Ubuntu is root, and the password is the one you set during ECS creation.
13.1.3 How Can I Set the Validity Period of the Image Password?

If an ECS cannot be logged in because of expired image password, you can contact the administrator for handling.

If the ECS can still be logged in, you can perform the following operations to set the password validity period.

Procedure

The following operations use EulerOS 2.2 as an example.

1. Log in to the ECS.
2. Run the following command to check the password validity period:
   - `vi /etc/login.defs`
   The value of parameter `PASS_MAX_DAYS` is the password validity period.
3. Run the following command to change the value of parameter `PASS_MAX_DAYS`:
   - `chage -M 99999 user_name`
   99999 is the password validity period, and `user_name` is the system user, for example, user `root`.

   **NOTE**
   You are advised to configure the password validity period as needed and change it at a regular basis.
4. Run command `vi /etc/login.defs` to verify that the configuration has taken effect.
13.1.4 Changing the Login Password on an ECS

Scenarios

This section describes how to change the password for logging in to an ECS when the password is about to expire, the password is forgotten, or you log in to the ECS for the first time. You are advised to change the initial password upon the first login.

Resetting the ECS password on the management console is preferentially recommended.

Prerequisites

The ECS can be logged in.

Background

Table 13-1 shows the ECS password complexity requirements.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>• Consists of 8 characters to 26 characters.</td>
<td>Test12!@</td>
</tr>
<tr>
<td></td>
<td>• Contains at least three of the following character types:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Uppercase letters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Lowercase letters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Digits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Special characters for Windows: $!@%_-+=[]:/.,?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Special characters for Linux: !@%_-+=[]:/^,{}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cannot contain the username or the username spelled backwards.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)</td>
<td></td>
</tr>
</tbody>
</table>
Windows
1. Log in to the ECS.
   For details, see Login Overview.
2. Press Win+R to start the Open dialog box.
3. Enter cmd to open the command-line interface (CLI) window.
4. Run the following command to change the password (the new password must meet the requirements described in Table 13-1):
   \image{net user Administrator New password}

Linux
1. Use the existing key file to log in to the Linux ECS as user root through SSH.
   For details, see Login Using an SSH Key.
2. Run the following command to reset the password of user root:
   \image{passwd}
   To reset the passwords of other users, replace passwd with passwd username.
3. Enter the new password as prompted. Ensure that the new password meets the requirements described in Table 13-1.
\image{New password:
Retype new password:
If the following information is displayed, the password has been changed:
passwd: password updated successfully}

13.1.5 Resetting the Password for Logging In to a Windows ECS

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

For details about the operations performed on Linux ECSs, see 13.1.6 Resetting the Password for Logging In to a Linux ECS.

NOTE
- If your ECS has had password reset plug-ins installed, follow the instructions provided in Resetting the ECS Password on the Management Console to obtain a new password.
- The password reset plug-ins have been installed on the ECSs created using a public image by default. To reset the password, see Resetting the ECS Password on the Management Console.

Prerequisites
- A temporary Linux ECS which runs Ubuntu 14.04 or later and locates in the same AZ as the target ECS is available.
- You have bound an EIP to the temporary ECS and configured the apt-get source.
- You have used either of the following methods to install ntfs-3g and chntpw software packages on the temporary ECS:
  Method 1:
  Run the following command to install the ntfs-3g and chntpw software packages:
**Elastic Cloud Server**
**FAQs**

### Passwords and Key Pairs

#### Method 2:
Download the desired `ntfs-3g` and `chntpw` software packages according to the temporary ECS OS. For detailed installation and use guide, see the [NTFS official website](https://tuxera.com/community) and [chntpw official website](https://pkgs.org/download/chntpw).

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

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

### Procedure

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

   **NOTE**
   Do not forcibly stop the Windows ECS. Otherwise, password reset may fail.
   e. Locate the row containing the system disk and click **Detach** to detach the system disk from the ECS.
   f. On the page providing details about the temporary ECS, click the **Disks** tab.
   g. Click **Attach Disk**. In the displayed dialog box, select the system disk detached in step 1.e and attach it to the temporary ECS.

2. Log in to the temporary ECS remotely and attach the system disk.
   a. Run the following command to view the directory of the system disk detached from the original Windows ECS now attached to the temporary ECS:

```
fdisk -l
```

b. Run the following command to mount the file system of the detached system disk to the temporary ECS:

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

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

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

If the following error information is displayed after the preceding command is executed, the ntfs file systems may be inconsistent. In such an event, rectify the file system inconsistency.

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

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

```
ntfsfix /dev/Result obtained in step 2.a
```
For example, if the result obtained in step 2.a is \texttt{xvde2}, run the following command:
\texttt{ntfsfix /dev/xvde2}

3. Change the password and clear the original password.
   a. Run the following command to back up the SAM file:
      \texttt{cp /mnt/Windows/System32/config/SAM /mnt/Windows/System32/config/SAM.bak}
   b. Run the following command to change the password of a specified user:
      \texttt{chntpw -u Administrator /mnt/Windows/System32/config/SAM}
   c. Enter \texttt{1}, \texttt{q}, and \texttt{y} as prompted, and press \texttt{Enter}

   The password has been reset if the following information is displayed:
   Select: [q] > 1
   Password cleared!
   Select: [q] > q
   Hives that have changed:
   #Name
   0<SAM>
   Write hive files? (y/n) [n] : y
   0<SAM> - OK

4. Stop the temporary ECS, detach the system disk, and attach the system disk to the original Windows ECS.
   a. Stop the temporary ECS, switch to the page providing details about the ECS, and click the \texttt{Disks} tab.
   b. Click \texttt{Detach} to detach the data disk temporarily attached in step 1.g.
   c. On the page providing details about the original Windows ECS, click the \texttt{Disks} tab.
   d. Click \texttt{Attach Disk}. In the displayed dialog box, select the data disk detached in step 4.b and device name \texttt{/dev/sda}.

5. Start the original Windows ECS and set a new login password.
   a. Click \texttt{Start} to start the original Windows ECS. After the status becomes \texttt{Running}, click \texttt{Remote Login} in the \texttt{Operation} column.
   b. Click \texttt{Start}. Enter CMD in the search box and press \texttt{Enter}.
   c. Run the following command to change the password (the new password must meet the requirements described in Table 13-2):
      \texttt{net user Administrator New password}

\textbf{Table 13-2 Password complexity requirements}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>• Consists of 8 characters to 26 characters.</td>
<td>Test12!@</td>
</tr>
<tr>
<td></td>
<td>• Contains at least three of the following character types:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Uppercase letters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Lowercase letters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Digits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Special characters for Windows: $!@-%_=-+[:;/.?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Special characters for Linux: !@-%_=-+[:;/^{}?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cannot contain the username or the username spelled</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Requirement</td>
<td>Example Value</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>backwards.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)</td>
<td></td>
</tr>
</tbody>
</table>

13.1.6 Resetting the Password for Logging In to a Linux ECS

Scenarios

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

For details about the operations performed on Windows ECSs, see 13.1.5 Resetting the Password for Logging In to a Windows ECS.

 החדש

- If your ECS has had password reset plug-ins installed, follow the instructions provided in Resetting the ECS Password on the Management Console to obtain a new password.
- The password reset plug-ins have been installed on the ECSs created using a public image by default. To reset the password, see Resetting the ECS Password on the Management Console.

Prerequisites

- A temporary Linux ECS which locates in the same AZ as the target ECS is available.
- You have bound an EIP to the temporary ECS.

Procedure

1. Download the script for resetting the password and upload the script to the temporary ECS.
   a. Log in to the management console and click Elastic Cloud Server under Computing.
   b. Click (in the upper left corner and select the desired region and project.
   c. Locate the row containing the target ECS, click More in the Operation column, and select Reset Password.

The Reset Password dialog box is displayed. Click the text in the red box shown in Figure 13-3 to download the script.
You can view the downloaded password reset script in the lower left corner of the
desktop.

d. Use a connection tool, such as WinSCP, to upload the obtained `changepasswd.sh`
   script to the temporary ECS.
   To download WinSCP, log in at [https://winscp.net/](https://winscp.net/).

2. Stop the original Linux ECS, detach the system disk, and attach the system disk to the
temporary ECS.
   a. Stop the original Linux ECS, switch to the page providing details about the ECS,
      and click the Disks tab.

   **NOTE**
   Do not forcibly stop the original ECS. Otherwise, password reset may fail.
   b. Locate the row containing the system disk to be detached and click Detach to
detach the system disk from the ECS.
   c. On the page providing details about the temporary ECS, click the Disks tab.
   d. Click Attach Disk. In the displayed dialog box, select the system disk detached in
      step 2.b and attach it to the temporary ECS.

3. Log in to the temporary ECS remotely and reset the password.
   a. Locate the row containing the temporary ECS and click Remote Login in the
      Operation column.
   b. Run the following command to view the directory of the system disk detached from
      the original Linux ECS now attached to the temporary ECS:
      
      `fdisk -l`
   c. Run the following commands in the directory where the script is stored to run the
      script for resetting the password:
      
      `chmod +x changepasswd.sh`
      `./changepasswd.sh`

   When you run the password reset script, if the system displays a message indicating
that there is no command related to logical volume manager (LVM), such as the
message "no lvs command", install an LVM tool on the temporary ECS. The LVM2
 tool is recommended, which can be installed by running the `yum install lvm2`
command.
If the original ECS and the temporary ECS both run CentOS 7, a mount failure may occur during script execution. To resolve this issue, replace `mount $dev $mountPath` with `mount -o nouuid $dev $mountPath` in the script.

4. Stop the temporary ECS, detach the system disk, attach the system disk to the original Linux ECS, and restart the original Linux ECS.
   a. Stop the temporary ECS, switch to the page providing details about the ECS, and click the Disks tab.
   b. Click Detach to detach the data disk attached in step 2.
   c. On the page providing details about the original Linux ECS, click the Disks tab.
   d. Click Attach Disk. In the displayed dialog box, select the data disk detached in step 4.b and device name /dev/sda.
   e. Restart the original Linux ECS.

13.1.7 What Should I Do If the System Displays a Message Indicating that the Password Is Incorrect When I Remotely Log In to My ECS?

Solution

Check the network configuration of the ECS and determine whether the fault is caused by a Cloud-Init failure.

- Verify that port 80 is bypassed in both inbound and outbound directions in the security group to which the target ECS belongs.

![Figure 13-4 Port 80](image)

- Verify that DHCP is enabled in the subnet to which the target ECS belongs.

![Figure 13-5 Checking DHCP status](image)

**NOTE**

After verifying the preceding configurations, restart the ECS, wait for 3 to 5 minutes, and remotely log in to the ECS using a password or key.
13.1.8 What Should I Do If I Cannot Log In to My ECS Using the Initial Password After I Use It for a Period of Time?

Solution

Check whether the remote login page can be displayed.

