



Elastic Cloud Server

User Guide

Date 2020-11-06

Contents

1 Service Overview.....	1
1.1 What Is ECS?.....	1
1.2 ECS Advantages.....	2
1.3 ECS Application Scenarios.....	4
1.4 Notes and Constraints on Using ECSs.....	5
1.5 Instances.....	6
1.5.1 Overview.....	6
1.5.2 ECS Lifecycle.....	7
1.5.3 ECS Types.....	8
1.6 x86 ECS Specifications and Types.....	9
1.6.1 General Computing ECSs.....	9
1.6.2 General Computing-plus ECSs.....	10
1.6.3 Memory-optimized ECSs.....	12
1.6.4 Disk-intensive ECSs.....	13
1.6.5 Ultra-high I/O ECSs.....	14
1.7 Kunpeng ECS Specifications and Types.....	16
1.7.1 Kunpeng General Computing-plus ECSs.....	17
1.7.2 Kunpeng Memory-optimized ECSs.....	18
1.8 Images.....	19
1.9 EVS Disks.....	20
1.10 Network.....	21
1.11 Security.....	23
1.11.1 Cloud-Init.....	23
1.12 Region and AZ.....	24
1.13 ECS and Other Services.....	25
2 Getting Started.....	28
2.1 Creating an ECS.....	28
2.1.1 Overview.....	28
2.1.2 Step 1: Configure Basic Settings.....	28
2.1.3 Step 2: Configure Network.....	31
2.1.4 Step 3: Configure Advanced Settings.....	32
2.1.5 Step 4: Confirm.....	34
2.2 Logging In to an ECS.....	35

2.3 Initializing EVS Data Disks.....	37
2.3.1 Scenarios and Disk Partitions.....	37
2.3.2 Initializing a Windows Data Disk (Windows Server 2008).....	38
2.3.3 Initializing a Windows Data Disk (Windows Server 2016).....	45
2.3.4 Initializing a Linux Data Disk (fdisk).....	53
2.3.5 Initializing a Linux Data Disk (parted).....	59
2.3.6 Initializing a Windows Data Disk Larger Than 2 TB (Windows Server 2008).....	64
2.3.7 Initializing a Windows Data Disk Larger Than 2 TB (Windows Server 2012).....	72
2.3.8 Initializing a Linux Data Disk Larger Than 2 TB (parted).....	80
3 Instances.....	87
3.1 Creating an ECS.....	87
3.1.1 Creating the Same ECS.....	87
3.2 Viewing ECS Information.....	88
3.2.1 Viewing ECS Creation Statuses.....	88
3.2.2 Viewing Failures.....	89
3.2.3 Viewing Details About an ECS.....	89
3.2.4 Exporting ECS Information.....	90
3.3 Logging In to a Windows ECS.....	90
3.3.1 Login Overview.....	91
3.3.2 Login Using VNC.....	92
3.3.3 Login Using MSTSC.....	93
3.3.4 Logging In to a Windows ECS from a Linux Computer.....	99
3.3.5 Logging In to a Windows ECS from a Mobile Terminal.....	101
3.3.6 Logging In to Windows ECS from a Mac.....	106
3.4 Logging In to a Linux ECS.....	109
3.4.1 Login Overview.....	109
3.4.2 Login Using VNC.....	110
3.4.3 Login Using an SSH Key.....	112
3.4.4 Login Using an SSH Password.....	115
3.4.5 Logging In to a Linux ECS from a Mobile Terminal.....	116
3.5 Managing ECSs.....	126
3.5.1 Changing an ECS Name.....	126
3.5.2 Reinstalling the OS.....	127
3.5.3 Changing the OS.....	128
3.5.4 Managing ECS Groups.....	131
3.5.5 Backing Up ECS Data.....	133
3.5.6 Changing the Time Zone for an ECS.....	134
3.6 Modifying ECS vCPU and Memory Specifications.....	136
3.6.1 General Operations for Modifying Specifications.....	136
3.7 Using User Data and Metadata.....	138
3.7.1 Obtaining Metadata.....	138
3.7.2 Injecting User Data into ECSs.....	147

3.8 (Optional) Configuring Mapping Between Hostnames and IP Addresses.....	155
4 Images.....	157
4.1 Overview.....	157
4.2 Creating an Image.....	158
5 EVS Disks.....	160
5.1 Adding a Disk to an ECS.....	160
5.2 Attaching an EVS Disk to an ECS.....	161
5.3 Detaching an EVS Disk from a Running ECS.....	162
5.4 Expanding the Capacity of an EVS Disk.....	164
5.5 Expanding the Local Disks of a Disk-intensive ECS.....	165
5.6 Enabling Advanced Disk.....	166
6 Passwords and Key Pairs.....	167
6.1 Changing the Login Password on an ECS.....	167
6.2 Resetting a Login Password.....	169
6.2.1 Resetting the Password for Logging In to a Windows ECS.....	169
6.2.2 Resetting the Password for Logging In to a Linux ECS.....	171
6.3 Creating a Key Pair.....	173
6.4 Obtaining the Password for Logging In to a Windows ECS.....	179
6.5 Deleting the Initial Password for Logging In to a Windows ECS.....	180
7 NICs.....	181
7.1 Adding a NIC.....	181
7.2 Deleting a NIC.....	182
7.3 Changing a VPC.....	183
7.4 Modifying a Private IP Address.....	184
7.5 Managing Virtual IP Addresses.....	184
7.6 Enabling NIC Multi-Queue.....	185
8 Security.....	190
8.1 Security Groups.....	190
8.1.1 Overview.....	190
8.1.2 Default Security Group and Rules.....	191
8.1.3 Security Group Configuration Examples.....	192
8.1.4 Configuring Security Group Rules.....	195
8.1.5 Changing a Security Group.....	197
9 EIPs.....	198
9.1 Binding an EIP.....	198
9.2 Unbinding an EIP.....	198
9.3 Changing an EIP.....	199
9.4 Changing an EIP Bandwidth.....	199
9.5 Having an ECS Without a Public IP Address Access the Internet.....	200
10 Resources.....	204

10.1 Quota Adjustment.....	204
11 Monitoring.....	206
11.1 Monitoring ECSs.....	206
11.2 Basic ECS Metrics.....	206
11.3 OS Monitoring Metrics Supported by ECSs with the Agent Installed.....	212
11.4 Setting Alarm Rules.....	218
11.5 Viewing ECS Metrics.....	219
12 CTS.....	220
12.1 Supported CTS Operations.....	220
12.2 Viewing Tracing Logs.....	221
13 FAQs.....	222
13.1 Product Consultation.....	222
13.1.1 What Restrictions Apply to ECSs?.....	222
13.1.2 What Can I Do with ECSs?.....	222
13.1.3 Can ECSs Automatically Recover After the Physical Host Accommodating the ECSs Becomes Faulty?.....	222
13.2 Creation and Deletion.....	223
13.2.1 Why Does the Failures Area Show an ECS Creation Failure But the ECS List Displays the Created ECS?.....	223
13.2.2 What Should I Do If It Is Slow to Create ECSs Using a Full-ECS Image?.....	223
13.2.3 How Long Does It Take to Obtain an ECS?.....	225
13.2.4 What Functions Does the Delete Button Provide?.....	225
13.2.5 Can a Deleted ECS Be Provisioned Again?.....	225
13.2.6 Can a Deleted ECS Be Restored?.....	225
13.2.7 What Should I Do When an ECS Remains in the Restarting or Stopping State for a Long Time?..	225
13.3 Login and Connection.....	226
13.3.1 Why Cannot I Use the Account Used to Create a GPU-accelerated ECS to Log In to the ECS Through SSH?.....	226
13.3.2 What Should I Do If Garbled Characters Are Displayed When I Log In to My ECS Using VNC?.....	227
13.3.3 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?.....	228
13.3.4 What Should I Do If I Cannot View Data After Logging In to an ECS Using VNC?.....	228
13.3.5 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?.....	229
13.3.6 What Should I Do If Error Code 1006 or 1000 Is Displayed When I Log In to an ECS Through the Management Console?.....	229
13.3.7 Why No Audio File Can Be Properly Played on My Windows ECS Logged In Using VNC?.....	230
13.3.8 How Can I Change the Resolution of a Windows ECS?.....	231
13.3.9 What Should I Do If I Cannot Use MSTSC to Log In to an ECS Running the Windows Server 2012 OS?.....	234
13.3.10 How Can I Change a Remote Login Port?.....	235
13.3.11 What Should I Do If I Cannot Obtain the Password for Logging In to My Windows ECS Authenticated Using a Key Pair?.....	238

13.3.12 What Browser Version Is Required to Remotely Log In to an ECS?.....	239
13.3.13 Why Does the System Display a Message Indicating that the Password for Logging In to a Windows ECS Cannot Be Viewed?.....	240
13.3.14 What Should I Do If an Authentication Failure Occurs After I Attempt to Remotely Log In to a Windows ECS?.....	241
13.3.15 What Should I Do If the Local Computer Cannot Connect to My Windows ECS?.....	242
13.3.16 What Should I Do If I Do Not Have the Permission to Remotely Log In to a Windows ECS?.....	247
13.3.17 What Should I Do If the System Displays No Remote Desktop License Servers Available to Provide a License When I Log In to a Windows ECS?.....	249
13.3.18 What Should I Do If the System Displays Error Code 0x112f When I Log In to a Windows ECS?.....	251
13.3.19 What Should I Do If the System Displays Error Code 0x1104 When I Log In to a Windows ECS?.....	252
13.3.20 What Should I Do If the System Displays Error Code 122.112... When I Log In to a Windows ECS?.....	256
13.3.21 What Should I Do If the System Displays Invalid Certificate or Associated Chain When I Log In to a Windows ECS from a Mac?.....	258
13.3.22 Troubleshooting Disconnected Session Because of a Protocol Error.....	262
13.3.23 Troubleshooting an Identity Error of the Remote Computer.....	264
13.3.24 Troubleshooting the Connection Error of Two Computers in the Allotted Time.....	265
13.3.25 Troubleshooting a Denied Connection Because of Unauthorized User Account.....	265
13.3.26 Troubleshooting a Lost Connection Because of Another User's Login.....	269
13.3.27 What Should I Do If Error Message "Module is unknown" Is Displayed When I Remotely Log In to a Linux ECS?.....	272
13.3.28 What Should I Do If Error Message "Permission denied" Is Displayed When I Remotely Log In to a Linux ECS?.....	274
13.3.29 What Should I Do If Error Message "read: Connection reset by peer" Is Displayed When I Remotely Log In to a Linux ECS?.....	276
13.3.30 What Should I Do If Error Message "Access denied" Is Displayed When I Remotely Log In to a Linux ECS?.....	277
13.3.31 What Should I Do If Error Message "Disconnected: No supported authentication methods available" Is Displayed When I Remotely Log In to a Linux ECS?.....	278
13.4 ECS Management.....	278
13.4.1 How Can a Changed Static Hostname Take Effect Permanently?.....	279
13.4.2 Is an ECS Hostname with Suffix .novalocal Normal?.....	280
13.4.3 What Should I Do If the Disk of a Windows ECS Becomes Offline After the ECS Specifications Are Modified?.....	281
13.4.4 What Should I Do If the Disk of a Linux ECS Becomes Offline After the ECS Specifications Are Modified?.....	284
13.4.5 How Do I Handle Error Messages Displayed on the Management Console?.....	285
13.5 OS Management.....	287
13.5.1 Can I Install or Upgrade the OS by Myself?.....	287
13.5.2 Can the OS of an ECS Be Changed?.....	287
13.5.3 How Long Does It Take to Change an ECS OS?.....	288
13.5.4 Can I Select Another OS During ECS OS Reinstallation?.....	288
13.5.5 How Long Does It Take to Reinstall an ECS OS?.....	288

13.5.6 Do ECSs Support GUI?.....	288
13.5.7 How Can I Install a GUI on an ECS Running CentOS 6?.....	288
13.5.8 How Can I Install a GUI on an ECS Running CentOS 7 or EulerOS?.....	289
13.5.9 How Can I Install a GUI on an ECS Running Ubuntu?.....	289
13.6 File Transferring.....	290
13.6.1 How Can I Upload a File to an ECS?.....	290
13.6.2 How Can I Transfer Files from a Local Windows Computer to a Windows ECS?.....	291
13.6.3 How Can I Use WinSCP to Transfer Files from a Local Windows Computer to a Linux ECS?.....	294
13.6.4 How Can I Use SCP to Transfer Files Between a Local Linux Computer and a Linux ECS?.....	295
13.6.5 How Can I Use SFTP to Transfer Files Between a Local Linux Computer and a Linux ECS?.....	296
13.6.6 How Can I Use FTP to Transfer Files from a Local Windows Computer to a Windows or Linux ECS?	298
13.6.7 How Can I Use FTP to Transfer Files Between a Local Linux Computer and a Linux ECS?.....	299
13.6.8 What Should I Do If the Connection Between the Client and the Server Times Out When I Upload a File Using FTP?.....	300
13.6.9 What Should I Do If Writing Data Failed When I Upload a File Using FTP?.....	300
13.6.10 What Should I Do If an Error Occurs When I Open a Folder on an FTP Server?.....	302
13.7 Application Migration.....	303
13.7.1 Can an ECS Be Migrated to Another Region or Account?.....	303
13.8 Disk Management.....	304
13.8.1 What Should I Do If the Data Disk Attached a Windows ECS Is Unavailable?.....	304
13.8.2 How Can I Adjust System Disk Partitions?.....	305
13.8.3 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Windows ECS?.....	311
13.8.4 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Linux ECS?.....	314
13.8.5 How Can I Enable Virtual Memory on a Windows ECS?.....	316
13.8.6 Why Is the Memory of an ECS Obtained by Running the free Command Inconsistent with the Actual Memory?.....	318
13.8.7 How Can I Add the Empty Partition of an Expanded System Disk to the End Root Partition Online?	320
13.8.8 How Can I Add the Empty Partition of an Expanded System Disk to the Non-end Root Partition Online?.....	321
13.8.9 Can Multiple Disks Be Attached to an ECS?.....	323
13.8.10 What Are the Restrictions on Attaching an EVS Disk to an ECS?.....	325
13.8.11 Which ECSs Can Be Attached with SCSI EVS Disks?.....	325
13.8.12 What Is the Mapping Between Device Names and Disks?.....	325
13.8.13 What Should I Do If a Linux ECS with a SCSI Disk Attached Fails to Restart?.....	327
13.8.14 What Should I Do If a Disk Is Offline?.....	328
13.8.15 What Should I Do If the Drive Letter Changes After the ECS Is Restarted?.....	329
13.8.16 How Can I Obtain Data Disk Information If Tools Are Deleted?.....	330
13.9 Passwords and Key Pairs.....	331
13.9.1 How Can I Set the Validity Period of the Image Password?.....	331
13.9.2 How Can I Obtain the Key Pair Used by an ECS?.....	332
13.9.3 What Should I Do If a Key Pair Cannot Be Imported?.....	332
13.9.4 Why Was My Login to a Linux ECS Using a Key File Unsuccessful?.....	333

13.9.5 What Should I Do If a Key Pair Created Using puttygen.exe Cannot Be Imported to the Management Console?.....	333
13.9.6 What Is the cloudbase-init Account in Windows ECSs?.....	335
13.9.7 What Should I Do If Cloud-Init Does Not Work After Python Is Upgraded?.....	336
13.10 Network Configurations.....	337
13.10.1 Can Multiple EIPs Be Bound to an ECS?.....	337
13.10.2 Can an ECS Without an EIP Access the Internet?.....	338
13.10.3 Why Cannot an EIP Be Pinged?.....	339
13.10.4 Why Can I Remotely Access an ECS But Cannot Ping It?.....	344
13.10.5 Will NICs Added to an ECS Start Automatically?.....	344
13.10.6 How Can I Obtain the MAC Address of My ECS?.....	344
13.10.7 How Can I Test Network Performance?.....	346
13.10.8 Why Cannot I Use DHCP to Obtain a Private IP Address?.....	354
13.10.9 How Can I View and Modify Kernel Parameters of a Linux ECS?.....	357
13.10.10 How Can I Configure Port Redirection?.....	362
13.10.11 Can the ECSs of Different Accounts Communicate over an Intranet?.....	364
13.10.12 Are ECSs I Purchased Deployed in the Same Subnet?.....	364
13.11 Resource Management and Tags.....	364
13.11.1 How Can I Create and Delete Tags and Search for ECSs by Tag?.....	364
13.12 Resource Monitoring.....	364
13.12.1 Troubleshooting High Bandwidth or CPU Usage of a Windows ECS.....	365
13.12.2 Troubleshooting High Bandwidth or CPU Usage of a Linux ECS.....	370
13.13 Database Applications.....	374
13.13.1 Can a Database Be Deployed on an ECS?.....	374
13.13.2 Does an ECS Support Oracle Databases?.....	374
A Change History.....	375

1 Service Overview

1.1 What Is ECS?

An Elastic Cloud Server (ECS) is a basic computing unit that consists of vCPUs, memory, OS, and Elastic Volume Service (EVS) disks. After creating an ECS, you can use it on the cloud like using your local PC or physical server.