- If the login page cannot be displayed, an error may have occurred in the GuestOS process on the ECS. In such a case, contact technical support for troubleshooting.
- If the login page can be displayed, log in to the OS in single-user mode for troubleshooting. The procedure is as follows:
  - Check whether the password can be changed in single-user mode.
    - If the password can be changed, change it and contact technical support to check whether the password has been maliciously changed due to an attack.
    - If the password cannot be changed, verify that the values of `hard` and `soft` in `/etc/security/limits.conf` are not greater than 65535.

Change the password in single-user mode and try to log in to the ECS again.

13.1.9 What Should I Do If I Cannot Log In to My ECS Using the Reset Password?

Scenarios

A new password obtained using the one-click password reset function cannot be used to log in to the ECS. To troubleshoot this issue, see this section.

**NOTE**

Ensure that the one-click password reset plug-ins are not blocked by security software. Otherwise, the one-click password reset function cannot be used.

Windows

Perform the following operations to locate the fault:

**Step 1** Check whether port 80 in the outbound direction of the security group is permitted.

1. Log in to management console.
2. Select the target ECS to switch to the page providing details about the ECS.
3. On the **Security Groups** tab, check whether port 80 in the outbound direction of the security group is bypassed.

By default, the **Protocol** and **Port Range/ICMP Type** values in the outbound direction are both **Any**, indicating that port 80 is bypassed.
Step 2  Check whether DHCP is enabled in the VPC of the ECS.

Under Network, click Virtual Private Network. Switch to the page providing details about the target VPC, click Subnets, and enable DHCP.

Step 3  If both the security group and DHCP are properly configured but one-click password reset still fails to take effect, use the original password to log in to the ECS.

- If the original password is invalid, reset the password. For details, see 13.1.5 Resetting the Password for Logging In to a Windows ECS.

- If the original password is valid, use it to log in to the ECS and reset the password. For details, see 13.1.4 Changing the Login Password on an ECS.

Step 4  Check whether password reset plug-ins CloudResetPwdAgent and CloudResetPwdUpdateAgent have been installed on the ECS. To do so, perform the following operations:

Start the Task Manager and check whether cloudResetPwdAgent and cloudResetPwdUpdateAgent are displayed on the Services tab. If no, the one-click password reset plug-ins have not been installed on the ECS.

To install the plug-ins, see Installing One-Click Password Reset Plug-ins.

Figure 13-6 Successful plug-ins installation

----End
**Linux**

Perform the following operations to locate the fault:

**Step 1** Check whether port 80 in the outbound direction of the security group is permitted.

1. Log in to management console.
2. Select the target ECS to switch to the page providing details about the ECS.
3. On the **Security Groups** tab, check whether port 80 in the outbound direction of the security group is bypassed.

   By default, the **Protocol** and **Port Range/ICMP Type** values in the outbound direction are both **Any**, indicating that port 80 is bypassed.

**Step 2** Check whether DHCP is enabled in the VPC of the ECS.

Under **Network**, click **Virtual Private Network**. Switch to the page providing details about the target VPC, click **Subnets**, and enable DHCP.

**Step 3** If both the security group and DHCP are properly configured but one-click password reset still fails to take effect, use the original password to log in to the ECS.

- If the original password is invalid, enter the single-user mode and reset the password.
  
  For details, see [Troubleshooting Resetting the Password of User root in the Single-User Mode](#).

- If the original password can be used, perform the following operations for further check:
  a. Use the original password to log in to the ECS.
  b. Run the `curl http://169.254.169.254/openstack/latest/resetpwd_flag` command to check whether the one-click password reset function is available.
     - If the return value is **true**, the password can be reset with a few clicks.
     - If other values are returned, the password cannot be reset or the network malfunctions.

**Step 4** Check whether CloudResetPwdAgent has been installed.

1. Check whether the **CloudResetPwdAgent** directory is available in the root directory on the ECS.
   - If yes, go to **Step 4.2**.
   - If no, the one-click password reset plug-ins have not been installed on the ECS.
     
     To install the plug-ins, see [Installing One-Click Password Reset Plug-ins](#).

2. Run the following command to check the CloudResetPwdAgent status:

   ```shell
   service cloudResetPwdAgent status
   ```

   If the command output is "unrecognized service", the one-click password reset plug-ins have not been installed on the ECS.

   To install the plug-ins, see [Installing One-Click Password Reset Plug-ins](#).

---End
13.1.10 What Should I Do If a Service Port Is Used by a One-Click Password Reset Plug-in?

**Symptom**

When an application is to run on an ECS, the system displays a message indicating that the required port is used by a one-click password reset plug-in. What should I do if such an issue occurs?

**Possible Causes**

If an ECS works in AUTO mode, when its one-click password reset plug-ins start, the plug-ins randomly use a port, which may be a service port.

**NOTE**

The one-click password reset plug-ins have been upgraded to work in PIPE mode by default.

- Newly created ECSs run in PIPE mode by default, and their one-click password reset plug-ins will not use service ports.
- Existing ECSs still work in AUTO mode, in which the plug-ins randomly use a service port ranging from 31000 to 32999. The system will automatically select an idle port with the smallest port number.

**Method 1 (Recommended): Modifying the wrapper Files of the One-Click Password Reset Plug-ins for the PIPE Mode**

In the wrapper files, change from AUTO (SOCKET) to PIPE. After the change, the plug-ins will not use service ports.

1. Open CloudResetPwdAgent configuration files.
   - Linux
     /CloudResetPwdAgent/conf/wrapper.conf and /CloudResetPwdUpdateAgent/conf/wrapper.conf
   - Windows
     C:/CloudResetPwdUpdateAgent/conf/wrapper.conf and C:/CloudResetPwdUpdateAgent/conf/wrapper.conf

2. Add the following data to the end of the files:

   ```
   wrapper.backend.type=PIPE
   ```

3. Restart CloudResetPwdUpdateAgent.
   - Linux
     /CloudResetPwdUpdateAgent/bin/cloudResetPwdUpdateAgent.script restart
   - Windows
     i. Press Win+R to start the **Open** text box.
     ii. Enter **services.msc** and click **OK**.
iii. Right-click **cloud reset password update agent** and choose **Restart** from the shortcut menu.

**Figure 13-8 Services (Local)**

**Method 2: Modifying the Configuration to Change the Port Range**

Modify the CloudResetPwdAgent configuration to change the default port range for the password reset plug-ins so that the service port is out of the port range.

For example, to change the port range for the password reset plug-ins to 40000-42000, perform the following operations:

1. Open CloudResetPwdAgent configuration files.
   - Linux
     `/CloudrResetPwdAgent/conf/wrapper.conf` and
     `/CloudResetPwdUpdateAgent/conf/wrapper.conf`
   - Windows
     `C:\CloudResetPwdUpdateAgent\conf\wrapper.conf` and
     `C:\CloudResetPwdUpdateAgent\conf\wrapper.conf`

2. Add the following data to the configuration files:

   \[\text{wrapper.port.min}=40000\]
   \[\text{wrapper.port.max}=41000\]
   \[\text{wrapper.jvm.port.min}=41001\]
   \[\text{wrapper.jvm.port.max}=42000\]
3. Restart CloudResetPwdUpdateAgent.
   - Linux
     `/CloudResetPwdUpdateAgent/bin/cloudResetPwdUpdateAgent.script restart`
   - Windows
     i. Press Win+R to start the Open text box.
     ii. Enter `services.msc` and click OK.
     iii. Right-click `cloud reset password update agent` and choose Restart from the shortcut menu.
13.2 Key Pairs

13.2.1 How Can I Obtain the Key Pair Used by an ECS?

**Symptom**

If a user has created multiple key pairs, the user might not know which is the required one for logging in to the target ECS. This section describes how to quickly identify the target key pair on the management console.

**Procedure**

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, select the target ECS.
5. Click the name of the ECS.
   The page providing details about the ECS is displayed.
6. Obtain the **Key Pair** value.
   The value is the key pair used by the ECS.

13.2.2 How Can I Use a Key Pair?

**Symptom**

When you purchase an ECS, the system asks you to select a login mode. If you select **Key pair**, you are required to select an existing key pair or create a new pair.

If no key pair is available, create one on the management console.

**Solution**

1. In the navigation pane of the ECS console, choose **Key Pair**. Then, click **Create Key Pair**.
2. After the key pair is created, download the private key to a local directory.

**Figure 13-13** Downloading a key pair

3. When purchasing an ECS, select the created or existing key pair in **Key pair**.

**Figure 13-14** Selecting a key pair

### 13.2.3 What Should I Do If a Key Pair Cannot Be Imported?

If you use Internet Explorer 9 to access the management console, the key pair may fail to import or the file injection function may become unavailable. In this case, perform the following steps to modify browser settings and then try again:
13.2.4 Why Was My Login to a Linux ECS Using a Key File Unsuccessful?

Symptom

When the key file for creating a Linux ECS was used to log in to the ECS, the login failed.

Possible Causes

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

- Cause 1: The image used to create the Linux ECS is a private image, on which Cloud-Init is not installed.
- Cause 2: Cloud-Init is installed on the image, but the key pair was not obtained during ECS creation.

Solution

- If the issue is a result of cause 1, proceed as follows:
  If a private image is created without Cloud-Init installed, the ECS configuration cannot be customized. As a result, you can log in to the ECS only using the original image password or key pair.
  The original image password or key pair is the OS password or key pair configured when the private image was created. If the original image password was forgotten or key pair has been lost, use the password reset function available on the Elastic Cloud Server page to reset the password.
- If the issue is a result of cause 2, proceed as follows:
  a. Locate the row containing the target ECS, click More in the Operation column, and select Restart.
  b. Use the key file to log in to the ECS again and check whether the login is successful.
     - If the login is successful, no further action is required.
     - If no, contact technical support.
13.2.5 What Should I Do If I Cannot Download a Key Pair?

The private key file of a key pair can be downloaded only once.

If your private key file has been lost, create a key pair and download the private key file again.

Solution

1. Log in to the management console and choose Key Pair.

**Figure 13-15 Key Pair**

2. Click Create Key Pair.

**Figure 13-16 Create Key Pair**

3. Click OK to save the private key to your local directory.

**Figure 13-17 Saving the private key**
13.2.6 What Should I Do If a Key Pair Created Using `puttygen.exe` Cannot Be Imported to the Management Console?

Symptom

When a key pair created using `puttygen.exe` was imported to the management console, the system displayed a message indicating that importing the public key failed.

Possible Causes

The format of the public key content does not meet system requirements.

Storing a public key by clicking Save public key of `puttygen.exe` will change the format of the public key content. Such a key cannot be imported to the management console.

Solution

Use the locally stored private key and `PuTTY Key Generator` to restore the format of the public key content. Then, import the public key to the management console.

1. Double-click `puttygen.exe` to switch to the PuTTY Key Generator page.

Figure 13-18 PuTTY Key Generator
2. Click **Load** and select the private key.
   The system automatically loads the private key and restores the format of the public key content in **PuTTY Key Generator**. The content in the red box in **Figure 13-19** is the public key with the format meeting system requirements.