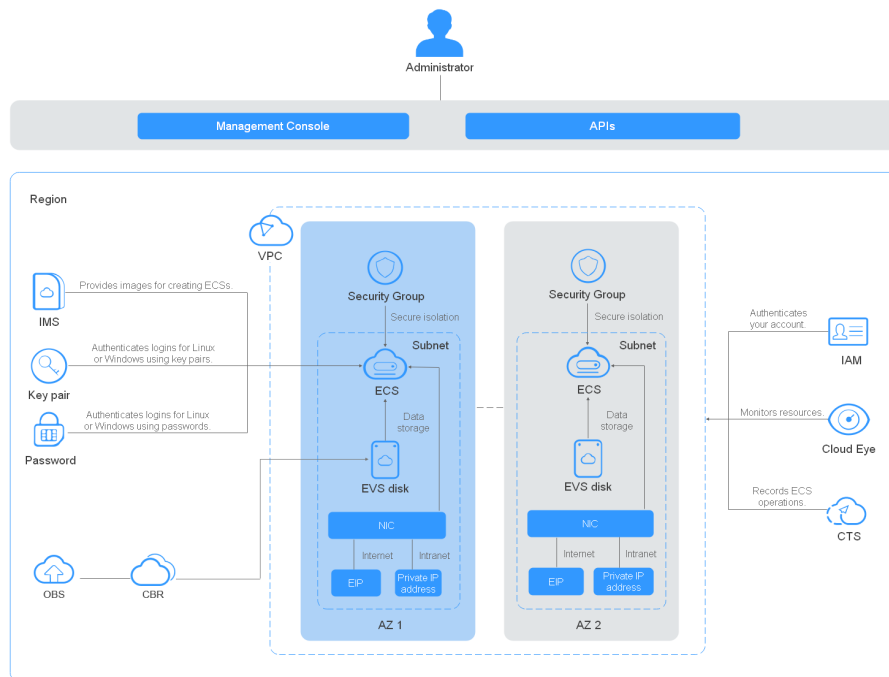
ECSs support self-service creation, modification, and operation. You can create an ECS by specifying its vCPUs, memory, OS, and login authentication. After creating an ECS, you can modify its specifications as required. ECS works with other services to provide a reliable, secure, efficient computing environment.

System Architecture

ECS works with other products and services to provide computing, storage, network, and image functions.

- ECSs are deployed in multiple availability zones (AZs) connected with each other through an internal network. If an AZ becomes faulty, other AZs in the same region will not be affected.
- With the Virtual Private Cloud (VPC) service, you can build a dedicated network, set subnets and security groups, and allow the VPC to communicate with the external network through an EIP (bandwidth support required).
- With the Image Management Service (IMS), you can install images on ECSs, or create ECSs using private images for rapid service deployment.
- Elastic Volume Service (EVS) provides storage and Volume Backup Service (VBS) provides data backup and restoration functions.
- Cloud Eye is a key measure to monitor ECS performance, reliability, and availability. Using Cloud Eye, you can view ECS resource usage in real time.
- Cloud Backup and Recovery (CBR) backs up data for EVS disks and ECSs, and uses snapshot backups to restore the EVS disks and ECSs.

Figure 1-1 System architecture



Access Methods

The public cloud provides a web-based service management platform. You can access ECSs through HTTPS-compliant application programming interfaces (APIs) or the management console.

- Accessing ECSs through APIs

Use this method if you are required to integrate the ECSs on the public cloud platform into a third-party system for secondary development. For detailed operations, see *Elastic Cloud Server API Reference*.

- Accessing ECSs through the management console

Use this method if you are not required to integrate ECSs with a third-party system.

1.2 ECS Advantages

ECS supports automatic adjustment of computing resources based on service requirements and scaling policies. You can customize ECS configurations as needed, including vCPUs, memory, and bandwidth for secure, flexible, and efficient applications.

Stability and Reliability

- Differentiated EVS disks

Common I/O, high I/O, and ultra-high I/O EVS disks are available for all of your service requirements.

Common I/O EVS disks: secure, reliable, and scalable. They are ideal for applications requiring large capacity, moderate read/write speed, and few transactions.

High I/O EVS disks: feature high performance, scalability, and reliability. They are ideal for applications requiring high performance, high read/write speed, and instant data storage.

Ultra-high I/O EVS disks: feature low latency and high performance. They are ideal for intensive read/write applications requiring extremely high performance and read/write speed, and low latency.

- Reliable data

ECS provides scalable, reliable high-throughput virtual block storage based on a distributed architecture. This ensures that data can be rapidly migrated and restored if any data replica is unavailable, preventing data loss caused by a single hardware fault.

- Backup and restoration of ECSs and EVS disks

You can set automatic backup policies to back up in-service ECSs and EVS disks. Additionally, the data of ECSs and EVS disks at a specified time can be automatically backed up through the management console or API.

Security

- Various security services are provided for multi-dimensional protection.

Security services, such as WAF and VSS are available.

- Security evaluation

Cloud environment security evaluation helps you quickly identify security vulnerabilities and threats. Security configuration check and recommendations reduce or eliminate your loss from network viruses or attacks.

- Intelligent process management

You can customize an allowlist to automatically prohibit the execution of unauthorized programs.

- Vulnerability scan

Various scan services are provided, including general web vulnerability scan, third-party application vulnerability scan, port detection, and fingerprint identification.

Competitive Advantage

- Professional hardware devices

ECSs are deployed on professional hardware devices that support in-depth virtualization optimization, relieving you of equipment-room concerns.

- Always available virtualized resources

Scalable, dedicated resources can be obtained from the virtualized resource pool any time, ensuring reliable, secure, flexible, and efficient application environments. You can use your ECS like using your local computer.

Auto Scaling

- Automatic adjustment of computing resources

Dynamic scaling: AS automatically increases or decreases the number of ECSs in an AS group based on monitored data.

Periodic/Scheduled scaling: AS increases or decreases the number of ECSs in an AS group periodically or at a specified time based on the service expectation and operation plan.

- Flexible adjustment of ECS configurations
ECS specifications and bandwidth can be flexibly adjusted based on service requirements.

1.3 ECS Application Scenarios

Internet

No special requirements on CPUs, memory, disk space, or bandwidth; strong security and reliability; application deployment based on one or only a few ECSs to minimize initial investment and maintenance costs, such as website R&D and testing, and small-scale databases

Use general computing ECSs, which provide a balance of computing, memory, and network resources. This ECS type is appropriate for medium-workload applications and meets the cloud service needs of both enterprises and individuals.

E-Commerce

Large amount of memory; capable of processing large volumes of data; fast network and rapid data processing, such as precision marketing, E-Commerce, and mobile apps

Use memory-optimized ECSs, which have a large amount of memory and provide ultra-high I/O EVS disks and appropriate bandwidths.

Graphics Rendering

High-quality graphics and video; large amount of memory, capable of processing large volumes of data, and high I/O concurrency; fast network and rapid data processing; high GPU performance, such as graphics rendering and engineering drawing

Use GPU-accelerated ECSs, including G1 ECSs, which are based on NVIDIA Tesla M60 hardware virtualization and provide cost-effective graphics acceleration. These ECSs support DirectX and OpenGL, provide computing with up to 1 GB of GPU memory and 4096 x 2160 resolution.

Data Analysis

Capable of processing large volumes of data; high I/O performance and rapid data switching and processing, such as MapReduce and Hadoop

Use disk-intensive ECSs, which are designed for applications requiring sequential read/write on ultra-large datasets in local storage (such as distributed Hadoop computing) as well as large-scale parallel data processing and log processing. Disk-intensive ECSs are based on HDD and a default network bandwidth of 10GE,

providing high PPS and low network latency. They also support up to 24 local disks, 48 vCPUs, and 384 GB of memory.

High-Performance Computing

High computing performance and throughput, such as scientific computing, genetic engineering, games and animation, biopharmaceuticals, and storage

Use high-performance computing ECSs to meet the computing, storage, and rendering needs of high-performance infrastructure services and applications that require a large number of parallel computing resources.

1.4 Notes and Constraints on Using ECSs

Notes on Using ECSs

- Do not use ECSs for any illegal services, such as gambling, unauthorized services, or cross-border VPN.
- Do not use ECSs for fake transactions, such as click farming on e-commerce websites.
- Do not use ECSs to initiate network attacks, such as DDoS attacks, CC attacks, web attacks, brute force cracking, or to spread viruses and Trojan horses.
- Do not use ECSs for traffic transit.
- Do not use ECSs to set up any crawler environment for data crawling.
- Do not use ECSs for probing operations, such as scanning or penetrating external systems, without written authorization from the external systems.
- Do not deploy any illegal websites or applications on ECSs.

General Constraints and Precautions

- Do not uninstall the driver on the ECS hardware.
- ECSs do not support external hardware devices, such as encryption locks or USB flash drives.
- Do not change the MAC address of NICs.
- ECSs do not support secondary virtualization.
- The authentication of certain software may associate a license with the physical server accommodating an ECS. Once the ECS deployed on the physical server is migrated, the associated license will not take effect because the physical server will change.
- If an ECS is migrated from a faulty physical server, the ECS may be stopped or restarted. For high service availability, deploy applications in a cluster or on ECSs working in active/standby mode, or configure automatic ECS startup upon a physical server failure or startup.
- Back up data for the ECSs where core applications are deployed.
- Monitor application metrics on ECSs.
- Do not change the default DNS server. If you are required to configure public DNS, configure public and intranet DNS on your ECS.

Precautions for Using Windows ECSs

- Do not stop system processes. Otherwise, blue screen of death (BSOD) may occur on the ECS, or the ECS may restart.
- Ensure that there is at least 2 GB of idle memory. Otherwise, BSOD, frame freezing, or service running failure may occur.
- Do not modify the registry. Otherwise, starting the system may fail. If the modification is mandatory, back up the registry before modifying it.
- Do not modify ECS clock settings. Otherwise, DHCP lease may fail, leading to the loss of IP addresses.
- Do not disable virtual memory. Otherwise, system performance may deteriorate, or system exceptions may occur.
- Do not delete the VMTool program. Otherwise, the ECS may fail to run properly.

Precautions for Using Linux ECSs

- Do not modify the `/etc/issue` file. Otherwise, the system edition will not be identified.
- Do not delete system directories or files. Otherwise, the system may fail to start or run.
- Do not change the permissions or names of system directories. Otherwise, the system may fail to start or run.
- When upgrading a Linux kernel, strictly follow the instructions provided in
- Do not change the default DNS server `/etc/resolv.conf`. Otherwise, software sources and NTP may be unavailable.
- Do not modify default intranet configurations, such as IP addresses, subnet mask, and gateway address of an ECS. Otherwise, network exceptions may occur.

1.5 Instances

1.5.1 Overview

An ECS is a basic computing unit that consists of vCPUs, memory, OS, and EVS disks.

After creating an ECS, you can use it like using your local computer or physical server, ensuring secure, reliable, and efficient computing. ECSs support self-service creation, modification, and operation. You can create an ECS by specifying its vCPUs, memory, OS, and login authentication. After the ECS is created, you can modify its specifications as required. This ensures a reliable, secure, efficient computing environment.

The cloud platform provides multiple ECS types for different computing and storage capabilities. One ECS type provides various flavors with different vCPU and memory configurations for you to select.

- For details about ECS types, see [1.5.3 ECS Types](#).

- For details about all ECS statuses in a lifecycle, see [1.5.2 ECS Lifecycle](#).

1.5.2 ECS Lifecycle

A lifecycle indicates the ECS statuses recorded from the time when the ECS is created through the time when the ECS is deleted or released.

Table 1-1 ECS statuses

Status	Status Attribute	Description
Creating	Intermediate	The ECS has been created but is not running.
Starting	Intermediate	The ECS is between the Stopped and Running states.
Running	Stable	The ECS is running properly. An ECS in this state can provide services.
Stopping	Intermediate	The ECS is between the Running and Stopped states.
Stopped	Stable	The ECS has been properly stopped. An ECS in this state cannot provide services.
Restarting	Intermediate	The ECS is being restarted.
Resizing	Intermediate	The ECS has received a resizing request and has started to resize.
Verifying resizing	Intermediate	The ECS is verifying the modified configuration.
Deleting	Intermediate	The ECS is being deleted. If the ECS remains in this state for a long time, exceptions may have occurred. In such a case, contact the administrator.
Deleted	Intermediate	The ECS has been deleted. An ECS in this state cannot provide services and will be promptly cleared from the system.
Faulty	Stable	An exception has occurred on the ECS. An ECS in this state cannot provide services. Contact the administrator.
Reinstalling OS	Intermediate	The ECS has received a request to reinstall the OS and has begun the reinstallation.
Reinstalling OS failed	Stable	The ECS received a request to reinstall the OS, but due to exceptions, the reinstallation failed. An ECS in this state cannot provide services. Contact the administrator.