**Figure 13-19** Restoring the format of the public key content

3. Copy the public key content to a .txt file and save the file in a local directory.
4. Import the public key to the management console.
   a. Log in to the management console.
   b. Click 📍 in the upper left corner and select the desired region and project.
   c. Under **Computing**, click **Elastic Cloud Server**.
   d. In the navigation pane on the left, choose **Key Pair**.
   e. On the right side of the page, click **Import Key Pair**.
   f. Copy the public key content in the .txt file to **Public Key Content** and click **OK**.
13.2.7 What Is the cloudbase-init Account in Windows ECSs?

Description

In Windows ECSs, cloudbase-init is the default account of the Cloudbase-Init agent program. It is used to obtain the metadata and execute configurations when the ECS starts.

NOTE

This account is unavailable on Linux ECSs.

Do not modify or delete this account or uninstall the Cloudbase-Init agent program. Otherwise, injecting the customized data for initializing the ECS generated using the Windows private image created based on this ECS will fail.

Security Hardening for Randomized cloudbase-init Passwords

In Cloudbase-Init 0.9.10, the security of randomized cloudbase-init passwords has been hardened to ensure that the hash values (LM-HASH and NTLM-HASH) of the passwords are different.

In Windows, the hash passwords are in the format of "Username:RID:LM-HASH value:NT-HASH value".

For example, in "Administrator:500:C8825DB10F2590EAAAD3B435B51404EE:683020925C5D8569C23A A724774CE9CC::",

- **Username**: Administrator
- **RID**: 500
- **LM-HASH value**: C8825DB10F2590EAAAD3B435B51404EE
- **NT-HASH value**: 683020925C5D8569C23AA724774CE9CC

Use an image to create two ECSs, ecs01 and ecs02. Then, verify that the hash values of the cloudbase-init account for the two ECSs are different.

- LM-HASH and NT-HASH values of the cloudbase-init account for ecs01

- LM-HASH and NT-HASH values of the cloudbase-init account for ecs02
13.2.8 What Should I Do If Cloud-Init Does Not Work After Python Is Upgraded?

Symptom

Take an ECS running CentOS 6.8 as an example. After Python was upgraded from 2.6 to 2.7, Cloud-Init did not work. Data, such as the login password, key, and hostname could not be imported to the ECS using Cloud-Init.

After the `cloud-init -v` command was executed to view the Cloud-Init version, the system displayed errors, as shown in Figure 13-20.

Figure 13-20 Errors in Cloud-Init

Possible Causes

The Python version used by Cloud-Init was incorrect.

Solution

Change the Python version used by Cloud-Init to the source version. To do so, change the environment variable value of `/usr/bin/cloud-init` from the default value `#!/usr/bin/python` to `#!/usr/bin/python2.6`. 
Figure 13-21 Changing the Python version

[root@ecs-0568 ~]# head -n 1 /usr/bin/cloud-init
#!usr/bin/python2.6
[root@ecs-0568 ~]# /usr/bin/python -V
Python 2.7.7
[ruser@centos5 1 root root 24 Jun 19 18:55 /usr/bin/python -> /usr/local/bin/python2.7
[ruser@centos5 1 root root 6 Jan 3 2017 /usr/bin/python2 -> python
[ruser@centos5 1 root root 8 Aug 10 2016 /usr/bin/python2.6

14.1 EIP FAQs

14.1.1 Can Multiple EIPs Be Bound to an ECS?

Scenarios

An ECS can be bound with multiple EIPs, though this configuration is not recommended.

To bind multiple EIPs, you must manually configure routing policies. Exercise caution when you perform this operation.

Configuration Example

Table 14-1 lists ECS configurations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>ecs_test</td>
</tr>
<tr>
<td>Image</td>
<td>Red Hat Enterprise Linux 6.5 64bit</td>
</tr>
<tr>
<td>EIP</td>
<td>2</td>
</tr>
<tr>
<td>Primary NIC</td>
<td>eth0</td>
</tr>
<tr>
<td>Secondary NIC</td>
<td>eth1</td>
</tr>
</tbody>
</table>

Example 1:

If you are required to access public network 11.11.11.0/24 through standby NIC eth1, perform the following operations to configure a routing policy:

1. Log in to the ECS.
2. Run the following command to configure a routing policy:

   ```
   ip route add 11.11.11.0/24 dev eth1 via 192.168.2.1
   ```

   In the preceding command, `192.168.2.1` is the gateway IP address of standby NIC eth1.
Example 2:
Based on example 1, if you are required to enable routing for default public network traffic through standby NIC eth1, perform the following operations to configure a routing policy:

1. Log in to the ECS.
2. Run the following command to delete the default route:
   ```
   ip route delete default
   ```
3. Run the following command to configure a new default route:
   ```
   ip route add 0.0.0.0/0 dev eth1 via 192.168.2.1
   ```
   In the preceding command, 192.168.2.1 is the gateway IP address of standby NIC eth1.

14.1.2 Can an ECS Without an EIP Access the Internet?
Yes.
You can use the NAT Gateway service available on the public cloud platform. This service offers NAT for ECSs in a VPC, allowing these ECSs to access the Internet using an EIP. The SNAT function provided by the NAT Gateway service allows the ECSs in a VPC to access the Internet without requiring an EIP. Additionally, SNAT supports a large number of concurrent connections for the applications requiring a large number of requests and connections. For more information about NAT Gateway, see NAT Gateway Service Overview.

14.1.3 Why Cannot an EIP Be Pinged?
Symptom
After I purchased an EIP and bound it to an ECS, pinging the EIP failed, or the ECS failed to access the Internet.

Solution
1. Check security group rules.
   Check whether the ECS NIC security group allows the inbound ICMP traffic. Any rule in the following figure can be met.

<table>
<thead>
<tr>
<th>Transfer Direction</th>
<th>Type</th>
<th>Protocol/Port Range</th>
<th>Source End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>IPv4</td>
<td>Any/Any</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

2. Check network ACLs.
   a. Check the network ACL status.
Obtain the network ACL status.

**Figure 14-1** Enabled network ACL

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Associate</th>
<th>Description</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw:51ce</td>
<td>Enabled</td>
<td>subnet:...</td>
<td></td>
<td>Associate Subnet</td>
</tr>
</tbody>
</table>

**Figure 14-2** Disabled network ACL

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Associate</th>
<th>Description</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw:51ce</td>
<td>Disabled</td>
<td>subnet:he...</td>
<td></td>
<td>Associate Subnet</td>
</tr>
</tbody>
</table>

b. Check whether the NIC to which the EIP bound belongs to the subnet associated with the network ACL.

**Figure 14-3** Associated subnet

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Associated Subnets</th>
<th>Description</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw:51ce</td>
<td>Enabled</td>
<td></td>
<td></td>
<td>Associate Subnet</td>
</tr>
</tbody>
</table>
c. If the network ACL is enabled, add an ICMP rule to allow traffic.

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

3. Check whether the default route is available in the ECS.
   a. Log in to the ECS and run the following command to check whether the default route is available:
      ```
      ip route
      ```
      
      b. If the route is unavailable, run the following command to add it:
      ```
      ip route add default via XXXX dev eth0
      ```

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

4. Ping the affected EIP from another ECS in the same region.
   If the affected EIP can be pinged from another ECS in the same region, the virtual network is functional. In such a case, contact customer service for technical support.

5. Check the ECS.
   a. Check whether the ECS has multiple NICs. If the ECS has multiple NICs and the EIP is bound to an extension NIC, configure a policy route in the ECS.
b. Log in to the ECS and check whether the target NIC has been configured and obtained a private IP address. If the ECS cannot be logged in using the preset password, contact customer service to obtain the default image password for login.

c. If the NIC has not been correctly configured, contact customer service for troubleshooting.

d. Run the following command to check whether the CPU usage of the ECS is high:

```
top
```

e. If the ECS runs Linux, run the following command to check whether the ECS is restricted by security rules:

```
iptables-save
```

f. If the ECS runs Windows, check whether the ECS is restricted by firewall rules.

**Related Operations**

If the host cannot be found after you ping a domain name, this issue may be caused by slow response from the DNS server. In such a case, see Troubleshooting Slow Access of a Website Outside the Chinese Mainland over an ECS.

### 14.1.4 Why Can I Remotely Access an ECS But Cannot Ping It?

**Symptom**

An ECS can be remotely accessed, but the EIP bound to it cannot be pinged.

**Possible Causes**

A desired inbound rule is not added for the security group, and ICMP is not enabled.

**Solution**

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. On the **Elastic Cloud Server** page, click the name of the target ECS.

   The page providing details about the ECS is displayed.
4. Click the **Security Groups** tab, expand the information of the security group, and click the security group ID.
5. On the **Inbound Rules** tab of the **Security Group** page, click **Add Rule**.
6. Add an inbound rule for the security group and enable ICMP.
   - **Protocol/Application**: ICMP
   - **Source**: IP address 0.0.0.0/0
14.1.5 What Do I Do If Outbound Access Through TCP Port 25 Is Restricted?

**Symptom:** TCP port 25 cannot be used to access an external address. For example, you cannot run the `Telnet smtp.***.com 25` command.

**Cause:** Outbound traffic from TCP port 25 is denied by default.

**Solution:** Request to allow outbound traffic from TCP port 25.

---

**NOTICE**

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

1. On the **Create Service Ticket** page, choose **Products > Elastic Cloud Server**. For details about how to submit a service ticket, see [Submitting a Service Ticket](#).
2. Click **Open Port 25** under **Select Subtype** and click **Create Service Ticket**.

   ![Creating a service ticket](image)

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

---

14.2 DNS and NTP Configurations

14.2.1 How Can I Configure the NTP and DNS Servers for an ECS?

**For Linux OSs**

Take the NTP and DNS servers running SUSE as an example.

**Step 1** Configure the NTP server for the ECS.

1. Log in to the ECS.
2. Run the following command to switch to user **root**:
   
   ```bash
   sudo su -
   ```
3. Run the following command to edit the **ntp.conf** configuration file:
   
   ```bash
   vim /etc/ntp.conf
   ```
4. Add the following statement to configure the NTP server:

   ```
   server Domain name or IP address of the NTP server
   ```

   An example is provided as follows:

   ```
   server 192.168.56.1
   ```

5. Run the following command to start the NTP service upon system restart:

   ```
   service ntp restart
   ```

6. Run the following command to check the status of the NTP server:

   ```
   service ntp status
   ```

**Step 2** Configure the DNS server for the ECS.

1. Log in to the ECS.
2. Run the following command to switch to user `root`:

   ```
   sudo su -
   ```

3. Run the following command to edit the `resolv.conf` configuration file:

   ```
   vi /etc/resolv.conf
   ```

4. Add the following statement to configure the DNS server:

   ```
   nameserver = IP addresses of the DNS servers
   ```

   An example is provided as follows:

   ```
   nameserver = 8.8.8.8
   nameserver = 4.4.4.4
   ```

   **NOTE**

   The IP addresses of the DNS servers must be the same as those in the VPC subnet. Otherwise, the DNS modification cannot persistently take effect.