Status	Status Attribute	Description
Changing OS	Intermediate	The ECS received a request to change the OS and has begun implementing the changes.
OS Change failed	Stable	The ECS has received a request to change the OS, but due to exceptions, the changes failed to be implemented. An ECS in this state cannot provide services. Contact the administrator.
Forcibly restarting	Intermediate	The ECS is being forcibly restarted.
Rolling back resizing	Intermediate	The ECS is rolling back resizing.
Frozen	Stable	The ECS has been stopped by the administrator because the order has expired or is overdue. An ECS in this state cannot provide services. The system retains it for a period of time. If it is not renewed after the time expires, the system will automatically delete the ECS.

1.5.3 ECS Types

The public cloud provides the following ECS types for different application scenarios:

- [1.7.1 Kunpeng General Computing-plus ECSs](#)
- [1.7.2 Kunpeng Memory-optimized ECSs](#)
- [1.6.1 General Computing ECSs](#)
- [1.6.2 General Computing-plus ECSs](#)
- [1.6.3 Memory-optimized ECSs](#)
- [1.6.4 Disk-intensive ECSs](#)
- [1.6.5 Ultra-high I/O ECSs](#)

ECS Flavor Naming Rules

ECS flavors are named using the format "AB.C.D".

The format is defined as follows:

- **A** specifies the ECS type. For example, **s** indicates a general ECS, **c** a computing ECS, and **m** a memory-optimized ECS.
Kunpeng flavor names are started with letter **k**. For example, **kc** indicates Kunpeng general computing-plus.
- **B** specifies the type ID. For example, the **1** in **s1** indicates a general first-generation ECS, and the **2** in **s2** indicates a general second-generation ECS.

- **C** specifies the flavor size, such as medium, large, xlarge, 2xlarge, 4xlarge, or 8xlarge.
- **D** specifies the ratio of memory to vCPUs expressed in a digit. For example, value **4** indicates that the ratio of memory to vCPUs is 4.

Network Bandwidth

The intranet bandwidth and PPS of an ECS are determined based on ECS flavors.

- Assured intranet bandwidth: indicates the assured ECS bandwidth.
- Maximum intranet bandwidth: indicates the maximum ECS bandwidth.
- Maximum intranet PPS: indicates the maximum ECS capabilities in transmitting and receiving packets.

1.6 x86 ECS Specifications and Types

1.6.1 General Computing ECSs

Overview

General computing ECSs provide a balance of computing, memory, and network resources and a baseline level of vCPU performance with the ability to burst above the baseline. These ECSs are suitable for many applications, such as web servers, enterprise R&D, and small-scale databases.

S6 ECSs are suitable for applications that require moderate performance generally but occasionally burstable high performance, such as light-workload web servers, enterprise R&D and testing environments, and low- and medium-performance databases. S6 ECS performance is neither restricted by vCPU credits nor billed for additional credits. You can determine the CPU usage and vCPU credits in monitoring details.

Specifications

Table 1-2 S6 ECS specifications

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Maximum PPS (10,000)	NIC Multi-Queue	Maximum NICs	Virtualization Type
s6.medium.2	1	2	0.8/0.1	10	1	2	KVM
s6.large.2	2	4	1.5/0.2	15	1	2	KVM
s6.xlarge.2	4	8	2/0.35	25	1	2	KVM

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Maximum PPS (10,000)	NIC Multi-Queue	Maximum NICs	Virtualization Type
s6.2xlarge.2	8	16	3/0.75	50	2	2	KVM
s6.medium.4	1	4	0.8/0.1	10	1	1	KVM
s6.large.4	2	8	1.5/0.2	15	1	2	KVM
s6.xlarge.4	4	16	2/0.35	25	1	2	KVM
s6.2xlarge.4	8	32	3/0.75	50	2	2	KVM

Scenarios

- Web servers, light-workload applications, and R&D and testing environments
- Small- and medium-sized databases, cache servers, and search clusters

1.6.2 General Computing-plus ECSs

Overview

Compared with general computing ECSs, general computing-plus ECSs provide the combinations of vCPUs and memory with larger specifications, offering more options for you to select. In addition, the ECSs use latest-generation network acceleration engines and Data Plane Development Kit (DPDK) to provide higher network performance, meeting requirements in different scenarios.

C6 ECSs use second-generation Intel® Xeon® Scalable processors with technologies optimized and 25GE high-speed intelligent NICs to offer powerful and stable computing performance, including ultra-high network bandwidth and PPS.

Specifications

Table 1-3 C6 ECS specifications

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Max. PPS (10,000)	NIC Multi-Queue	Maximum NICs	Virtualization Type
c6.large.2	2	4	4/1.2	40	2	2	KVM
c6.xlarge.2	4	8	8/2.4	80	2	3	KVM
c6.2xlarge.2	8	16	15/4.5	150	4	4	KVM
c6.4xlarge.2	16	32	20/9	280	8	8	KVM
c6.8xlarge.2	32	64	30/18	550	16	8	KVM
c6.16xlarge.2	64	128	40/36	1000	32	8	KVM
c6.large.4	2	8	4/1.2	40	2	2	KVM
c6.xlarge.4	4	16	8/2.4	80	2	3	KVM
c6.2xlarge.4	8	32	15/4.5	150	4	4	KVM
c6.4xlarge.4	16	64	20/9	280	8	8	KVM
c6.8xlarge.4	32	128	30/18	550	16	8	KVM
c6.16xlarge.4	64	256	40/36	1000	32	8	KVM

Scenarios

Websites and web applications, generalized databases and cache servers, and medium- and heavy-workload enterprise applications with strict requirements on computing and network performance

1.6.3 Memory-optimized ECSs

Overview

Memory-optimized ECSs have a large memory size and provide high memory performance. They are designed for memory-intensive applications that process a large amount of data, such as precision advertising, e-commerce big data analysis, and IoV big data analysis.

M6 ECSs use second-generation Intel® Xeon® Scalable processors with technologies optimized to offer powerful and stable computing performance. Using 25GE high-speed intelligent NICs, M6 ECSs provide a maximum memory size of 512 GB based on DDR4 for large-memory applications with high requirements on network bandwidth and Packets Per Second (PPS).

Specifications

Table 1-4 M6 ECS specifications

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Maximum PPS (10,000)	NIC Multi-Queue	Virtualization Type
m6.large.8	2	16	4/1.2	40	2	KVM
m6.xlarge.8	4	32	8/2.4	80	2	KVM
m6.2xlarge.8	8	64	15/4.5	150	4	KVM
m6.4xlarge.8	16	128	20/9	280	8	KVM
m6.8xlarge.8	32	256	30/18	550	16	KVM
m6.16xlarge.8	64	512	40/36	1000	32	KVM

Scenarios

- Applications
Memory-optimized ECSs are suitable for applications that process large volumes of data and require a large amount of memory, rapid data switching and processing, and low-latency storage resources.
- Application scenarios
Big data analysis, precision advertising, e-commerce big data analysis, IoV big data analysis, relational databases, NoSQL databases, and memory data analysis

1.6.4 Disk-intensive ECSs

Overview

Disk-intensive ECSs are delivered with local disks for high storage bandwidth and IOPS. In addition, local disks are more cost-effective in massive data storage scenarios. Disk-intensive ECSs have the following features:

- They use local disks to provide high sequential read/write performance and low latency, improving file read/write performance.
- They provide powerful and stable computing capabilities, ensuring efficient data processing.
- They provide high intranet performance, including high intranet bandwidth and PPS, meeting requirements for data exchange between ECSs during peak hours.

D3 ECSs use Intel® Xeon® Scalable processors to offer powerful and stable computing performance. Equipped with proprietary 25GE high-speed intelligent NICs and local SAS disks, D3 ECSs offer ultra-high network bandwidth, PPS, and local storage.

Specifications

Table 1-5 D3 ECS specifications

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Maximum PPS (10,000)	NIC Multi-Queue	Local Disks (GB)	Virtualization Type
d3.xlarge.8	4	32	5/2.5	50	2	2 x 1800	KVM
d3.2xlarge.8	8	64	10/5	100	2	4 x 1800	KVM
d3.4xlarge.8	16	128	20/10	160	4	8 x 1800	KVM
d3.6xlarge.8	24	192	25/15	220	6	12 x 1800	KVM
d3.8xlarge.8	32	256	30/20	280	8	16 x 1800	KVM
d3.12xlarge.8	48	384	40/32	400	16	24 x 1800	KVM
d3.14xlarge.10	56	560	40/40	500	16	28 x 1800	KVM

1.6.5 Ultra-high I/O ECSs

Overview

Ultra-high I/O ECSs use high-performance local NVMe SSDs to provide high storage input/output operations per second (IOPS) and low read/write latency. You can create such ECSs with high-performance local NVMe SSDs attached on the management console.

Ultra-high I/O ECSs can be used for high-performance relational databases, NoSQL databases (such as Cassandra and MongoDB), and Elasticsearch.

Specifications

Table 1-6 I3 ECS specifications

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Maximum PPS (10,000)	NIC Multi-Queue	Local Disks	Maximum NICs	Virtualization Type
i3.2xlarge.8	8	64	8/3.5	100	4	1 x 1600 GB NVMe	4	KVM
i3.4xlarge.8	16	128	15/7	160	4	2 x 1600 GB NVMe	8	KVM
i3.8xlarge.8	32	256	20/14	280	8	4 x 1600 GB NVMe	8	KVM
i3.12xlarge.8	48	384	25/20	420	8	6 x 1600 GB NVMe	8	KVM

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Maximum PPS (10,000)	NIC Multi-Queue	Local Disks	Maximum NICs	Virtualization Type
i3.16xlarge.8	64	512	25/25	500	16	8 x 1600 GB NVMe	8	KVM

Features

[Table 1-7](#) lists the IOPS performance of I3 ECSs.

Table 1-7 I3 ECS IOPS performance

Flavor	Maximum IOPS for Random 4 KB Read
i3.2xlarge.8	750,000
i3.4xlarge.8	1,500,000
i3.8xlarge.8	3,000,000
i3.12xlarge.8	4,500,000
i3.15xlarge.8	5,250,000

Table 1-8 Specifications of a single NVMe disk attached to an I3 ECS

Metric	Performance
Disk capacity	1.6 TB
IOPS for random 4 KB read	750,000
IOPS for random 4 KB write	200,000
Read throughput	2.9 GB/s
Write throughput	1.9 GB/s
Access latency	Within microseconds

Notes

- When the physical host where a ultra-high I/O ECS is deployed becomes faulty, the ECS cannot be migrated.
- Ultra-high I/O ECSs do not support specifications modification.
- Ultra-high I/O ECSs do not support local disk snapshots or backups.
- Ultra-high I/O ECSs can use both local disks and EVS disks to store data. In addition, they can have EVS disks attached to provide a larger storage size. Use restrictions on the two types of storage media are as follows:
 - Only an EVS disk, not a local disk, can be used as the system disk of a ultra-high I/O ECS.
 - Both EVS disks and local disks can be used as data disks of a ultra-high I/O ECS.
 - A ultra-high I/O ECS can be attached with a maximum of 60 disks (including VBD, SCSI, and local disks). Among the 60 disks, the maximum number of SCSI disks is 30, and the maximum number of VBD disks is 22 (including the system disk).
 - You are advised to use World Wide Names (WWNs), but not drive letters, in applications to perform operations on local disks to prevent drive letter drift (low probability) on Linux. Take local disk attachment as an example:

If the local disk WWN is `wwn-0x50014ee2b14249f6`, run the **`mount /dev/disk/by-id/wwn-0x50014ee2b14249f6`** command.

NOTE

How can I view the local disk WWN?

1. Log in to the ECS.
2. Run the following command:

```
ll /dev/disk/by-id
```

- The local disk data of a ultra-high I/O ECS may be lost due to some reasons, such as physical server breakdown or local disk damage. If the data reliability of your application cannot be ensured, you are strongly advised to use EVS disks to build your ECS.
- After a ultra-high I/O ECS is deleted, the data on local NVMe SSDs is automatically deleted. Back up the data before deleting such an ECS. Deleting local disk data is time-consuming. Therefore, a ultra-high I/O ECS requires a longer period of time than other ECSs for releasing resources.
- The data reliability of local disks depends on the reliability of physical servers and hard disks, which are SPOF-prone. Therefore, you are advised to perform data redundancy at the application layer to ensure data availability. Use EVS disks to store long-term service data.
- The device name of a local disk attached to an I3 ECS is `/dev/nvme0n1` or `/dev/nvme0n2`.

1.7 Kunpeng ECS Specifications and Types

1.7.1 Kunpeng General Computing-plus ECSs

Overview

Kunpeng general computing-plus KC1 ECSs use Kunpeng 920 processors and 25GE high-speed intelligent NICs to offer powerful computing and high-performance networks, meeting the requirements of governments and Internet enterprises for cost-effective, secure, reliable cloud services.

Specifications

Table 1-9 KC1 ECS specifications

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Maximum PPS (10,000)	NIC Multi-Queue	Maximum NICs	Virtualization Type
kc1.large.2	2	4	3/0.8	30	2	2	KVM
kc1.xlarge.2	4	8	5/1.5	50	2	3	KVM
kc1.2xlarge.2	8	16	7/3	80	4	4	KVM
kc1.3xlarge.2	12	24	9/4.5	110	4	5	KVM
kc1.4xlarge.2	16	32	12/6	140	4	6	KVM
kc1.6xlarge.2	24	48	15/8.5	200	8	6	KVM
kc1.8xlarge.2	32	64	18/10	260	8	6	KVM
kc1.12xlarge.2	48	96	25/16	350	16	6	KVM
kc1.15xlarge.2	60	120	30/20	400	16	6	KVM
kc1.large.4	2	8	3/0.8	30	2	2	KVM
kc1.xlarge.4	4	16	5/1.5	50	2	3	KVM
kc1.2xlarge.4	8	32	7/3	80	4	4	KVM

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Maximum PPS (10,000)	NIC Multi-Queue	Maximum NICs	Virtualization Type
kc1.3xlarge.4	12	48	9/4.5	110	4	5	KVM
kc1.4xlarge.4	16	64	12/6	140	4	6	KVM
kc1.6xlarge.4	24	96	15/8.5	200	8	6	KVM
kc1.8xlarge.4	32	128	18/10	260	8	6	KVM
kc1.12xlarge.4	48	192	25/16	350	16	6	KVM

Scenarios

KC1 ECSs are suitable for governments, enterprises, and the financial industry with strict requirements on security and privacy, for Internet applications with high requirements on network performance, for big data and HPC requiring a large number of vCPUs, and for website setups and e-Commerce requiring cost-effectiveness.

1.7.2 Kunpeng Memory-optimized ECSs

Overview

Kunpeng memory-optimized KM1 ECSs use Kunpeng 920 processors and 25GE high-speed intelligent NICs to provide up to 480 GB DDR4-based memory with high network performance for large-memory datasets.