5. Run the following command to restart the network:

   ```
   rcnetwork restart
   ```

   ```
   service network restart
   ```

   ```
   /etc/init.d/network restart
   ```

--- End

**For Windows OSs**

Take an ECS running Windows 7 OS as an example.

**Step 1** Log in to the ECS as user **Administrator**.

**Step 2** Enable the local area connection.

1. In the lower right corner of the taskbar, click the network connection icon.
2. Click **Open Network and Sharing Center**.
3. In the navigation pane on the left, click **Change adapter settings**.

**Step 3** Configure the DNS server for the ECS.
1. Double-click **Local Area Connection**.
2. Click **Properties** in the lower left corner, as shown in **Figure 14-7**.

**Figure 14-7** Local area connection

3. Select **Internet Protocol (TCP/IP)** and click **Properties**, as shown in **Figure 14-8**.

**Figure 14-8** Selecting a protocol type

4. Select **Use the following DNS server addresses** and set the IP addresses of the DNS servers as prompted, as shown in **Figure 14-9**.
Figure 14-9 Setting the IP addresses of the DNS servers

![Internet Protocol (TCP/IP) Properties](image)

**Step 4** Configure the NTP server for the ECS.

1. Press **Win+R** to start the **Open** text box.
2. Enter **regedit** and click **OK**.
   The Registry Editor window is displayed.
3. Modify the registry entries.
   - In file `HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W32Time \ TimeProviders \ NtpClient`, set the value of **Enabled** to 1, indicating that the NTP server is used.
   - In file `HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W32Time \ TimeProviders \ NtpServer`, set the value of **Enabled** to 0, indicating that the NTP server is stopped.
   - In file `KEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W32Time \ Parameters`, set the value of **NtpServer** to `192.168.1.35` and that of **TYPE** to **NTP**.
   - In file `HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W32Time \ TimeProviders \ NtpClient`, set the value of **SpecialPollInterval** to 60 and that of **Base** to **Decimal**, indicating the clock synchronization cycle is 60s.
   - In file `HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W32Time \ config`, set the values of **MaxPosPhaseCorrection** and **MaxNegPhaseCorrection** to `ffffffff` and that of **Base** to **Hexadecimal**.
4. Press **Win+R** to start the **Open** text box.
5. Enter **services.msc** and click **OK**.
   The **Service** window is displayed.
6. View the service named **Windows Time** and set the **Start Type** to **Automatic** to synchronize time from the NTP server.
7. Press **Win+R** to start the **Open** text box.
8. Run the following command to restart the Windows Time service:
   ```plaintext
   net stop w32time
   net start w32time
   ```
Elastic Cloud Server
FAQs

14 Network Configurations

9. Manually change the client time to make it different from the server time. One minute later, check whether the client time is the same as the server time. If yes, the time is synchronized.

---End

14.2.2 Does HUAWEI CLOUD Provide the NTP Server and How Can I Install It?

Yes. HUAWEI CLOUD provides the NTP server, and it can only be installed and used on the ECSs that are purchased on the HUAWEI CLOUD management console.

You can install the NTP server provided on the management console or other NTP servers. The installation procedures are the same. This section describes how to install the NTP server provided on the management console on an ECS.

Background

If you use the NTP server provided by HUAWEI CLOUD, you also need to use the DNS server. Table 14-3 lists the NTP and DNS servers provided by HUAWEI CLOUD in different regions.

Table 14-3 NTP servers

<table>
<thead>
<tr>
<th>Region</th>
<th>NTP Server IP Address</th>
<th>DNS Server IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN North</td>
<td>ntp.myhuaweicloud.com</td>
<td>100.125.1.250</td>
</tr>
<tr>
<td>CN East</td>
<td>ntp.myhuaweicloud.com</td>
<td>100.125.17.29</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100.125.135.29</td>
</tr>
<tr>
<td>CN South</td>
<td>ntp.myhuaweicloud.com</td>
<td>100.125.1.250</td>
</tr>
<tr>
<td>CN Northeast</td>
<td>ntp.myhuaweicloud.com</td>
<td>100.125.1.250</td>
</tr>
<tr>
<td>AP-Hong-Kong</td>
<td>ntp.myhuaweicloud.com</td>
<td>100.125.1.250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100.125.3.250</td>
</tr>
<tr>
<td>AP-Bangkok</td>
<td>ntp.myhuaweicloud.com</td>
<td>100.125.1.250</td>
</tr>
</tbody>
</table>

Linux

Step 1 Check whether the IP address of the DNS server is correct on the ECS.

1. Log in to the Linux ECS.
2. Run the following command to open the resolv.conf file:

   vi /etc/resolv.conf

3. Check whether the nameserver value in the file is the same as the IP address of the DNS server provided in Table 14-3.
   a. If yes, go to Step 3.
   b. If no, go to Step 2.
Step 2  (Optional) Configure the DNS server for the ECS.
   1. Log in to the Linux ECS.
   2. Run the following command to edit the resolv.conf configuration file:
      `vi /etc/resolv.conf`
   3. Add the following statement to configure the DNS server:
      `nameserver IP address of the DNS server`
      An example is provided as follows:
      Take the CN North region as an example. Add the following statement:
      nameserver 100.125.1.250

Step 3  Configure the NTP server for the ECS.
   1. Log in to the Linux ECS.
   2. Run the following command to edit the ntp.conf configuration file:
      `vim /etc/ntp.conf`
   3. Add the following statement to configure the NTP server:
      `server Domain name of the NTP server`
      An example is provided as follows:
      server ntp.myhuaweicloud.com
   4. Run the following command to start the NTP service upon system restart:
      For SUSE:
      `service ntp restart`
      For Euler and CentOS:
      `systemctl restart ntpd`

   ☑ NOTE
   Run the required command based on the OS running on the ECS.
   5. Run the following command to check whether the time on the NTP server has been
      synchronized with that on the upper-layer NTP server:
      `ntpq -p`
      If "*" is displayed, the time has been synchronized.

   ☑ NOTE
   It takes several minutes to perform NTP time synchronization for the first time.
   6. Set the automatic startup of the NTP service.
      For SUSE:
      `chkconfig ntp on`
      For Euler and CentOS:
      `chkconfig ntpd on`

----End

Windows

Take an ECS running Windows 7 OS as an example.

Step 1  Log in to the ECS as user Administrator.
Step 2 Enable the local area connection.
1. In the lower right corner of the taskbar, click the network connection icon.
2. Click **Open Network and Sharing Center**.
3. In the navigation pane on the left, click **Change adapter settings**.

Step 3 Configure the DNS server for the ECS.
1. Double-click **Local Area Connection**.
2. Click **Properties** in the lower left corner.

**Figure 14-10** Local area connection

3. Select **Internet Protocol (TCP/IP)** and click **Properties**.
4. Select **Use the following DNS server addresses** and set the IP addresses of the DNS servers as prompted. Set **Preferred DNS server** to the IP address of the DNS server provided in **Table 14-3**.

**Figure 14-12** Setting the IP addresses of the DNS servers

---

**Step 4** Configure the NTP server for the ECS.

1. Press **Win+R** to start the **Open** text box.
2. Enter **regedit** and click **OK**.
The Registry Editor window is displayed.
3. Modify the registry entries.
   - In **HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ W32Time \ TimeProviders \ NtpClient**, set the value of **Enabled** to **1**, indicating that the NTP server is used.
In **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer**, set the value of **Enabled** to 0, indicating that the NTP server is stopped.

In **KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters**, set the value of **NtpServer** to `ntp.myhuaweicloud.com` and that of **TYPE** to **NTP**.

In **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient**, set the value of **SpecialPollInterval** to 60 and that of **Base** to **Decimal**, indicating the clock synchronization cycle is 60s.

In **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\config**, set the values of **MaxPosPhaseCorrection** and **MaxNegPhaseCorrection** to `ffffffff` and that of **Base** to **Hexadecimal**.

4. Press **Win+R** to start the **Open** text box.
5. Enter **services.msc** and click **OK**.
   The **Service** window is displayed.
6. View the service named **Windows Time** and set the **Start Type** to **Automatic** to synchronize time from the NTP server.
7. Press **Win+R** to start the **Open** text box.
8. Run the following commands to restart the Windows Time service:
   ```
   net stop w32time
   net start w32time
   ```
9. Manually change the time on the client to make it different from that on the NTP server. One minute later, check whether the time on the client is the same as that on the NTP server. If yes, the time is synchronized.

----
End

**Follow-up Procedure**

After the ECS is restarted, the DNS configuration is reset, and its IP address is changed to the IP address of the DNS server in the VPC subnet. Therefore, before restarting the ECS, check whether the DNS configuration in the VPC subnet is the same as the target DNS configuration. If they are different, change the DNS configuration in the VPC subnet. For details, see **Modifying a Subnet**.

### 14.2.3 Configuring DNS

A DNS server is used to resolve domain names of file systems. For details about DNS server IP addresses, see **What Are the Private DNS Server Addresses Provided by the DNS Service?**

By default, the IP address of the DNS server used to resolve domain names of file systems is automatically configured on ECSs when creating ECSs. No manual configuration is needed except when the resolution fails due to a change in the DNS server IP address.

Windows 2012 is used as an example in the operation procedures for Windows.

#### Procedure (Linux)

**Step 1** Log in to the ECS as user **root**.

**Step 2** Run the `vi /etc/resolv.conf` command to edit the `/etc/resolv.conf` file. Add the DNS server IP address above the existing nameserver information. See **Figure 14-13**.
**Figure 14-13 Configuring DNS**

![Configuring DNS](image)

The format is as follows:

```
nameserver 100.125.1.250
```

**Step 3** Press Esc, input :wq, and press Enter to save the changes and exit the vi editor.

**Step 4** Run the following command to check whether the IP address is successfully added:

```
cat /etc/resolv.conf
```

**Step 5** Run the following command to check whether an IP address can be resolved from the file system domain name:

```
nslookup File system domain name
```

**NOTE**

Obtain the file system domain name from the file system shared path.

**Step 6** (Optional) In a network environment of the DHCP server, edit the `/etc/resolv.conf` file to prevent the file from being automatically modified upon an ECS startup, and prevent the DNS server IP address added in **Step 2** from being reset.

1. Run the following command to lock the file:

```
chattr +i /etc/resolv.conf
```

**NOTE**

Run the `chattr -i /etc/resolv.conf` command to unlock the file if needed.

2. Run the following command to check whether the editing is successful:

```
lsattr /etc/resolv.conf
```

If a command output similar to **Figure 2** is displayed, the file has been locked.

**Figure 14-14 A locked file**

```
[-rw-------.----------] 2019-01-21 12:34 /etc/resolv.conf
```

----End----

**Procedure (Windows)**

**Step 1** Go to the ECS console and log in to the ECS running Windows 2012.

**Step 2** Click This PC in the lower left corner.
Step 3  On the page that is displayed, right-click **Network** and choose **Properties** from the drop-down list. The **Network and Sharing Center** page is displayed, as shown in Figure 14-15. Click **Local Area Connection**.

Figure 14-15 Page for network and sharing center

![Network and Sharing Center](image)

Step 4  In the **Activity** area, select **Properties**. See Figure 14-16.

Figure 14-16 Local area connection

![Local area connection](image)

Step 5  In the **Local Area Connection Properties** dialog box that is displayed, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. See Figure 14-17.
Step 6  In the dialog box that is displayed, select **Use the following DNS server addresses**: and configure DNS, as shown in Figure 14-18. The DNS server IP address is 100.125.1.250. After completing the configuration, click **OK**.
14.3 NICs

14.3.1 Will NICs Added to an ECS Start Automatically?

Based on test results, if the ECS runs CentOS 7.0, NICs added to the ECS cannot start automatically. You must start the NICs manually.

14.3.2 How Can I Check Whether the Network Communication Between Two ECSs Equipped with an InfiniBand NIC Driver Is Normal?

For high-performance H2 ECSs equipped with an InfiniBand NIC driver (InfiniBand ECSs for short), perform the following operations to check whether the driver installation is successful and whether the network communication between the ECSs is normal.

**NOTE**

During the check, if your ECS has no command tool installed, such as ibstat, obtain the tool from the installation package for the InfiniBand NIC driver and install the tool.

**Step 1** Check whether the NICs of the InfiniBand ECSs are functional.

1. Log in to an ECS.
2. Run the following command to check whether the NIC is functional:
   ```
   ibstat
   ```
   - If yes, go to **Step 2**.
   - If no, contact technical support.

**Step 2** Check whether the network communication between two InfiniBand ECSs is normal.

1. Log in to one InfiniBand ECS and run the following command:
   ```
   ib_write_bw -x 0 --pkey_index 0
   ```
2. Log in to the other InfiniBand ECS and run the following command:
   ```
   ib_write_bw -x 0 --pkey_index 0ip_addr
   ```
   In the preceding command, `ip_addr` is the NIC IP address of the first InfiniBand ECS.
3. Check whether the terminal display is correct.
Figure 14-19 Normal network communication

− If the terminal display is shown in Figure 14-19, the network communication between the two InfiniBand ECSs is normal.
− If the network communication is abnormal, contact technical support.

---End

14.3.3 How Can I Manually Configure an IP Address for an InfiniBand NIC?

IP over InfiniBand (IPoIB) allows IP data transmission over InfiniBand. For SUSE high-performance H2 and HL1 ECSs, if IPoIB is required, you must manually configure an IP address for the InfiniBand NIC after installing the InfiniBand NIC driver.

Prerequisites

The InfiniBand NIC driver has been installed on the high-performance H2 or HL1 ECSs.

Background

To prevent IP address conflict of the InfiniBand NICs configured for the ECSs of a tenant, determine the IP address to be configured for an InfiniBand NIC according to the IP addresses available in the VPC. The method is as follows:

For example, if the first two eight-bits of the IP address (specified by IPADDR) to be configured for the InfiniBand NIC are consistently 169.254, the latter two eight-bits must be the same as those of the eth0 IP address, and the subnet mask must be the same as that of the eth0 NIC.

An example is provided as follows:

If the IP address of the eth0 NIC is 192.168.0.100/24, the IP address to be configured for the InfiniBand NIC is 169.254.0.100/24.

Procedure

1. Log in to the ECS.
2. Run the following command to switch to user root:

   sudo su -
3. Run the following command to edit the `/etc/sysconfig/network/ifcfg-ib0` file:
   
   ```
   vi /etc/sysconfig/network/ifcfg-ib0
   ```

4. Enter the following information:
   
   ```
   DEVICE=ib0
   BOOTPROTO=static
   IPADDR=IP address to be configured for the InfiniBand NIC
   NETMASK=Subnet mask
   STARTMODE=auto
   ```

   **NOTE**
   
   For instructions about how to obtain the IP address and subnet mask for an InfiniBand NIC, see Background.

5. Run the following command to restart the network for the configuration to take effect:
   
   ```
   service network restart
   ```

### 14.3.4 How Can I Handle the Issue that a Windows 7 ECS Equipped with an Intel 82599 NIC Reports an Error in SR-IOV Scenarios?

**Symptom**

When the 20.4.1 driver package downloaded at Intel website https://downloadcenter.intel.com/search?keyword=Intel++Ethernet+Connections+CD was installed in a Windows 7 64bit ECS with SR-IOV passthrough enabled, the system displayed the message "No Intel adapter found".

**Cause Analysis**

The OS identifies an Intel 82599 passthrough NIC without a driver installed as an Ethernet controller. When the 20.4.1 driver package was installed, the OS did not identify the Intel NIC, leading to the error.

**Solution**

Run `Autorun.exe` in the folder where the 20.4.1 driver package is stored. Install a driver on the NIC before installing the driver package so that the NIC can be identified as an Intel 82599 virtual function (VF) device by the OS. Use either of the following methods to install the driver:

- **Method 1: Update the version.**
  a. Download the 18.6 driver package at the Intel website.
  b. Run `Autorun.exe`.
  c. Run `Autorun.exe` in the folder where the 20.4.1 driver package is stored to update the driver.

- **Method 2: Use the device manager.**
  a. Start the Windows resource manager. Right-click **Computer** and choose **Manage** from the shortcut menu. In the **Device Manager** window, locate the NIC. When the NIC has no driver installed, the NIC locates in **Other devices** and is named **Ethernet Controller**.
b. Right-click **Ethernet Controller** and choose **Update Driver Software**.
c. Click **Browse**, select the path where the driver package is stored, and click **Next**.
d. Locate the NIC in **Network Adapter** of **Device Manager**.
e. Run **Autorun.exe** to install the 20.4.1 driver package.

### 14.4 Routing

#### 14.4.1 How Can I Add a Static Route to a CentOS 6.5 OS?

**Scenarios**

After the system restarts, non-static routes are lost, affecting network availability. To prevent this issue from occurring, you must add static routes to the system.

**Procedure**

The following section uses a CentOS 6.5 OS as an example.

1. Log in to the ECS.
2. Create or modify the static route configuration file.
   If the **static-routes** configuration file is not in the */etc/sysconfig/* directory, create this file. If such a file is available, run the following command to add a static route into this file:
   ```
   any net 192.168.2.0 netmask 255.255.255.0 gw 192.168.1.34
   ```
   After the configuration, save and exit the file. The following figure shows the modified file content.

3. Run the following command to restart the network service to make the static route take effect:
   ```
   service network restart
   ```

4. Run the following command to view routes:
   ```
   route -n
   ```
14.5 Website or Application Access Failures

14.5.1 What Should I Do If My Windows ECS Cannot Access the Internet?

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

Possible Causes

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

Solution

Perform the following operations for troubleshooting:

1. Check whether the ECS has an EIP bound. If not, bind an EIP to it and check whether the fault is rectified.
   For instructions about how to bind an EIP, see Binding an EIP.
2. Check whether the ECS can access the Internet with the EIP bandwidth.
   If accessing the Internet failed, check whether the EIP bandwidth exceeds the bandwidth limit.
   For details, see How Do I Check Whether the Bandwidth Exceeds the Limit?
   For instructions about how to increase the bandwidth, see Changing an EIP Bandwidth.
3. Check whether the fault occurs on specific IP addresses. If so, these IP addresses may be blocked by the ISP.
4. On the CLI of the ECS, run the `ipconfig /all` command to check whether the NIC configuration is correct. Run the `ncpa.cpl` command to start Network and Sharing Center and check whether the NIC is functional.
5. Run the `route print` command to obtain the routing table of the ECS and check whether the default route of 0.0.0.0 designates to the default gateway.
6. Run the `ping` command to check whether data can be exchanged between the ECS and the gateway.
7. Run the `ping` command to obtain the IP address of the DNS server.
   Compare the time required for pinging the DNS server and the time for pinging a specific IP address, and determine whether the DNS server is running properly.
8. Run the `netstat` command to detect SYN-SENT, CLOSE_WAIT, or FIN_WAIT.
If such information is detected, port resources are exhausted. This issue is generally caused by a software bug. To handle this issue, rectify the fault and restart the ECS.

9. Check whether the security group of the ECS is correctly configured. If a whitelist is configured for the outbound rules of the security group, the network traffic in the outbound direction is permitted. As shown in Figure 14-20, all network traffic in the outbound direction is permitted.

For instructions about how to permit a protocol or port, see Configuring Security Group Rules.

Figure 14-20 Permitting all network traffic in the outbound direction

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

If the fault is rectified, check the firewall rules.

11. Disable or uninstall the third-party antivirus software on the ECS, and check whether the fault is rectified.

To precisely locate the fault, use Wireshark or tcpdump to obtain the IP packets transmitted from and received by the affected NIC. Analyze the obtained packets for the clues of DNS resolution, ARP resolution, or TCP connection failures.

14.5.2 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.

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.
b. Run the `ifconfig` or `ip addr` command to obtain the ECS IP address.

**Figure 14-21 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:ff:fe00:fe24:1e7f prefixlen 64 scopeid 0x2a0x24:1e7f
    ether fa:16:3e:24:1e:7f txqueuelen 1000 (Ethernet)
    RX packets 227259083 bytes 21176287838 (19.7 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 149514514 bytes 27269532634 (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 fe80:ff:fe00:fe24:1e7f prefixlen 64 scopeid 0x2a0x24:1e7f
    ether 00:16:3e:24:1e:7f txqueuelen 0 (Loopback)
    RX packets 14 bytes 1058 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14 bytes 1058 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

**Figure 14-22 ip addr command output**

```
[root@elb-mq02 ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       validlink forever preferred_lifeforever
    inet6 ::1/128 scope host
       validlink forever preferred_lifeforever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc htb state UP qlen 1000
    link/ether 00:16:3e:24:1e:7f brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.120/24 brd 192.168.2.255 scope global noprefixroute dynamic eth0
       valid_lifef 10.000ms preferred_lifef 10.000ms
    inet6 fe80:ff:fe00:fe24:1e7f%eth0/64 scope global link
       valid_lifef 10.000ms preferred_lifef 10.000ms
```

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

**Figure 14-23 route -n command output**

```
[root@elb-mq02 ~]# route -n
Kernel IP routing table
Destination Gateway      Genmask Flags Metric Ref  Use Iface
default                 0.0.0.0     UG    100      0        0 eth0
102.168.2.0/24          192.168.0.1  255.255.255.0  U       100        0 eth0
```

- **Windows**
  - a. Run `cmd.exe`.
  - b. Run the `ipconfig` command to obtain the ECS IP address.
c. Run the `route print` command to obtain the gateway in the routing table.