Specifications

Table 1-10 KM1 ECS specifications

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Max. PPS (10,000)	NIC Multi-Queue	Maximum NICs	Virtualization Type
km1.large.8	2	16	3/0.8	30	2	2	KVM

Flavor	vCPUs	Memory (GB)	Maximum/Assured Bandwidth (Gbit/s)	Max. PPS (10,000)	NIC Multi-Queue	Maximum NICs	Virtualization Type
km1.xlarge.8	4	32	5/1.5	50	2	3	KVM
km1.2xlarge.8	8	64	7/3	80	4	4	KVM
km1.3xlarge.8	12	96	9/4.5	110	4	5	KVM
km1.4xlarge.8	16	128	12/6	140	4	6	KVM
km1.6xlarge.8	24	192	15/8	200	8	6	KVM
km1.8xlarge.8	32	256	18/10	260	8	6	KVM
km1.12xlarge.8	48	384	25/16	350	16	8	KVM
km1.15xlarge.8	60	480	30/20	400	16	8	KVM

Scenarios

Big data analysis, precision advertising, e-commerce, IoT, and in-memory storage (such as Memcache)

1.8 Images

What Is Image?

An image is an ECS template that contains an OS and may also contain proprietary software and application software, such as database software. You can use images to create ECSs.

Images can be public or private. Public images are provided by the system by default, and private images are manually created. You can use any type of image to create an ECS. You can also create a private image using an existing ECS. This provides you with a simple way to create ECSs that comply with your service requirements. For example, if you use web services, your image can contain web server configurations, static configurations, and dynamic page code. After you use this image to create an ECS, the web server will run.

Image Types

Image Type	Description
Public image	A public image is a standard, widely used image. It contains an OS and preinstalled public applications and is available to all users. Public images are highly stable and authorized. You can configure the application environment or related software as needed.
Private image	<p>A private image is an image that contains an OS or service data, pre-installed public applications, and the owner's private applications. It is available only to the user who created it.</p> <p>A private image can be a system disk image, data disk image, or full-ECS image.</p> <ul style="list-style-type: none">• System disk image: contains an OS and pre-installed application software for running services. You can use a system disk image to create ECSs and migrate your services to the cloud.• Data disk image: contains only the owner's service data. You can use a data disk image to create EVS disks and migrate your service data to the cloud.• Full-ECS image: contains an OS, pre-installed application software, and service data. A full-ECS image is created using differential backups and the creation takes a shorter time than creating a system or data disk image with the same size.
Shared image	A shared image is a private image other users share with you.

1.9 EVS Disks

What Is Elastic Volume Service?

Elastic Volume Service (EVS) offers scalable block storage for ECSs. With high reliability, high performance, and rich specifications, EVS disks can be used for distributed file systems, development and test environments, data warehouse applications, and high-performance computing (HPC) scenarios to meet diverse service requirements.

Disk Types

EVS disk types differ in performance. Choose the disk type based on your requirements. The details are described as follows:

For more information about EVS disk specifications and performance, see *Elastic Volume Service User Guide*.

Device Types

EVS disks have two device types, Virtual Block Device (VBD) and Small Computer System Interface (SCSI).

- VBD

When you create an EVS disk on the management console, **Device Type** of the EVS disk is VBD by default. VBD EVS disks support only simple SCSI read/write commands.

- SCSI

You can create EVS disks for which **Device Type** is SCSI on the management console. These EVS disks support transparent SCSI command transmission, allowing ECS OS to directly access underlying storage media. SCSI EVS disks support both basic and advanced SCSI commands.

NOTE

For more information about how to use SCSI EVS disks, for example, how to install the driver, see "Device Types and Usage Instructions" in *Elastic Volume Service User Guide*.

1.10 Network

VPC

Virtual Private Cloud (VPC) allows you to create customized virtual networks in your logically isolated AZ. Such networks are dedicated zones that are logically isolated for your ECSs. You can define security groups, virtual private networks (VPNs), IP address segments, and bandwidth for a VPC. This facilitates internal network configuration and management as well as secure and convenient network modification. You can also customize the ECS access rules within a security group and between security groups to improve ECS security.

For more information about VPC, see *Virtual Private Cloud User Guide*.

Subnet

A subnet is a range of IP addresses in your VPC and provides IP address management and DNS resolution functions for ECSs in it. The IP addresses of all ECSs in a subnet belong to the subnet.

By default, ECSs in all subnets of the same VPC can communicate with each other, while ECSs in different VPCs cannot.

Security Group

A security group is a collection of access control rules for ECSs that have the same security protection requirements and that are mutually trusted. After a security group is created, you can create different access rules for the security group to protect the ECSs that are added to this security group.

Your account automatically comes with a default security group. The default security group allows all outbound data, denies all inbound data, and allows all data between ECSs in the group. Your ECSs in the security group can communicate with each other without the need to add rules.

Figure 1-2 Default security group

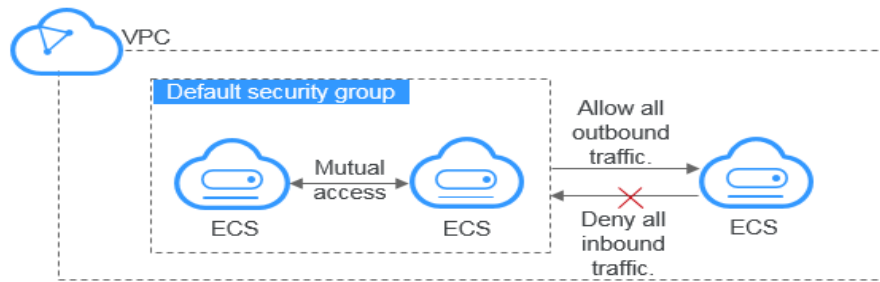


Table 1-11 describes default security group rules.

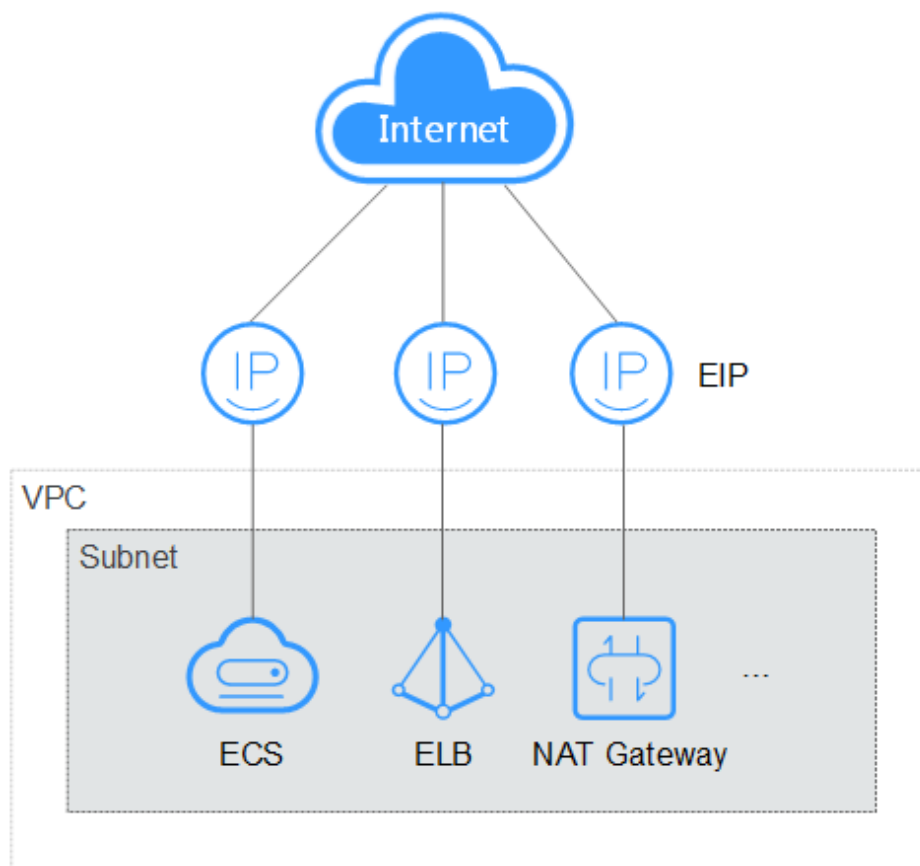
Table 1-11 Rules in the default security group

Direction	Protocol	Port/Range	Source/Destination	Description
Outbound	All	All	Destination: 0.0.0.0/0	Allows all outbound traffic.
Inbound	All	All	Source: the current security group (for example, sg-xxxxx)	Allows communication among ECSs within the security group and denies all inbound traffic (incoming data packets).
Inbound	TCP	22	Source: 0.0.0.0/0	Allows all IP addresses to access Linux ECSs over SSH.
Inbound	TCP	3389	Source: 0.0.0.0/0	Allows all IP addresses to access Windows ECSs over RDP.

EIP

An EIP is a public IP address that can be directly accessed over the Internet. An EIP consists of the public IP address and public network egress bandwidth. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, NAT gateways, or load balancers.

Each EIP can be used by only one cloud resource at a time.

Figure 1-3 Accessing the Internet using an EIP

1.11 Security

1.11.1 Cloud-Init

Cloud-Init is an open-source cloud initialization program, which initializes specified customized configurations, such as the hostname, key pair, and user data, of a newly created ECS.

Using Cloud-Init to initialize your ECSs will affect your ECS, IMS, and AS services.

Impact on IMS

To ensure that ECSs created using a private image support customized configurations, you must install Cloud-Init or Cloudbase-Init before creating the private image.

- For Windows OSs, download and install Cloudbase-Init.
- For Linux OSs, download and install Cloud-Init.

After Cloud-Init or Cloudbase-Init is installed in an image, Cloud-Init or Cloudbase-Init automatically configures initial ECS attributes when the ECS is created.

For instructions about the installation, see *Image Management Service User Guide*.

Impact on ECS

- When creating an ECS, if the selected image supports Cloud-Init, you can use user data injection to inject customized configuration, such as ECS login password, for initializing.
- After Cloud-Init is supported, you can view and use metadata to configure and manage running ECSs.

Impact on AS

- When creating an AS configuration, you can use user data injection to specify ECS configurations for initialization. If the AS configuration has taken effect in an AS group, the ECSs newly created in the AS group will automatically initialize their configurations.
- For an existing AS configuration, if its private image does not have Cloud-Init or Cloudbase-Init installed, the login mode of the ECSs created in the AS group where the AS configuration takes effect will be affected.
To resolve this issue, see "How Does Cloud-Init Affect the AS Service?" in *Auto Scaling User Guide*.

Notes

- When using Cloud-Init, enable DHCP in the VPC to which the ECS belongs.
- When using Cloud-Init, ensure that security group rules in the outbound direction meet the following requirements:
 - **Protocol: TCP**
 - **Port Range: 80**
 - **Remote End: 169.254.0.0/16**

NOTE

If you use the default security group rules in the outbound direction, the preceding requirements are met, and the metadata can be accessed. Default security group rules in the outbound direction are as follows:

- **Protocol: ANY**
- **Port Range: ANY**
- **Remote End: 0.0.0.0/0**

1.12 Region and AZ

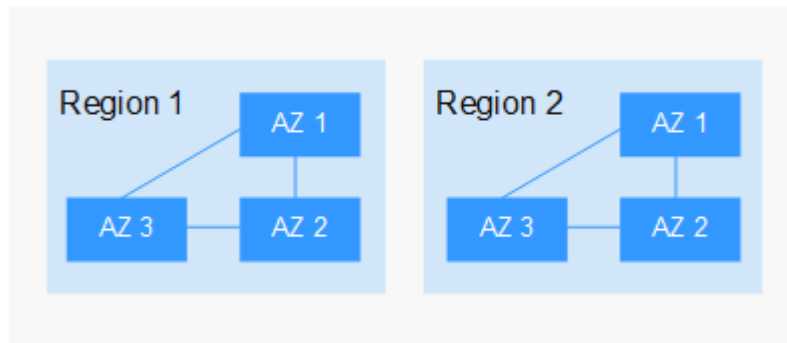
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in an AZ will not affect other AZs.

Figure 1-4 shows the relationship between regions and AZs.

Figure 1-4 Regions and AZs



Selecting a Region

Select a region closest to your target users for low network latency and quick access.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

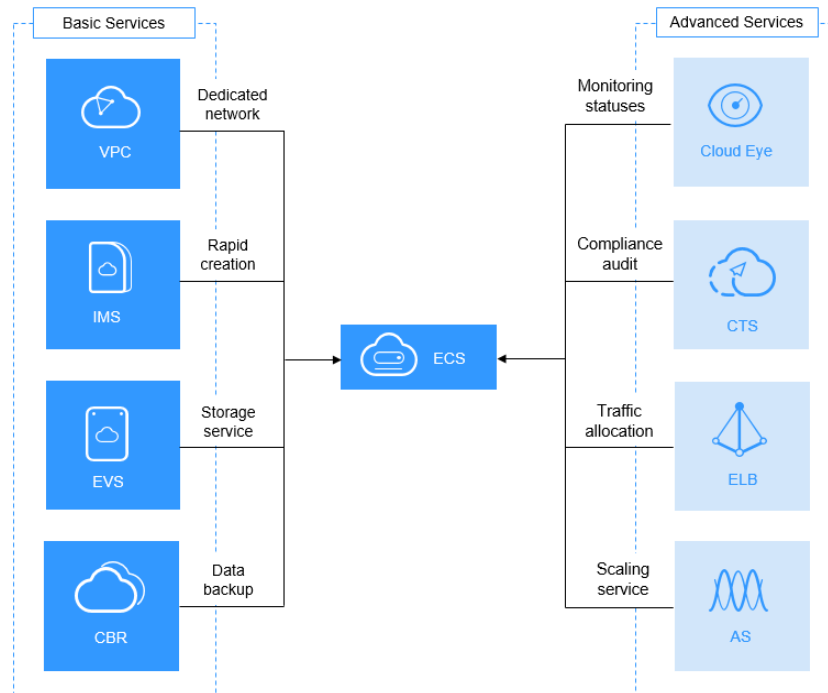
- For high DR capability, deploy resources in different AZs within the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

1.13 ECS and Other Services

Figure 1-5 shows the relationships between ECS and other services.

Figure 1-5 Relationships between ECS and other services

ECS-related Services

- **Auto Scaling (AS)**
Automatically adjusts ECS resources based on the configured AS policies. This improves resource usage and reduces resource costs.
- **Elastic Load Balancing (ELB)**
Automatically distributes traffic to multiple ECSs. This enhances system service and fault tolerance capabilities.
- **Elastic Volume Service (EVS)**
Enables you to attach EVS disks to an ECS and expand their capacity.
- **Virtual Private Cloud (VPC)**
Enables you to configure internal networks and change network configurations by customizing security groups, VPNs, IP address segments, and bandwidth. This simplifies network management. You can also customize the ECS access rules within a security group and between security groups to improve ECS security.
- **Image Management Service (IMS)**
Enables you to create ECSs using images. This improves the efficiency of ECS creation.
- **Cloud Eye**
Allows you to check the status of monitored service objects after you have obtained an ECS. This can be done without requiring additional plug-ins be installed. For details about ECS metrics supported by Cloud Eye, see [11.2 Basic ECS Metrics](#).
- **Cloud Trace Service (CTS)**
Records ECS-related operations for later query, audit, and backtrack.

- **Cloud Backup and Recovery (CBR)**
Backs up EVS disks and ECSs for restoration. You can back up all EVS disks (including the system disk and data disks) attached to an ECS and use the backup to restore the ECS data.

2 Getting Started

2.1 Creating an ECS

2.1.1 Overview

Scenarios

ECSs are more cost-effective than physical servers. Within minutes, you can obtain ECS resources from the public cloud. ECS resources are flexible and on-demand. This section describes how to create an ECS on the management console.