**Figure 14-25 route print** command output

<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 acknowledgment 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>FIN-WAIT-2</td>
<td>Waits for the network disconnection request from a</td>
<td>The network has been disconnected and requires 12 minutes to automatically recover.</td>
</tr>
<tr>
<td></td>
<td>remote TCP server.</td>
<td></td>
</tr>
<tr>
<td>SYN-SENT</td>
<td>Waits for the matched network connection request after</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></td>
<td>a network connection request is sent.</td>
<td></td>
</tr>
<tr>
<td>FIN-WAIT-1</td>
<td>Waits for the remote TCP disconnection request, or the</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>
<tr>
<td></td>
<td>acknowledgement for previous disconnection request.</td>
<td></td>
</tr>
</tbody>
</table>

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

  ![Figure 14-26 Checking port listening status](image)

- **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 14-27 Checking the TermService PID](image)

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

  ![Figure 14-28 Checking the PID used by the process](image)
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:
     ```
     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.

14.5.3 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 Private DNS server addresses.

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, `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 are delivered with Linux.

   `curl -I Target website`

   For example, `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, `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 detection 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.
14.6 Others

14.6.1 How Can I Obtain the MAC Address of My ECS?

This section describes how to obtain the MAC address of an ECS.

NOTE

The MAC address of an ECS cannot be changed.

Linux

1. Log in to the Linux ECS.
2. Run the following command to view the MAC address of the ECS:
   ```bash
   ifconfig
   ```

   ![ifconfig](image)

Windows

1. Press `Win+R` to start the Open text box.
2. Enter `cmd` and click OK.
3. Run the following command to view the MAC address of the ECS:
   ```bash
   ipconfig /all
   ```

   ![ipconfig](image)

14.6.2 How Can I Test Network Performance?

This section describes how to use netperf and iperf3 to test network performance between ECSs. The operations include test preparations, TCP bandwidth test, UDP PPS test, and latency test.
Background

- Tested ECS: an ECS that is tested for network performance. Such an ECS functions as the client (TX end) or server (RX end) in netperf tests.
- Auxiliary ECS: an ECS that is used to exchange test data with the tested ECS. The auxiliary ECS functions as the client (TX end) or server (RX end) in netperf tests.
- Table 14-4 and Table 14-5 list common test tool parameters.

<table>
<thead>
<tr>
<th>Table 14-4 Common netperf parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>-p</td>
</tr>
<tr>
<td>-H</td>
</tr>
<tr>
<td>-t</td>
</tr>
<tr>
<td>-l</td>
</tr>
<tr>
<td>-m</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 14-5 Common iperf3 parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>-p</td>
</tr>
<tr>
<td>-c</td>
</tr>
<tr>
<td>-u</td>
</tr>
<tr>
<td>-b</td>
</tr>
<tr>
<td>-t</td>
</tr>
<tr>
<td>-l</td>
</tr>
<tr>
<td>-A</td>
</tr>
</tbody>
</table>

In this section, the maximum number of 16 vCPUs is used as an example for each ECS. If an ECS has 8 vCPUs, the -A value ranges from 0 to 7.

Test Preparations

Step 1 Prepare ECSs.

Ensure that both type and specifications of the tested ECS and auxiliary ECSs are the same. In addition, these ECSs are deployed in the same ECS group with anti-affinity enabled.

<table>
<thead>
<tr>
<th>Table 14-6 Preparations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
</tr>
</tbody>
</table>

2019-12-02
### Step 2

Install the netperf, iperf3, and sar test tools on both the tested ECS and auxiliary ECSs.

Table 14-7 lists the procedures for installing these tools.

#### Table 14-7 Installing test tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>netperf</td>
<td>1. Run the following command to install gcc:</td>
</tr>
<tr>
<td></td>
<td>yum -y install unzip gcc gcc-c++</td>
</tr>
<tr>
<td></td>
<td>2. Run the following command to download the netperf installation</td>
</tr>
<tr>
<td></td>
<td>package:</td>
</tr>
<tr>
<td></td>
<td>wget --no-check-certificate</td>
</tr>
<tr>
<td></td>
<td><a href="https://github.com/HewlettPackard/netperf/archive/netperf-2.7.0.zip">https://github.com/HewlettPackard/netperf/archive/netperf-2.7.0.zip</a></td>
</tr>
<tr>
<td></td>
<td>-O netperf-2.7.0.zip</td>
</tr>
<tr>
<td></td>
<td>3. Run the following commands to decompress the installation package</td>
</tr>
<tr>
<td></td>
<td>and install netperf:</td>
</tr>
<tr>
<td></td>
<td>unzip netperf-2.7.0.zip</td>
</tr>
<tr>
<td></td>
<td>cd netperf-netperf-2.7.0/</td>
</tr>
<tr>
<td></td>
<td>./configure &amp;&amp; make &amp;&amp; make install</td>
</tr>
<tr>
<td>iperf3</td>
<td>1. Run the following command to download the iperf3 installation package:</td>
</tr>
<tr>
<td></td>
<td>wget --no-check-certificate</td>
</tr>
<tr>
<td></td>
<td><a href="https://codeload.github.com/esnet/iperf/zip/master">https://codeload.github.com/esnet/iperf/zip/master</a> -O iperf3.zip</td>
</tr>
<tr>
<td></td>
<td>2. Run the following commands to decompress the installation package</td>
</tr>
<tr>
<td></td>
<td>and install iperf3:</td>
</tr>
<tr>
<td></td>
<td>unzip iperf3.zip</td>
</tr>
<tr>
<td></td>
<td>cd iperf-master/</td>
</tr>
<tr>
<td></td>
<td>./configure &amp;&amp; make &amp;&amp; make install</td>
</tr>
<tr>
<td>sar</td>
<td>Run the following command to install sar:</td>
</tr>
<tr>
<td></td>
<td>yum -y install sysstat</td>
</tr>
</tbody>
</table>

#### Step 3

Enable NIC multi-queue.

Perform the following operations on both tested ECS and auxiliary ECSs.

1. Run the following command to check the number of queues supported by the ECSs:
   ```
   ethtool -l eth0 | grep -i Pre -A 5 | grep Combined
   ```
2. Run the following command to enable NIC multi-queue:
ethtool -L eth0 combined $X$

In the preceding command, $X$ is the number of queues obtained in Step 3.1.

----End

TCP Bandwidth Test (Using netperf)

Perform the test on multiple flows. This section uses 16 flows as an example, which are evenly distributed to eight ECSs.

**Step 1** Test the TCP TX bandwidth.

1. Run the following commands on all auxiliary ECSs to start the netserver process:

   ```bash
   netserver -p 12001
   netserver -p 12002
   ```

   In the preceding commands, `-p` specifies the listening port.

2. Start the netperf process on the tested ECS and specify a netserver port for each auxiliary ECS. For details about common netperf parameters, see Table 14-4.

   ```bash
   netperf -H 192.168.2.11 -p 12001 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.11 -p 12002 -t TCP_STREAM -l 300 --m 1440 &
   ```

   The IP address is for the first auxiliary ECS.

   ```bash
   netperf -H 192.168.2.12 -p 12001 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.12 -p 12002 -t TCP_STREAM -l 300 --m 1440 &
   ```

   The IP address is for the second auxiliary ECS.

   ```bash
   netperf -H 192.168.2.13 -p 12001 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.13 -p 12002 -t TCP_STREAM -l 300 --m 1440 &
   ```

   The IP address is for the third auxiliary ECS.

   ```bash
   netperf -H 192.168.2.14 -p 12001 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.14 -p 12002 -t TCP_STREAM -l 300 --m 1440 &
   ```

   The IP address is for the fourth auxiliary ECS.

   ```bash
   netperf -H 192.168.2.15 -p 12001 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.15 -p 12002 -t TCP_STREAM -l 300 --m 1440 &
   ```

   The IP address is for the fifth auxiliary ECS.

   ```bash
   netperf -H 192.168.2.16 -p 12001 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.16 -p 12002 -t TCP_STREAM -l 300 --m 1440 &
   ```

   The IP address is for the sixth auxiliary ECS.

   ```bash
   netperf -H 192.168.2.17 -p 12001 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.17 -p 12002 -t TCP_STREAM -l 300 --m 1440 &
   ```

   The IP address is for the seventh auxiliary ECS.

   ```bash
   netperf -H 192.168.2.18 -p 12001 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.18 -p 12002 -t TCP_STREAM -l 300 --m 1440 &
   ```

   The IP address is for the eighth auxiliary ECS.

**Step 2** Test the TCP RX bandwidth.

1. Start the netserver process on the tested ECS.
## The port number is for the first auxiliary ECS.
netserver -p 12001
netserver -p 12002
## The port number is for the second auxiliary ECS.
netserver -p 12003
netserver -p 12004
## The port number is for the third auxiliary ECS.
netserver -p 12005
netserver -p 12006
## The port number is for the fourth auxiliary ECS.
netserver -p 12007
netserver -p 12008
## The port number is for the fifth auxiliary ECS.
netserver -p 12009
netserver -p 12010
## The port number is for the sixth auxiliary ECS.
netserver -p 12011
netserver -p 12012
## The port number is for the seventh auxiliary ECS.
netserver -p 12013
netserver -p 12014
## The port number is for the eighth auxiliary ECS.
netserver -p 12015
netserver -p 12016

2. Start the netperf process on all auxiliary ECSs.
   Log in to auxiliary ECS 1.
   netperf -H 192.168.2.10 -p 12001 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.10 -p 12002 -t TCP_STREAM -l 300 --m 1440 &
   Log in to auxiliary ECS 2.
   netperf -H 192.168.2.10 -p 12003 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.10 -p 12004 -t TCP_STREAM -l 300 --m 1440 &
   Log in to auxiliary ECS 3.
   netperf -H 192.168.2.10 -p 12005 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.10 -p 12006 -t TCP_STREAM -l 300 --m 1440 &
   Log in to auxiliary ECS 4.
   netperf -H 192.168.2.10 -p 12007 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.10 -p 12008 -t TCP_STREAM -l 300 --m 1440 &
   Log in to auxiliary ECS 5.
   netperf -H 192.168.2.10 -p 12009 -t TCP_STREAM -l 300 --m 1440 &
   netperf -H 192.168.2.10 -p 12010 -t TCP_STREAM -l 300 --m 1440 &
   Log in to auxiliary ECS 6.
   netperf -H 192.168.2.10 -p 12011 -t TCP_STREAM -l 300 --m 1440 &
netperf -H 192.168.2.10 -p 12012 -t TCP_STREAM -l 300 --m 1440 &
Log in to auxiliary ECS 7.
netperf -H 192.168.2.10 -p 12013 -t TCP_STREAM -l 300 --m 1440 &
netperf -H 192.168.2.10 -p 12014 -t TCP_STREAM -l 300 --m 1440 &
Log in to auxiliary ECS 8.
netperf -H 192.168.2.10 -p 12015 -t TCP_STREAM -l 300 --m 1440 &
netperf -H 192.168.2.10 -p 12016 -t TCP_STREAM -l 300 --m 1440 &

Step 3 Analyze the test result.

After the test is complete, the output of the netperf process on one TX end is shown in Figure 14-29. The final result is the sum of the test results of the netperf processes on all TX ends.