Creation process:

- [Step 1: Configure Basic Settings](#)
- [Step 2: Configure Network](#)
- [Step 3: Configure Advanced Settings](#)
- [Step 4: Confirm](#)

2.1.2 Step 1: Configure Basic Settings


Switching to the ECS Creation Page

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. Click **Create ECS**.

The page for creating ECSs is displayed.

Performing Basic Configurations

1. Confirm the region.

If the region is incorrect, click  in the upper left corner of the page for correction.

2. Select an AZ.

An AZ is a physical region where power and networks are physically isolated. AZs in the same region can communicate with each other over an intranet.

- To enhance application availability, create ECSs in different AZs.
- To shorten network latency, create ECSs in the same AZ.

3. Set **Specifications**.

The public cloud provides various ECS types for different application scenarios. You can view released ECS types and flavors in the list. Alternatively, you can enter a flavor (such as **c3**) or specify vCPUs and memory size to search for the desired flavor.

 **NOTE**

- Before selecting an ECS type, learn the introduction and notes on each type of ECSs. For details, see [1.5.3 ECS Types](#).

4. Select an image.

- Public image

A public image is a standard, widely used image. It contains an OS and preinstalled public applications and is available to all users. You can configure the applications or software in the public image as needed.

- Private image

A private image is an image available only to the user who created it. It contains an OS, preinstalled public applications, and the user's private applications. Using a private image to create ECSs removes the need to configure multiple ECSs repeatedly.

You can also select an encrypted image. For details, see *Image Management Service User Guide*.

 **NOTE**

- If you use a full-ECS image to create an ECS, the EVS disks associated with the full-ECS image do not support the function of creating disks using a data disk image.
- If a full-ECS image is in **Normal** state and the system displays message "Available in AZx", the full-ECS image can be used to create ECSs in this AZ only, and the encryption attributes of the system and data disks of the created ECSs are the same as those of the system and data disks specified in the full-ECS image. Additionally, the SCSI, sharing attribute, and data encryption settings of the system and data disks cannot be modified during ECS creation.
- If a full-ECS image is in **Normal** state but the system does not display message "Available in AZx", the full-ECS image can be used to create ECSs in the entire region, and the encryption attributes of the system and data disks of the created ECSs are the same as those of the system and data disks specified in the full-ECS image. Additionally, the SCSI, sharing attribute, and data encryption settings of data disks can be modified during ECS creation.
- To ensure that NIC multi-queue is enabled on an ECS created using a private image, configure NIC multi-queue when creating such a private image. NIC multi-queue routes NIC interrupt requests among multiple vCPUs for higher network PPS and bandwidth.

For details, see "How Do I Set NIC Multi-Queue Feature of an Image?"

- Shared image

A shared image is a private image shared by another user.

5. Set **System Disk**, and **Data Disk** if required.

Disks are classified as EVS disks and DSS disks based on whether the storage resources used by the disks are dedicated. DSS disks allow you to use dedicated storage resources.

- If you have requested for a storage pool on the DSS page, click the **DSS** tab and create disks in the obtained storage pool.
- If you have not requested for a dedicated storage pool, click the **Disks** tab and create EVS disks that use public storage resources.

 **NOTE**

- When you use DSS resources to create a disk, the disk type must be the same as that of the requested storage pool. For example, both are of high I/O type.
- For more information about DSS, see *Dedicated Distributed Storage Service User Guide*.

- System disk

For the disk types supported by an ECS, see [1.9 EVS Disks](#).

- If the image based on which an ECS is created is not encrypted, the system disk of the ECS is not encrypted. If the image based on which an ECS is created is encrypted, the system disk of the ECS is automatically encrypted. For details, see [\(Optional\) Encryption-r...](#)

- Data disk

You can create multiple data disks for an ECS and enable sharing and encryption for each data disk. When creating an ECS, you can add up to 24 disks with customized sizes to it. After the ECS is created, you can add up to 60 disks to such a newly created ECS.

- **SCSI**: indicates that the device type of the data disk is SCSI. For more information about SCSI disks and the ECSs that can be attached with SCSI disks, see [1.9 EVS Disks](#).
- **Share**: indicates that the EVS disk is sharable. Such an EVS disk can be attached to multiple ECSs.
- (Optional) Encryption-related parameters
 - To enable encryption, click **Create Xrole** to grant KMS access rights to EVS. If you have rights granting permission, grant the KMS access rights to EVS. If you do not have the permission, contact the user having the security administrator rights to grant the KMS access rights.
 - **Encrypted**: indicates that the EVS disk has been encrypted.
 - **Create Xrole**: grants KMS access rights to EVS to obtain KMS keys. After the rights are granted, follow-up operations do not require granting rights again.
 - **KMS Key Name**: specifies the name of the key used by the encrypted EVS disk. By default, the name is **evs/default**.
 - **Xrole Name: EVSAccessKMS**: specifies that rights have been granted to EVS to obtain KMS keys for encrypting or decrypting EVS disks.
 - **KMS Key ID**: specifies the ID of the key used by the encrypted data disk.

6. Click **Next: Configure Network**.

2.1.3 Step 2: Configure Network

Network Configurations

1. Set **Network** by selecting an available VPC and subnet from the drop-down list and specifying a private IP address assignment mode.

VPC provides a network, including subnet and security group, for an ECS.

You can select an existing VPC or create a desired one.

For more information about VPC, see *Virtual Private Cloud User Guide*.

NOTE

- Ensure that DHCP is enabled in the VPC to which the ECS belongs.
 - When you use VPC for the first time, the system automatically creates a VPC for you, including the security group and NIC.
2. (Optional) Add an extension NIC. You can add multiple expansion NICs to an ECS and specify IP addresses for them (including primary NICs).

NOTE

When you specify an IP address for a NIC, if multiple ECSs are created in a batch:

- This IP address serves as the start IP address.
 - Ensure that the IP addresses required by the NICs are within the subnet, consecutive, and available.
 - This subnet cannot duplicate a subnet with a specified start IP address.
3. Set **Security Group** by selecting an available security group from the drop-down list or creating a new one.
- A security group controls ECS access within or between security groups by defining access rules. This enhances ECS security.
- When creating an ECS, you can select multiple (recommended not more than five) security groups. In such a case, the access rules of all the selected security groups apply on the ECS.

NOTE

Before initializing an ECS, ensure that the security group rule in the outbound direction meets the following requirements:

- **Protocol: TCP**
 - **Port Range: 80**
 - **Remote End: 169.254.0.0/16**
- If you use the default security group rule in the outbound direction, the preceding requirements are met, and the ECS can be initialized. The default security group rule in the outbound direction is as follows:
- **Protocol: ANY**
 - **Port Range: ANY**
 - **Remote End: 0.0.0.0/16**
4. Set **EIP**.
- An EIP is a static public IP address bound to an ECS in a VPC. Using the EIP, the ECS provides services externally.

The following options are provided:

- Do not use
Without an EIP, the ECS cannot access the Internet and is used in the private network or cluster only.
- Auto assign
The system automatically assigns an EIP for the ECS. The EIP provides a dedicated bandwidth that is configurable.
- An existing EIP is assigned for the ECS. When using an existing EIP, you are not allowed to create ECSs in a batch.

5. Click **Next: Configure Advanced Settings**.

2.1.4 Step 3: Configure Advanced Settings

Advanced Settings

1. Set **ECS Name**.

The name can be customized but must comply with the following naming rules: Can contain only letters, digits, underscores (_), hyphens (-), and periods (.).

If you want to create multiple ECSs at a time, the system automatically sequences these ECSs.

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental number to the end of each ECS name. For example, if you enter **ecs**, the ECSs will be named **ecs-0001**, **ecs-0002**, If you create multiple ECSs again, the values in the new ECS names increase from the existing maximum value. For example, the existing ECS with the maximum number in name is **ecs-0010**. If you enter **ecs**, the names of the new ECSs will be **ecs-0011**, **ecs-0012**, When the value reaches **9999**, it will start from **0001**.

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

2. Set **Login Mode**.

Key pair authentication is more secure than password authentication. If you select **Password**, ensure that the password meets complexity requirements listed in [Table 2-1](#) to prevent malicious attacks.

- Key pair

A key pair is used for ECS login authentication. You can select an existing key pair, or click **Create Key Pair** and create a desired one.

NOTE

If you use an existing key pair, make sure that you have saved the key file locally. Otherwise, logging in to the ECS will fail.

- Password

A username and its initial password are used for ECS login authentication.

The initial password of user **root** is used for authenticating Linux ECSs, while that of user **Administrator** is used for authenticating Windows ECSs.

The passwords must meet the requirements described in [Table 2-1](#).

Table 2-1 Password complexity requirements

Parameter	Requirement	Example Value
Password	<ul style="list-style-type: none">• Consists of 8 characters to 26 characters.• Contains at least three of the following character types:<ul style="list-style-type: none">– Uppercase letters– Lowercase letters– Digits– Special characters: \$!@%-_+[]:./^, {}?• Cannot contain the username or the username spelled backwards.• Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)	YNbUwp! dUc9MClnv NOTE The example password is generated randomly. Do not copy this example password.

 **NOTE**

The system does not periodically change the ECS password. It is recommended that you change your password regularly for security.

3. Set **Cloud Backup and Recovery**.

Cloud Backup and Recovery (CBR) provides backup protection for EVS disks and ECSs, and uses backups to restore the EVS disks and ECSs. After you set **Cloud Backup and Recovery**, the system binds the target ECS to the cloud backup vault and associates the ECS with the selected backup policy to periodically back up the ECS.


The following options are provided

- Auto assign
 - i. Set the name of the cloud backup vault, which is a character string consisting of 1 to 64 characters, including letters, digits, underscores (_), and hyphens (-). The name is in the format of "vault_xxxx" by default, for example, **vault-f61e**.
 - ii. Enter the vault capacity, which is required for backing up the ECS. The vault capacity cannot be smaller than that of the ECS to be backed up. Its value ranges from the total capacity of the ECS to 10,485,760 in the unit of GB.

- iii. Select a backup policy from the drop-down list, or log in to the CBR console and configure a desired one.
 - Specify
 - i. Select an existing cloud backup vault from the drop-down list.
 - ii. Select a backup policy from the drop-down list, or log in to the CBR console and configure a desired one.
 - Do not use

Skip this configuration if CBR is not required. If you require this function after creating the ECS, log in to the CBR console and bind the desired cloud backup vault to your ECS.
4. Set **ECS Group**.

An ECS group applies the anti-affinity policy to the ECSs in it so that the ECSs are automatically allocated to different hosts. This configuration is optional.

 **NOTE**

An existing ECS attached with a local disk cannot be added to an ECS group. To use ECS group functions, select an ECS group when creating an ECS.
5. To use functions listed in **Advanced Options**, select **Configure now**. Otherwise, do not select it.
 - User Data Injection

Enables the ECS to automatically inject user data when the ECS starts for the first time. This configuration is optional.

For example, if you activate user **root** permission using script file injection, you can log in to the ECS as user **root**.

For detailed operations, see [3.7.2 Injecting User Data into ECSs](#).
 - Agency

This configuration is optional. When your ECS resources need to be shared with other accounts, or your ECS is delegated to professional personnel or team for management, the tenant administrator creates an agency in IAM and grants the ECS management permissions to the personnel or team. The delegated account can log in to the cloud system and switch to your account to manage resources. You do not need to share security credentials (such as passwords) with other accounts, ensuring the security of your account.

If you have created an agency in IAM, you can select the agency from the drop-down list and obtain specified operation permissions. For instructions about how to create an agency, see *Identity and Access Management User Guide*.
6. Click **Next: Confirm**.

2.1.5 Step 4: Confirm

Confirming the Order

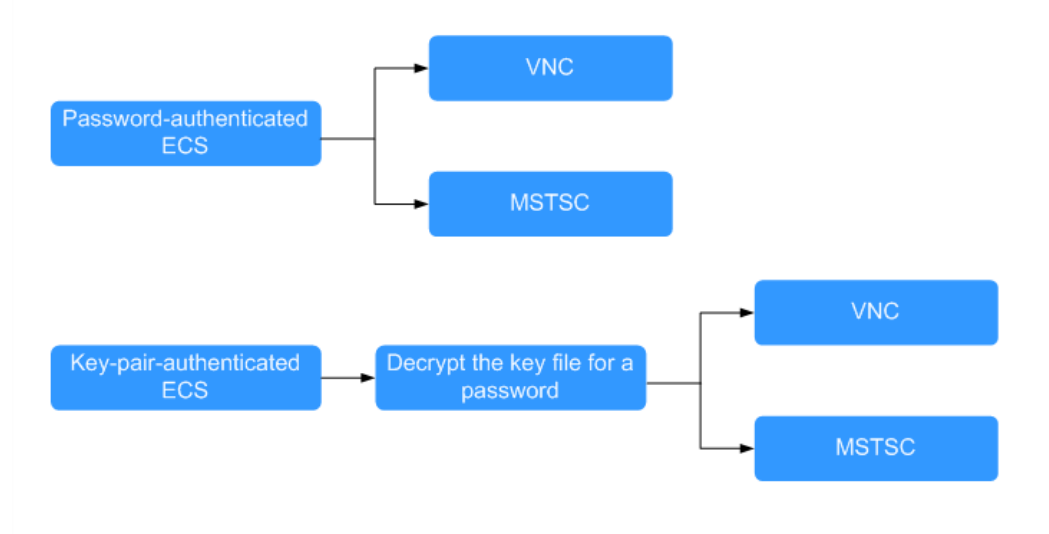
1. On the **Confirm** page, view details about the ECS configuration.
2. Configure the number of ECSs to be created.
3. Confirm the configuration and click **Apply Now**.

2.2 Logging In to an ECS

Logging In to a Windows ECS

You can log in to a Windows ECS using either VNC or MSTSC provided on the management console.