Figure 14-29 Output of the netperf process on one TX end

Recv  Send  Send
Socket  Socket  Message  Elapsed
Size   Size   Size   Time   Throughput
bytes  bytes  bytes  secs.  10^6bits/sec

- TX buffer  Test duration  Throughput
87380  16384  1440  120.02  956.30

- RX buffer  Data packet size

NOTE
There are a large number of netperf processes. To facilitate statistics collection, you are advised to run the following command to view test data on the tested ECS using sar:
sar -n DEV 1 60

----End

UDP PPS Test (Using iperf3)

Step 1 Test the UDP TX PPS.

1. Run the following commands on all auxiliary ECSs to start the server process:
   iperf3 -s -p 12001 &
ierf3 -s -p 12002 &
   In the preceding commands, -p specifies the listening port.
2. Start the client process on the tested ECS. For details about common iperf3 parameters, see Table 14-5.
   #Auxiliary ECS 1
iperf3 -c 192.168.2.11 -p 12001 -u -b 100M -t 300 -l 16 -A 0 &
iperf3 -c 192.168.2.11 -p 12002 -u -b 100M -t 300 -l 16 -A 1 &
## Auxiliary ECS 2
iperf3 -c 192.168.2.12 -p 12001 -u -b 100M -t 300 -l 16 -A 2 &
iperf3 -c 192.168.2.12 -p 12002 -u -b 100M -t 300 -l 16 -A 3 &

## Auxiliary ECS 3
iperf3 -c 192.168.2.13 -p 12001 -u -b 100M -t 300 -l 16 -A 4 &
iperf3 -c 192.168.2.13 -p 12002 -u -b 100M -t 300 -l 16 -A 5 &

## Auxiliary ECS 4
iperf3 -c 192.168.2.14 -p 12001 -u -b 100M -t 300 -l 16 -A 6 &
iperf3 -c 192.168.2.14 -p 12002 -u -b 100M -t 300 -l 16 -A 7 &

## Auxiliary ECS 5
iperf3 -c 192.168.2.15 -p 12001 -u -b 100M -t 300 -l 16 -A 8 &
iperf3 -c 192.168.2.15 -p 12002 -u -b 100M -t 300 -l 16 -A 9 &

## Auxiliary ECS 6
iperf3 -c 192.168.2.16 -p 12001 -u -b 100M -t 300 -l 16 -A 10 &
iperf3 -c 192.168.2.16 -p 12002 -u -b 100M -t 300 -l 16 -A 11 &

## Auxiliary ECS 7
iperf3 -c 192.168.2.17 -p 12001 -u -b 100M -t 300 -l 16 -A 12 &
iperf3 -c 192.168.2.17 -p 12002 -u -b 100M -t 300 -l 16 -A 13 &

## Auxiliary ECS 8
iperf3 -c 192.168.2.18 -p 12001 -u -b 100M -t 300 -l 16 -A 14 &
iperf3 -c 192.168.2.18 -p 12002 -u -b 100M -t 300 -l 16 -A 15 &

**Step 2** Test the UDP RX PPS.

1. Start the server process on the tested ECS. For details about common iperf3 parameters, see Table 14-5.

## Auxiliary ECS 1
iperf3 -s -p 12001 -A 0 -i 60 &
iperf3 -s -p 12002 -A 1 -i 60 &

## Auxiliary ECS 2
iperf3 -s -p 12003 -A 2 -i 60 &
iperf3 -s -p 12004 -A 3 -i 60 &

## Auxiliary ECS 3
iperf3 -s -p 12005 -A 4 -i 60 &
iperf3 -s -p 12006 -A 5 -i 60 &

## Auxiliary ECS 4
iperf3 -s -p 12007 -A 6 -i 60 &
Elastic Cloud Server
FAQs

### Network Configurations

2. Start the client process on all auxiliary ECSs. For details about common iperf3 parameters, see Table 14-5.

Step 3 Analyze the test result.

Figure 14-30 shows an example of the UDP PPS test result.
There are a large number of iperf3 processes. To facilitate statistics collection, you are advised to run the following command to view test data on the tested ECS using sar:

```
sar -n DEV 1 60
```

---End

## Latency Test

**Step 1** Run the following command to start the qperf process on the tested ECS:

```
qperf &
```

**Step 2** Log in to auxiliary ECS 1 and run the following command to perform a latency test:

```
qperf 192.168.2.10 -m 64 -t 60 -vu udp_lat
```

After the test is complete, the `lat` value in the command output is the latency between ECSs.

---End

### 14.6.3 How Can I View and Modify Kernel Parameters of a Linux ECS?

This document describes common Linux kernel parameters and how to view and modify them. Modify the kernel parameters only if the parameter settings affect your services. If the parameter settings must be modified, ensure that:

- The target parameter settings meet service requirements.
- Learn the kernel parameters to be modified, which vary depending on OS versions. For details about common kernel parameters, see Table 14-8.
- Back up key ECS data before modifying kernel parameter settings.

#### Background

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>net.core.rmem_default</td>
<td>Specifies the default size (in bytes) of the window for receiving TCP data.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>net.core.rmem_max</td>
<td>Specifies the maximum size (in bytes) of the window for receiving TCP data.</td>
</tr>
<tr>
<td>net.core.wmem_default</td>
<td>Specifies the default size (in bytes) of the window for transmitting TCP data.</td>
</tr>
<tr>
<td>net.core.wmem_max</td>
<td>Specifies the maximum size (in bytes) of the window for transmitting TCP data.</td>
</tr>
<tr>
<td>net.core.netdev_max_backlog</td>
<td>Specifies the maximum number of packets that can be sent to a queue when the rate at which each network port receives packets is faster than the rate at which the kernel processes these packets.</td>
</tr>
<tr>
<td>net.core.somaxconn</td>
<td>Defines the maximum length of the listening queue for each port in the system. This parameter applies globally.</td>
</tr>
<tr>
<td>net.core.optmem_max</td>
<td>Specifies the maximum size of the buffer allowed by each socket.</td>
</tr>
<tr>
<td>net.ipv4.tcp_mem</td>
<td>Uses the TCP stack to show memory usage in memory pages (4 KB generally).</td>
</tr>
<tr>
<td></td>
<td>• The first value is the lower limit of memory usage.</td>
</tr>
<tr>
<td></td>
<td>• The second value is the upper limit of the load added to the buffer when the memory is overloaded.</td>
</tr>
<tr>
<td></td>
<td>• The third value is the upper limit of memory usage. When this value is reached, packets can be discarded to reduce memory usage. For a large BDP, increase the parameter value as needed. The unit of this parameter is memory page but not byte.</td>
</tr>
<tr>
<td>net.ipv4.tcp_rmem</td>
<td>Specifies the memory used by sockets for automatic optimization.</td>
</tr>
<tr>
<td></td>
<td>• The first value is the minimum number of bytes allocated to the socket buffer for receiving data.</td>
</tr>
<tr>
<td></td>
<td>• The second value is the default value, which is overwritten by rmem_default. The buffer size can increase to this value when the system load is not heavy.</td>
</tr>
<tr>
<td></td>
<td>• The third value is the maximum number of bytes allocated to the socket buffer for receiving data. This value is overwritten by rmem_max.</td>
</tr>
<tr>
<td>net.ipv4.tcp_wmem</td>
<td>Specifies the memory used by sockets for automatic optimization.</td>
</tr>
<tr>
<td></td>
<td>• The first value is the minimum number of bytes allocated to the socket buffer for transmitting data.</td>
</tr>
<tr>
<td></td>
<td>• The second value is the default value, which is overwritten by wmem_default. The buffer size can increase to this value when the system load is not heavy.</td>
</tr>
<tr>
<td></td>
<td>• The third value is the maximum number of bytes allocated to the socket buffer for transmitting data. This value is overwritten by wmem_max.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>allocated to the socket buffer for transmitting data. This value is overwritten by <strong>wmem_max</strong>.</td>
</tr>
<tr>
<td>net.ipv4.tcp_keepalive_time</td>
<td>Specifies the interval at which keepalive detection messages are sent in seconds for checking TCP connections.</td>
</tr>
<tr>
<td>net.ipv4.tcp_keepalive_intvl</td>
<td>Specifies the interval at which keepalive detection messages are resent in seconds when no response is received.</td>
</tr>
<tr>
<td>net.ipv4.tcp_keepalive_probes</td>
<td>Specifies the maximum number of keepalive detection messages that are sent to determine a TCP connection failure.</td>
</tr>
<tr>
<td>net.ipv4.tcp_sack</td>
<td>Enables selective acknowledgment (value 1 indicates enabled). This configuration allows the transmitter to resend only lost packets, thereby improving system performance. However, this configuration will increase the CPU usage. You are suggested to enable selective acknowledgment for WAN communication.</td>
</tr>
<tr>
<td>net.ipv4.tcp_fack</td>
<td>Enables forwarding acknowledgment for selective acknowledgment (SACK), thereby reducing congestion. You are suggested to enable forwarding acknowledgment.</td>
</tr>
<tr>
<td>net.ipv4.tcp_timestamps</td>
<td>Specifies a TCP timestamp, which will add 12 bytes in the TCP packet header. This configuration calculates RTT using RFC1323, a more precise retransmission method upon timeout than retransmission. You are suggested to use this configuration for higher system performance.</td>
</tr>
<tr>
<td>net.ipv4.tcp_window_scaling</td>
<td>Enables RFC1323-based window scaling by setting the parameter value to 1 if the TCP window is larger than 64 KB. The maximum TCP window is 1 GB. This parameter takes effect only when window scaling is enabled on both ends of the TCP connection.</td>
</tr>
<tr>
<td>net.ipv4.tcp_syncookies</td>
<td>Specifies whether to enable TCP synchronization (<strong>syncookie</strong>). This configuration prevents socket overloading when a large number of connections are attempted to set up. <strong>CONFIG_SYN_COOKIES</strong> must be enabled in the kernel for compilation. The default value is 0, indicating that TCP synchronization is disabled.</td>
</tr>
<tr>
<td>net.ipv4.tcp_tw_reuse</td>
<td>Specifies whether a <strong>TIME-WAIT</strong> socket (<strong>TIME-WAIT</strong> port) can be used for new TCP connections. <strong>NOTICE</strong> This parameter cannot be set to 1 if NAT is enabled. Otherwise, an error will occur in remote ECS logins.</td>
</tr>
<tr>
<td>net.ipv4.tcp_tw_recycle</td>
<td>Allows fast recycle of <strong>TIME-WAIT</strong> sockets. <strong>NOTICE</strong> This parameter cannot be set to 1 if NAT is enabled. Otherwise, an error will occur in remote ECS logins.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>net.ipv4.tcp_fin_timeout</td>
<td>Specifies the time (in seconds) during which a socket TCP connection that is disconnected from the local end retains in <strong>FIN-WAIT-2</strong> state. Process suspension may be caused by the disconnection from the peer end, continuous connection from the peer end, or unexpected causes.</td>
</tr>
<tr>
<td>net.ipv4.ip_local_port_range</td>
<td>Specifies local port numbers allowed by TCP/UDP.</td>
</tr>
<tr>
<td>net.ipv4.tcp_max_syn_backlog</td>
<td>Specifies the maximum number of connection requests that are not acknowledged by the peer end and that can be stored in the queue. The default value is <strong>1024</strong>. If the server is frequently overloaded, try to increase the value.</td>
</tr>
<tr>
<td>net.ipv4.tcp_low_latency</td>
<td>This option should be disabled if the TCP/IP stack is used for high throughput, low latency.</td>
</tr>
<tr>
<td>net.ipv4.tcp westwood</td>
<td>Enables the congestion control algorithm on the transmitter end to evaluate throughput and improve the overall bandwidth utilization. You are suggested to enable the congestion control algorithm for WAN communication.</td>
</tr>
<tr>
<td>net.ipv4.tcp_bic</td>
<td>Enables binary increase congestion for fast long-distance networks so that the connections with operations being performed at a rate of Gbit/s can be functional. You are suggested to enable binary increase congestion for WAN communication.</td>
</tr>
<tr>
<td>net.ipv4.tcp_max_tw_buckets</td>
<td>Specifies the number of <strong>TIME_WAIT</strong> buckets, which defaults to <strong>180000</strong>. If the number of buckets exceeds the default value, extra ones will be cleared.</td>
</tr>
<tr>
<td>net.ipv4.tcp_synack_retries</td>
<td>Specifies the number of times that SYN+ACK packets are retransmitted in <strong>SYN_RECV</strong> state.</td>
</tr>
<tr>
<td>net.ipv4.tcp_abort_on_overflow</td>
<td>When this parameter is set to <strong>1</strong>, if the system receives a large number of requests within a short period of time but fails to process them, the system will send reset packets to terminate the connections. It is recommended that you improve system processing capabilities by optimizing the application efficiency but not simply performing reset operations. Default value: <strong>0</strong></td>
</tr>
<tr>
<td>net.ipv4.route.max_size</td>
<td>Specifies the maximum number of routes allowed by the kernel.</td>
</tr>
<tr>
<td>net.ipv4.ip_forward</td>
<td>Forward packets between interfaces.</td>
</tr>
<tr>
<td>net.ipv4.ip_default_ttl</td>
<td>Specifies the maximum number of hops that a packet can pass through.</td>
</tr>
<tr>
<td>net.netfilter.nf_conntrack_tcp_timeout_established</td>
<td>Clears iptables connections that are inactive for a specified period of time.</td>
</tr>
<tr>
<td>net.netfilter.nf_conntrack_max</td>
<td>Specifies the maximum value of hash entries.</td>
</tr>
</tbody>
</table>
Viewing Kernel Parameters