Figure 2-1 Windows ECS login modes

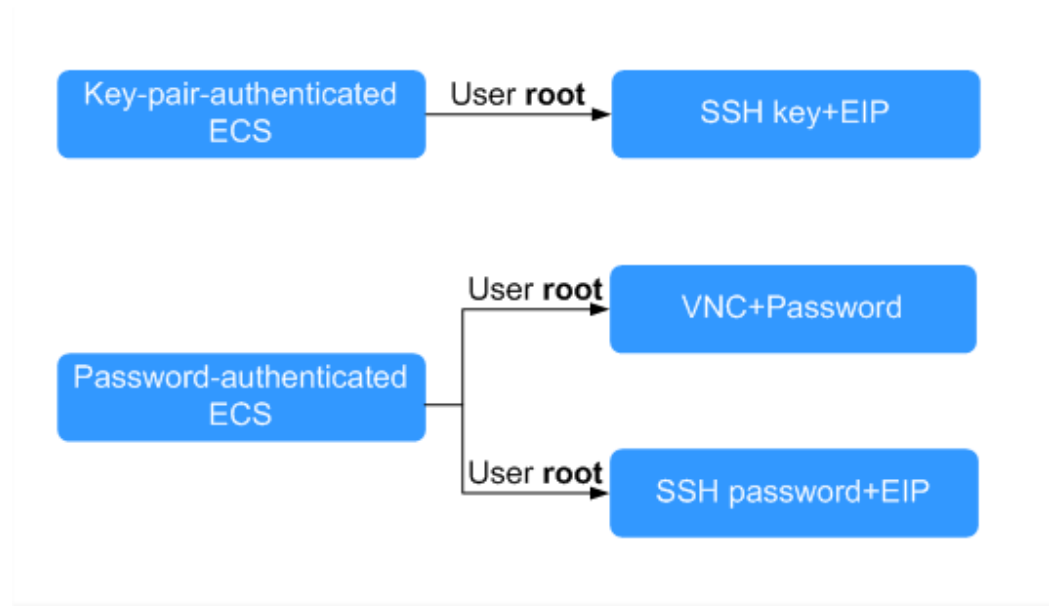


1. (Optional) Use the key file to resolve a password.
To log in to a key-pair-authenticated ECS, use the password obtaining function provided by the management console to decrypt the key file to obtain a password.
For details, see [6.4 Obtaining the Password for Logging In to a Windows ECS](#).
2. Select a login mode as required to log in to the ECS.
 - Management console (VNC)
For details, see [3.3.2 Login Using VNC](#).
 - Remote desktop connection (MSTSC)
For details, see [3.3.3 Login Using MSTSC](#).

Logging In to a Linux ECS

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

Figure 2-2 Linux ECS login modes



- To log in to a key-pair-authenticated ECS for the first time, use a tool, such as PuTTY or XShell, and the desired SSH key as user **root**. Ensure that the ECS has an EIP bound.

For instructions about how to log in to a Linux ECS using an SSH key, see [3.4.3 Login Using an SSH Key](#).

NOTE

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

- To log in to a password-authenticated ECS for the first time, use either of the following methods:
 - Management console (VNC) with login username **root**
For details about how to log in to the ECS using VNC, see [3.4.2 Login Using VNC](#).
 - For logins using an SSH password, the login username is **root** and the ECS must have an EIP bound.
For details, see [3.4.4 Login Using an SSH Password](#).

Follow-up Procedure

- If you have added a data disk during ECS creation, you must initialize the data disk after logging in to the ECS.
For details, see [2.3.1 Scenarios and Disk Partitions](#).
- Certain ECSs require the installation of a driver after you log in to them. For details about available ECS types as well as their functions and usage, see "Notes" in [1.5.3 ECS Types](#).

2.3 Initializing EVS Data Disks

2.3.1 Scenarios and Disk Partitions

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

Scenarios

After a disk is attached to a server, you need to log in to the server to initialize the disk, that is, format the disk. You must initialize a disk before accessing it.

- System disk
A system disk does not require manual initialization because it is automatically created and initialized upon server creation. The default disk partition style is master boot record (MBR).
- Data disk
 - If a data disk is created along with a server, it will be automatically attached to the server.
 - If a data disk is created separately, you need to manually attach it to a server.

In both cases, you must initialize the data disk before using it. Choose a proper disk partition style based on your service plan.

Disk Partition Styles

[Table 2-2](#) lists the common disk partition styles. In Linux, different disk partition styles require different partitioning tools.

Table 2-2 Disk partition styles

Disk Partition Style	Maximum Disk Capacity Supported	Maximum Number of Partitions Supported	Linux Partitioning Tool
Master Boot Record (MBR)	2 TB	<ul style="list-style-type: none"> • 4 primary partitions • 3 primary partitions and 1 extended partition <p>With MBR, one may create several primary partitions and an extended partition. An extended partition must be divided into several logical partitions before use. For example, if 6 partitions need to be created, you can create the partitions in the following two ways:</p> <ul style="list-style-type: none"> • 3 primary partitions and 1 extended partition, with the extended partition divided into 3 logical partitions • 1 primary partition and 1 extended partition, with the extended partition divided into 5 logical partitions 	<ul style="list-style-type: none"> • fdisk • parted
GUID Partition Table (GPT)	18 EB 1 EB = 1048576 TB	Unlimited Disk partitions created using GPT are not categorized.	parted

NOTICE

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Because a data disk currently supports up to 32 TB, use the GPT partition style if your disk capacity is larger than 2 TB.

If you change the disk partition style after the disk has been used, the data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

2.3.2 Initializing a Windows Data Disk (Windows Server 2008)

Scenarios

This topic uses Windows Server 2008 R2 Enterprise 64bit to describe how to initialize a data disk attached to a server running Windows.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is larger than 2 TB. For details, see [2.3.6 Initializing a Windows Data Disk Larger Than 2 TB \(Windows Server 2008\)](#). For details about disk partition styles, see [2.3.1 Scenarios and Disk Partitions](#).

The method for initializing a disk varies depending on the OS running on the server. This document is used for reference only. For the detailed operations and differences, see the product documents of the corresponding OS.

Prerequisites

- A data disk has been attached to a server and has not been initialized.
- You have logged in to the server.
 - For how to log in to an ECS, see the *Elastic Cloud Server User Guide*.
 - For how to log in to a BMS, see the *Bare Metal Server User Guide*.

Procedure

Step 1 On the desktop of the server, right-click **Computer** and choose **Manage** from the shortcut menu.

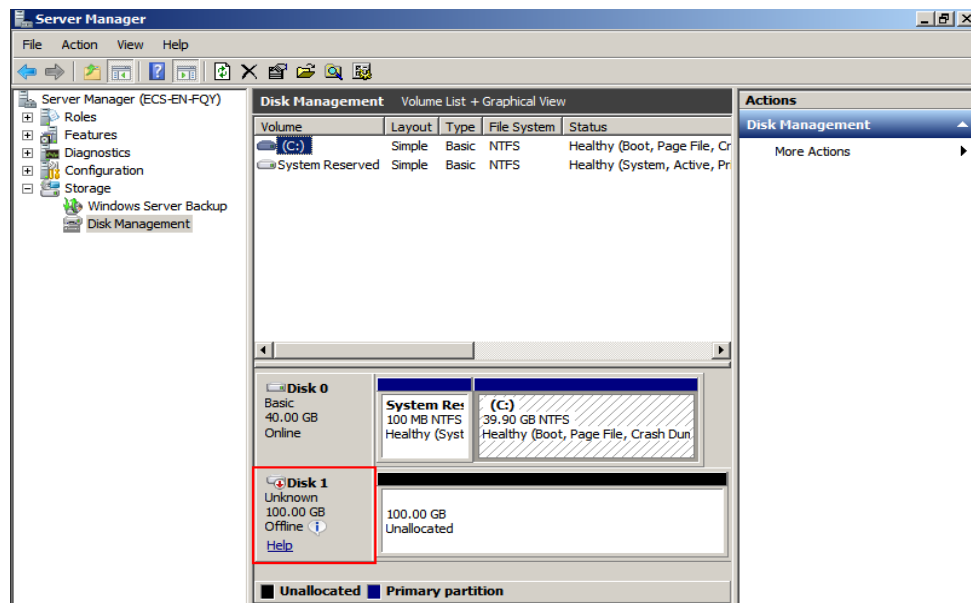
The **Server Manager** window is displayed.

Step 2 In the navigation tree, choose **Storage > Disk Management**.

The **Disk Management** window is displayed.

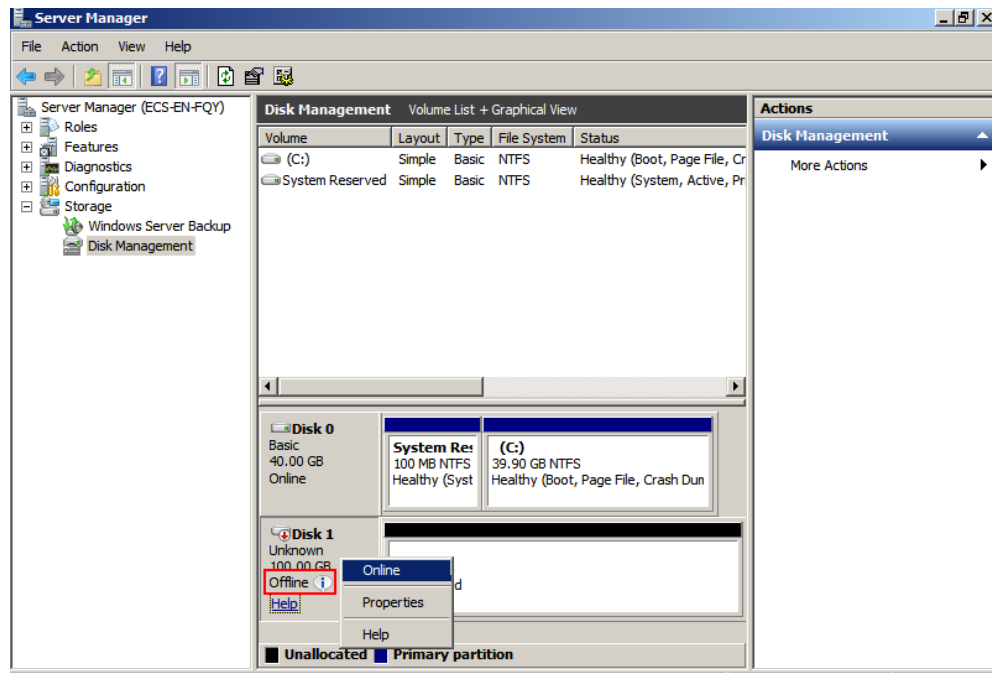
- If [Figure 2-3](#) is displayed, the new disk is offline. Go to [Step 3](#).
- If [Figure 2-6](#) is displayed, the **Initialize Disk** window is prompted. Go to [Step 5](#).

Figure 2-3 Disk Management



Step 3 Disks are displayed in the right pane. In the **Disk 1** area, right-click **Offline** and choose **Online** from the shortcut menu to online the disk.

Figure 2-4 Online the disk

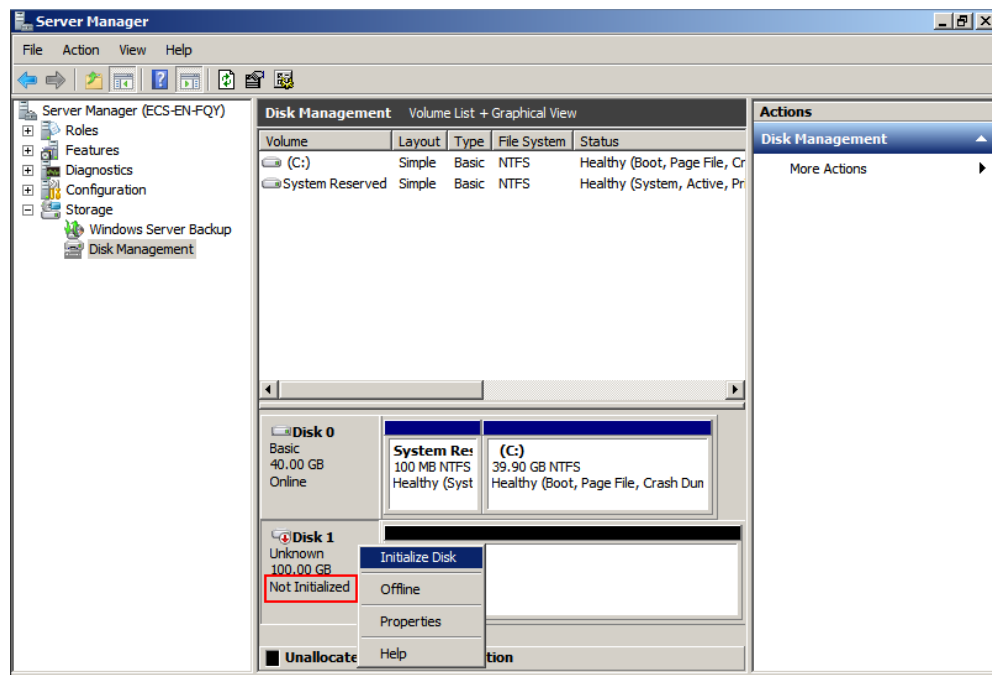


NOTE

If the disk is offline, you need to online the disk before initializing it.

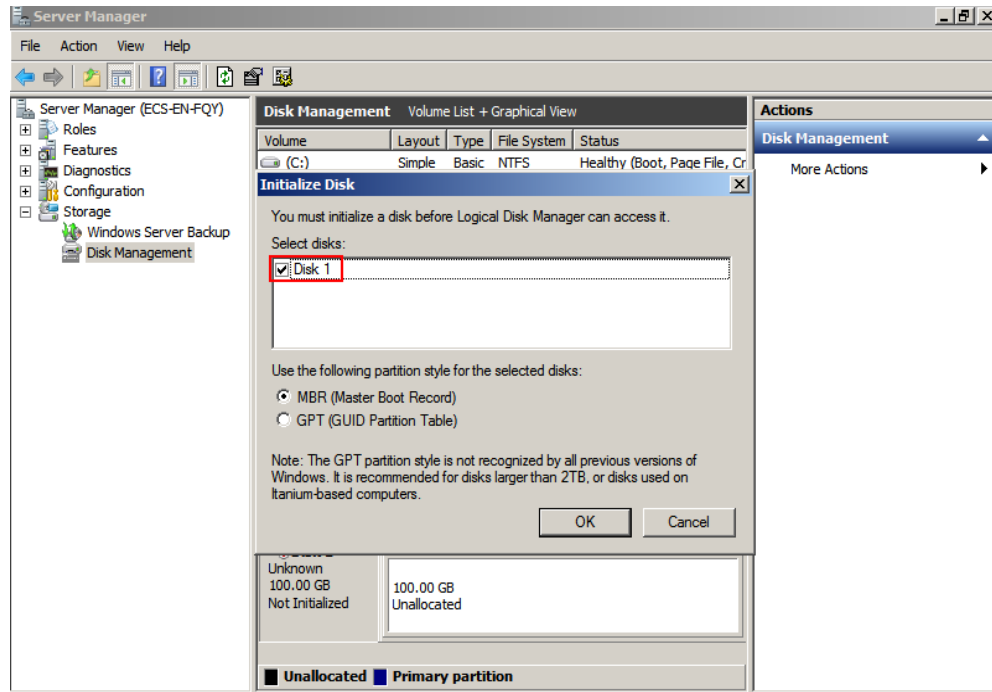
- Step 4** After making the disk online, the disk status changes from **Offline** to **Not Initialized**. Right-click the disk status and choose **Initialize Disk** from the shortcut menu, as shown in [Figure 2-5](#).

Figure 2-5 Initialize Disk



Step 5 In the **Initialize Disk** dialog box, select the target disk, click **MBR (Master Boot Record)** or **GPT (GUID Partition Table)**, and click **OK**, as shown in **Figure 2-6**.

Figure 2-6 Unallocated space



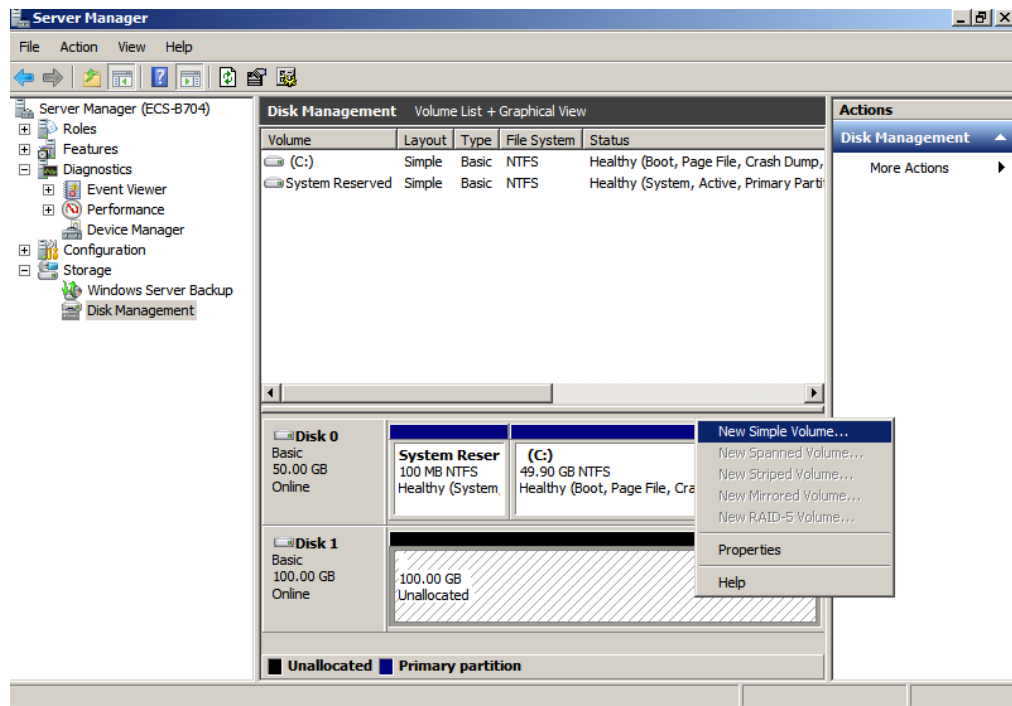
NOTICE

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Because a data disk currently supports up to 32 TB, use the GPT partition style if your disk capacity is larger than 2 TB.

If you change the disk partition style after the disk has been used, the data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

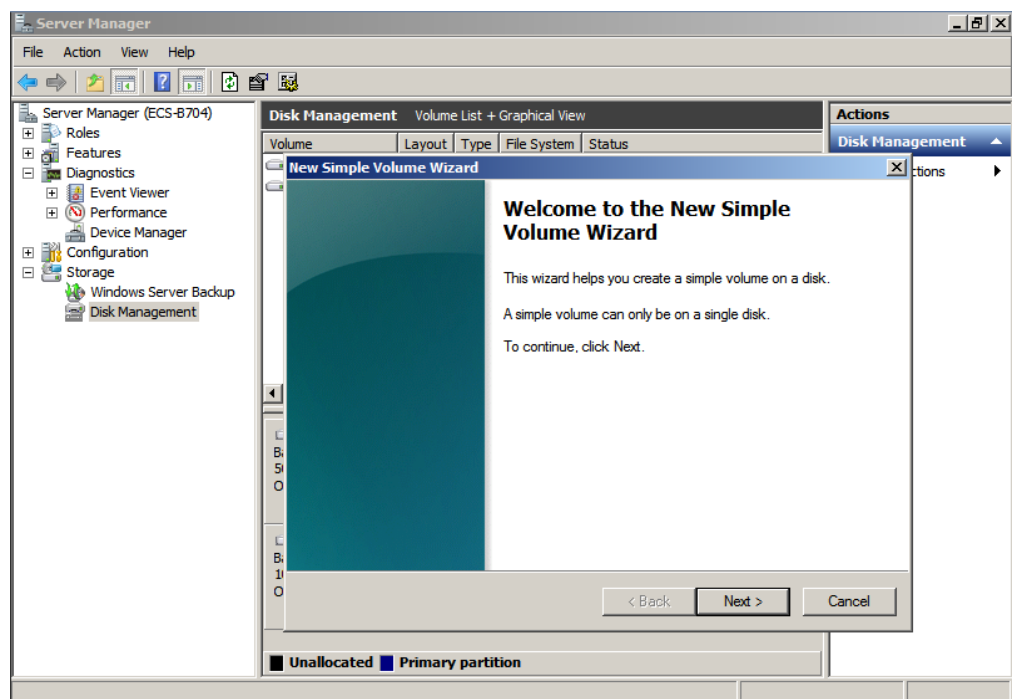
Step 6 Right-click at the unallocated space and choose **New Simple Volume** from the shortcut menu, as shown in **Figure 2-7**.

Figure 2-7 New Simple Volume



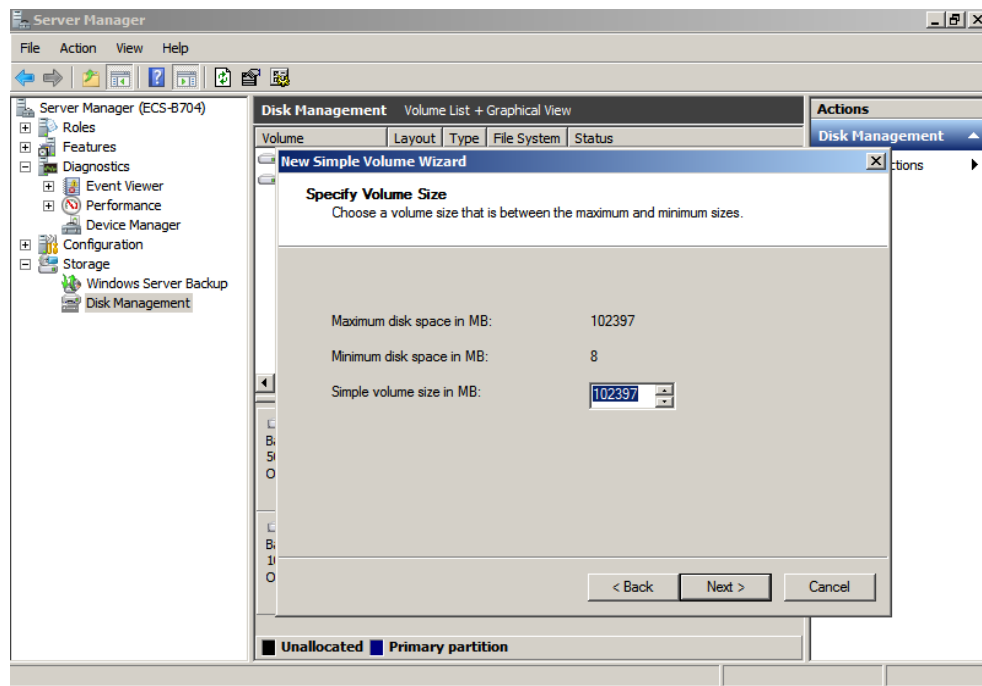
Step 7 On the displayed **New Simple Volume Wizard** window, click **Next**.

Figure 2-8 New Simple Volume Wizard



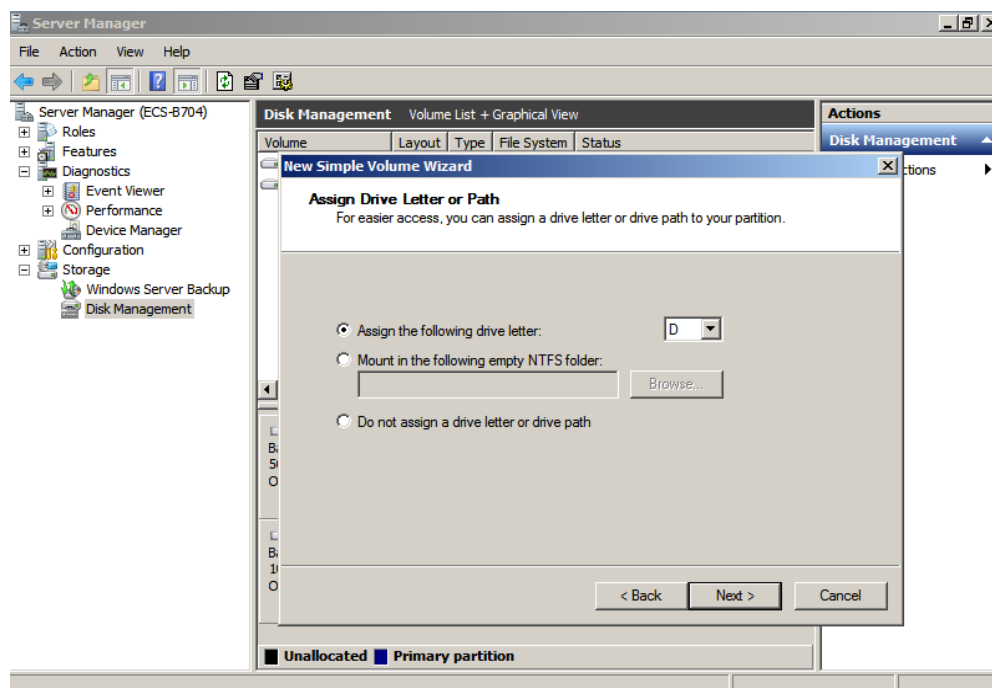
Step 8 Specify the volume size and click **Next**. The default value is the maximum size.

Figure 2-9 Specify Volume Size



Step 9 Assign the driver letter and click **Next**.

Figure 2-10 Assign Driver Letter or Path



Step 10 Select **Format this volume with the following settings**, set parameters based on the actual requirements, and select **Perform a quick format**. Then, click **Next**.

Figure 2-11 Format Partition

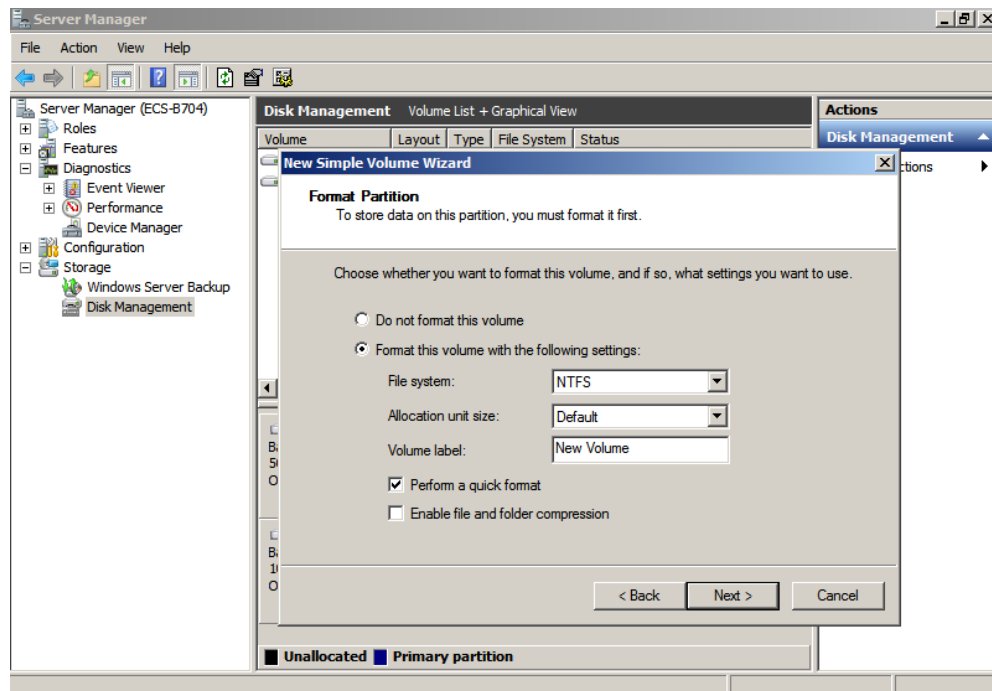
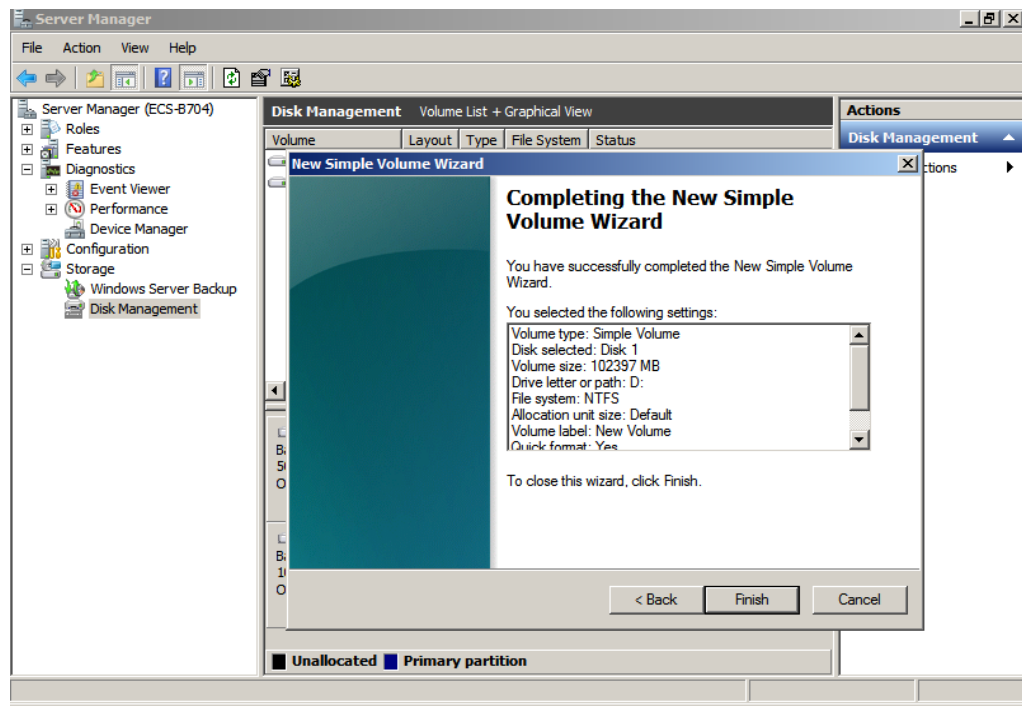


Figure 2-12 Completing the partition creation

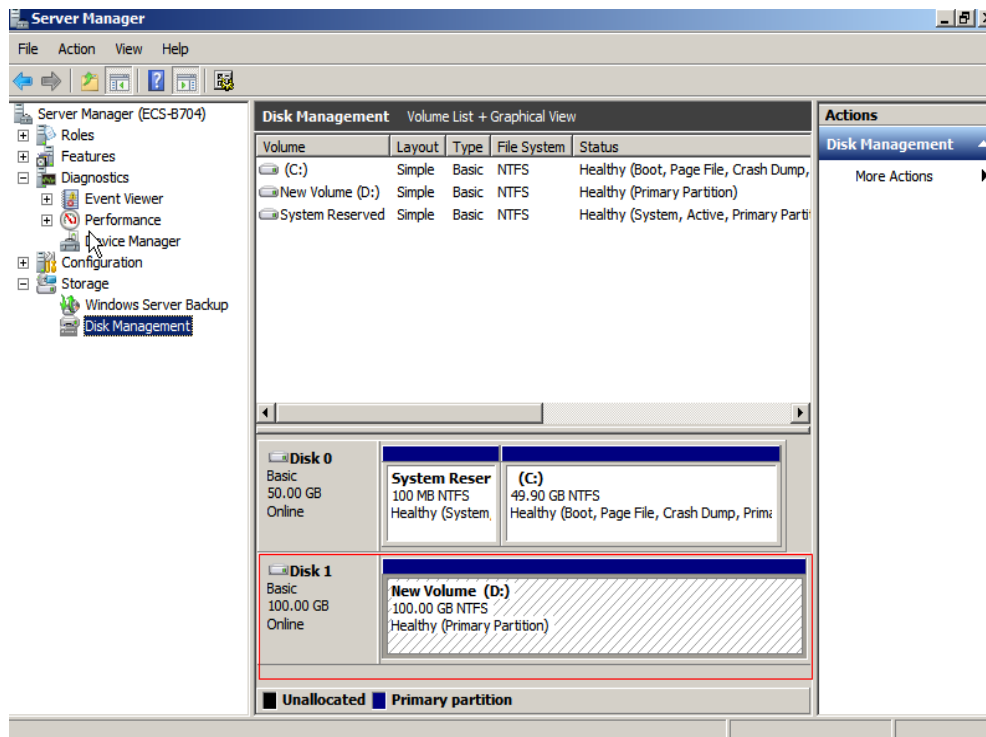


NOTICE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

- Step 11** Click **Finish**. Wait for the initialization to complete. When the volume status changes to **Healthy**, the initialization has finished successfully, as shown in [Figure 2-13](#).