- Method 1: Run the cat command in `/proc/sys` to view file content.
  
  `/proc/sys/` is a pseudo directory generated after the Linux kernel is started. The `net` folder in this directory stores all kernel parameters that have taken effect in the system. The directory tree structure is determined based on complete parameter names. For example, `net.ipv4.tcp_tw_recycle` corresponds to the `/proc/sys/net/ipv4/tcp_tw_recycle` file, and the content of the file is the parameter value.
  
  An example is provided as follows:
  
  To view the `net.ipv4.tcp_tw_recycle` value, run the following command:
  ```
  cat /proc/sys/net/ipv4/tcp_tw_recycle
  ```

- Method 2: Use the `/etc/sysctl.conf` file.

  Run the following command to view all parameters that have taken effect in the system:
  ```
  /usr/sbin/sysctl -a
  ```

```
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_tw_buckets = 4096
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_tw_recycle = 1
net.ipv4.tcp_keepalive_time = 1800
net.ipv4.tcp_fin_timeout = 30
......
net.ipv4.tcp_keepalive_time = 1200
net.ipv4.ip_local_port_range = 1024 65000
net.ipv4.tcp_max_syn_backlog = 8192
net.ipv4.tcp_rmem = 16384 174760 349520
net.ipv4.tcp_wmem = 16384 131072 262144
net.ipv4.tcp_mem = 262144 524288 1048576
......
```

Modifying Kernel Parameter Settings

- Method 1: Run the echo command in `/proc/sys` to modify the file for the target kernel parameters.

  The parameter values changed using this method take effect only during the current running and will be reset after the system is restarted. This method is used for temporary verification. To make the modification take effect permanently, see method 2.

  `/proc/sys/` is a pseudo directory generated after the Linux kernel is started. The `net` folder in this directory stores all kernel parameters that have taken effect in the system. The directory tree structure is determined based on complete parameter names. For example, `net.ipv4.tcp_tw_recycle` corresponds to the `/proc/sys/net/ipv4/tcp_tw_recycle` file, and the content of the file is the parameter value.

  An example is provided as follows:
  
  To change the `net.ipv4.tcp_tw_recycle` value to 0, run the following command:
  ```
  echo "0" > /proc/sys/net/ipv4/tcp_tw_recycle
  ```

- Method 2: Use the `/etc/sysctl.conf` file.

  The parameter values changed using this method take effect permanently.

  a. Run the following command to change the value of a specified parameter:
  ```
  /sbin/sysctl -w kernel.domainname="example.com"
  ```
An example is provided as follows:

```bash
sysctl -w net.ipv4.tcp_tw_recycle="0"
```

b. Run the following command to change the parameter value in the `/etc/sysctl.conf` file:

```bash
vi /etc/sysctl.conf
```

c. Run the following command for the configuration to take effect:

```bash
/sbin/sysctl -p
```

### 14.6.4 Can the ECSs of Different Accounts Communicate over the Intranet?

No. The ECSs of different accounts cannot communicate with each other over the intranet.

### 14.6.5 Are ECSs I Purchased Deployed in the Same Subnet?

You can customize your network to deploy the ECSs. Therefore, whether they are in the same subnet is totally up to you.
15 Security Configurations

15.1 How Does an ECS Defend Against DDoS Attacks?

When detecting an exception, the monitoring system automatically enables traffic cleaning and advises you to disable unused ports. In addition, the Anti-DDoS service is provided to prevent your ECSs from being attacked.

15.2 How Can I Disable Operation Protection?

Symptom

When I perform critical operations on my ECS with operation protection enabled, for example, deleting my ECS or modifying ECS specifications, I have to enter the password and verification code for authentication. To disable operation protection, perform the operations described in this section.

Procedure

1. Log in to the management console.
2. Move the cursor to the username in the upper right corner of the page and select Account Security Settings from the drop-down list.
3. On the **Account Security Settings** page, click the **Critical Operations** tab and click **Change**.

**Figure 15-2 Operation Protection**

4. On the **Operation Protection** page, select **Disable** and click **OK**.

**Figure 15-3 Disabling operation protection**
16.1 How Can I Create an Agency for Monitoring My ECS?

2. In the navigation pane on the left, choose Agencies and then click Create Agency in the upper right corner.
   - **Agency Name**: Enter ECS_monitor_agency.
   - **Agency Type**: Select Cloud service.
   - **Cloud Service**: This parameter is available if you select Cloud service for Agency Type. Click Select, select ECS BMS in the displayed Select Cloud Service dialog box, and click OK.
   - **Validity Period**: Select Permanent.
   - **Description**: This parameter is optional. You can enter Support ECS monitoring.
   - **Permissions**: Locate the region where your ECS resides or the sub-project of the region and click Select Policy in the Operation column. In the displayed dialog box, enter CES in the Available Policies search box. Then select CES (CES Administrator) and click OK.

**NOTE**
If the ECS belongs to a sub-project, ensure that the sub-project has the CES Administrator permission.

3. Click OK.

The operations to create an agency for monitoring the ECS are complete.

16.2 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.

16.3 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
Mem: 2.0 us, 0.3 sy, 0.0 bl, 99.5 bv, 0.0 sw, 0.0 hi, 0.1 si, 0.0 st
Total: 30008624 total, 2963399 free, 1796864 used, 739068 buffers/cache
Swap: 0 total, 0 free, 0 used, 3431904 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>0115</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>152521</td>
<td>0</td>
<td>205</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>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>kthreadd</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>kmserver</td>
</tr>
<tr>
<td>7</td>
<td>root</td>
<td>0</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>0:00.10</td>
<td>migration</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>resolv</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>7:32.10</td>
<td>runcushed</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>lrz-addr</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.
   - t: Show or hide the first line for the top information.
   - i: Show or hide the second line for tasks and the third line for CPUs.
   - m: Show or hide the fourth line for Mem and the fifth line for Swap.
   - N: Sort processes by PID in ascending or descending order.
   - P: Sort processes by CPU usage in ascending or descending order.
   - M: Sort processes by memory usage in ascending or descending order.
   - h: Show help for commands.
   - n: Set the number of processes displayed in the process list.
4. Run the `ll /proc/PID/exe` command to obtain the program file specified by a PID.

**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 Command Output]

   Press Enter.

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

   ![Top Command Output]

   • 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 Command Output]

   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.
17 Database Applications

17.1 Can a Database Be Deployed on an ECS?

Yes. There is no limitation on this operation. You can deploy a database of any type on an ECS.

17.2 Does an ECS Support Oracle Databases?

Yes. You are advised to perform a performance test beforehand to ensure that the Oracle database can meet your requirements.
## 18 Change History

<table>
<thead>
<tr>
<th>Released On</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2019-12-02 | This issue is the eighth official release.  
* Adjusted the FAQs structure. |
| 2019-11-20 | This issue is the eighth official release.  
* Added 12.3.6 How Can I Check Whether the ECSs Attached with the Same Shared SCSI Disk Are in the Same ECS Group?  
* Modified 13.1.9 What Should I Do If I Cannot Log In to My ECS Using the Reset Password?  
* Added 14.2.3 Configuring DNS. |
| 2019-09-12 | This issue is the sixth official release.  
Added the following content:  
* Added 15.2 How Can I Disable Operation Protection?  
* Added 6.1.4 What Should I Do If My Remote Login Password Was Forgotten? |
| 2019-06-30 | This issue is the fifth official release.  
Added the following content:  
* 13.1.4 Changing the Login Password on an ECS  
* 13.1.5 Resetting the Password for Logging In to a Windows ECS  
* 13.1.6 Resetting the Password for Logging In to a Linux ECS  
Modified the following content:  
* 6.4.2 What Should I Do If the System Displays a Message Indicating Invalid Credentials?  
* 14.1.3 Why Cannot an EIP Be Pinged? |
| 2019-05-30 | This issue is the fourth official release.  
Added the following content:  
* 9 File Uploading  
* 5.2.4 Can a Deleted ECS Be Restored?  
* 5.1.2 What Should I Do If the ECS Resources to Be Purchased Are Sold Out? |
<table>
<thead>
<tr>
<th>Released On</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2019-04-20 | This issue is the third official release. Added the following content:  
- 6.2.7 How Can I Change the Resolution of a Windows ECS?  
Modified the following content:  
- 14.6.2 How Can I Test Network Performance? |
| 2019-02-25 | This issue is the second official release. Added the following content:  
- 2.2.1 How Can I Use BYOL? |
| 2018-11-19 | This issue is the first official release. |