Figure 2-13 Disk initialization succeeded



----End

2.3.3 Initializing a Windows Data Disk (Windows Server 2016)

Scenarios

This topic uses Windows Server 2016 Standard 64bit to describe how to initialize a data disk attached to a server running Windows.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is larger than 2 TB. For details, see [2.3.6 Initializing a Windows Data Disk Larger Than 2 TB \(Windows Server 2008\)](#). For details about disk partition styles, see [2.3.1 Scenarios and Disk Partitions](#).

The method for initializing a disk varies depending on the OS running on the server. This document is used for reference only. For the detailed operations and differences, see the product documents of the corresponding OS.

Prerequisites

- A data disk has been attached to a server and has not been initialized.
- You have logged in to the server.
 - For how to log in to an ECS, see the *Elastic Cloud Server User Guide*.

- For how to log in to a BMS, see the *Bare Metal Server User Guide*.

Procedure

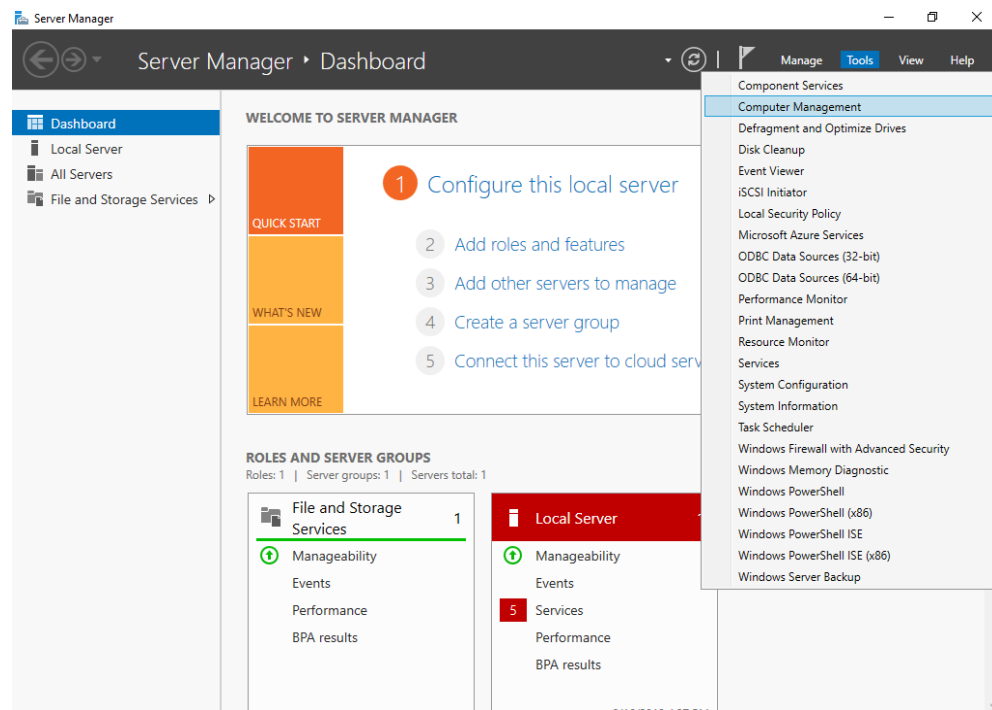
Step 1 On the desktop of the server, click the start icon in the lower left corner.

The **Windows Server** window is displayed.

Step 2 Click **Server Manager**.

The **Server Manager** window is displayed.

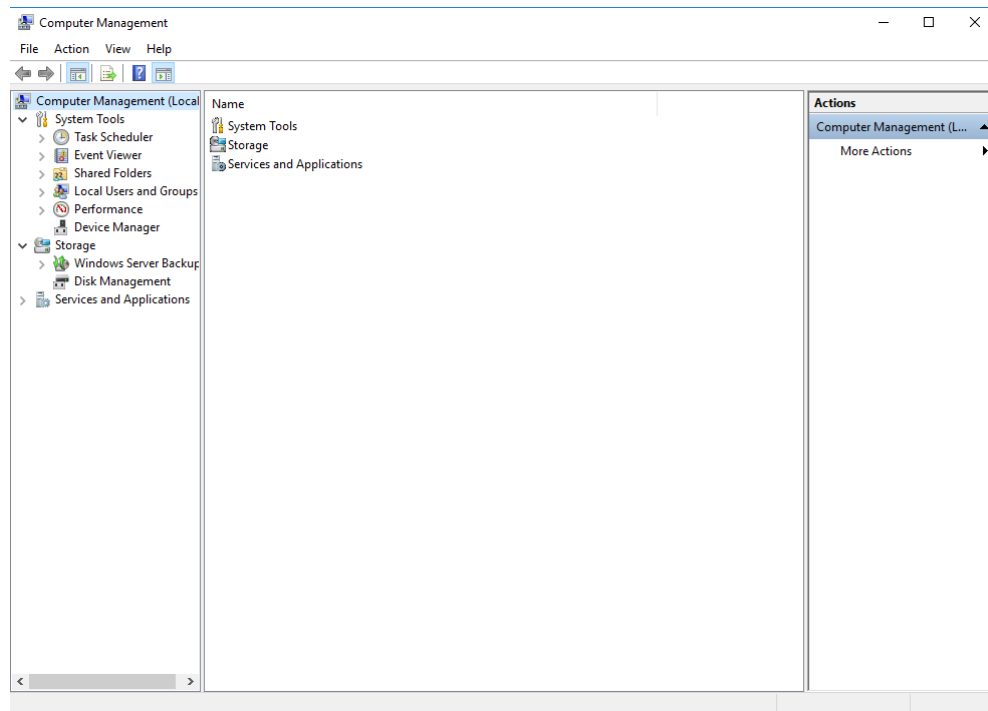
Figure 2-14 Server Manager



Step 3 In the upper right corner, choose **Tools > Computer Management**.

The **Computer Management** window is displayed.

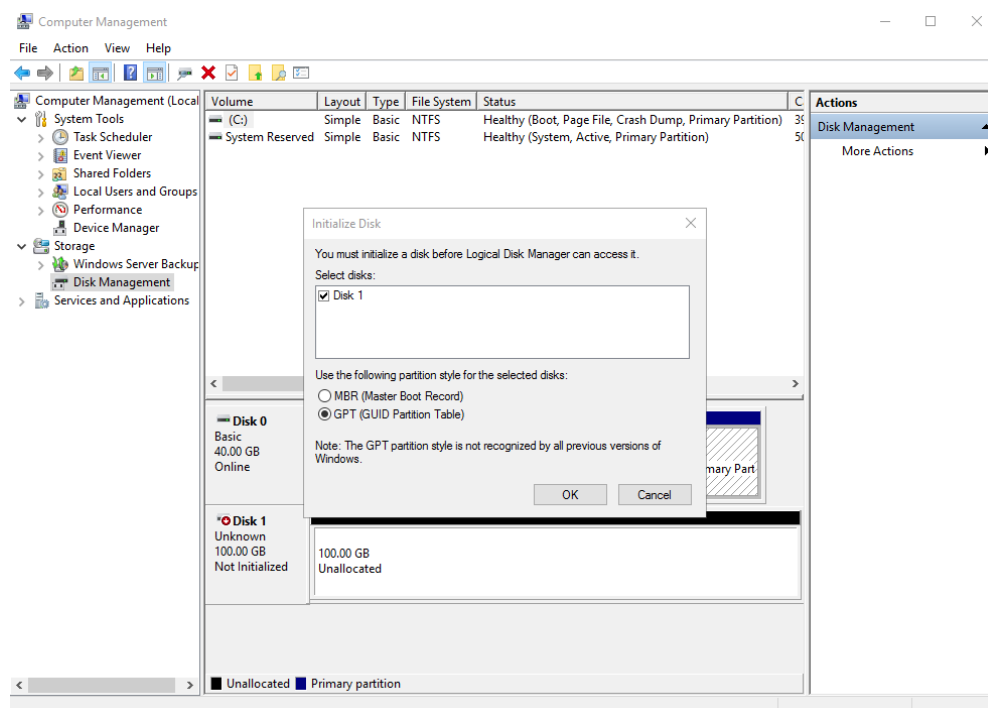
Figure 2-15 Computer Management



Step 4 Choose **Storage > Disk Management**.

Disks are displayed in the right pane. If there is a disk that is not initialized, the system will prompt you with the **Initialize Disk** dialog box.

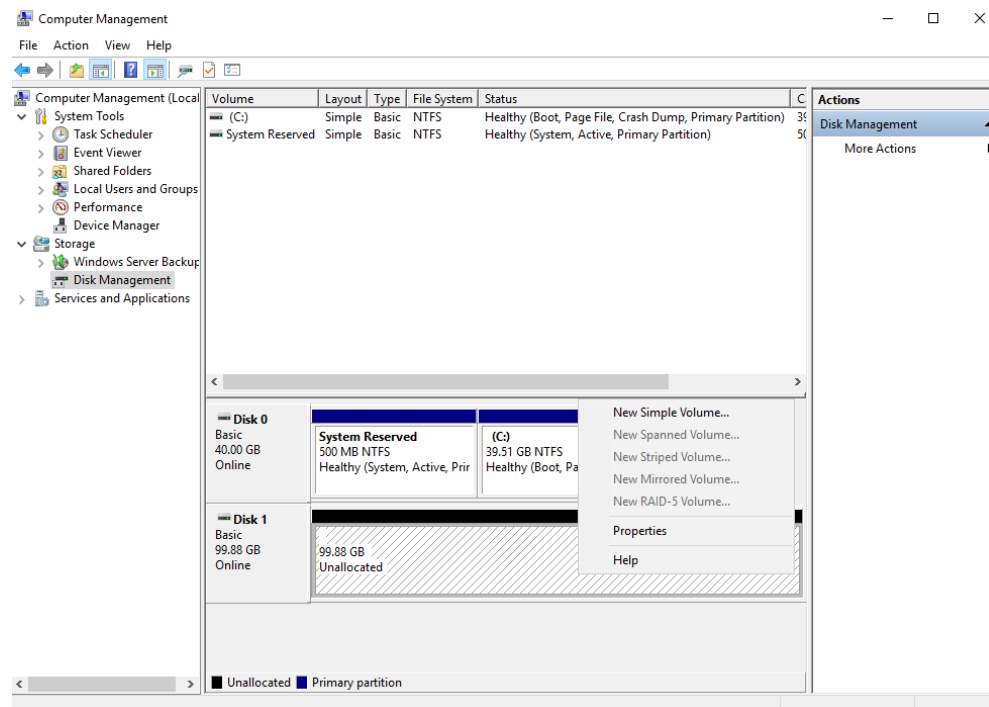
Figure 2-16 Disk list



Step 5 In the **Initialize Disk** dialog box, the to-be-initialized disk is selected. Select a disk partition style and click **OK**. In this example, **GPT (GUID Partition Table)** is selected.

The **Computer Management** window is displayed.

Figure 2-17 Computer Management (Windows Server 2016)



NOTICE

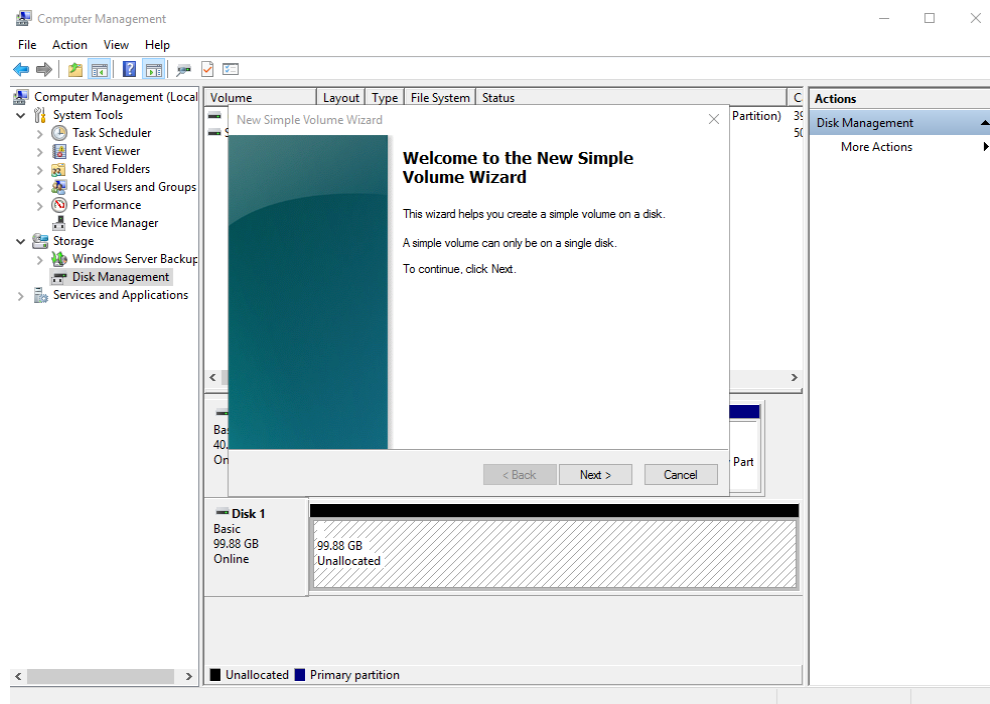
The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Because a data disk currently supports up to 32 TB, use the GPT partition style if your disk capacity is larger than 2 TB.

If you change the disk partition style after the disk has been used, the data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

Step 6 Right-click at the unallocated disk space and choose **New Simple Volume** from the shortcut menu.

The **New Simple Volume Wizard** window is displayed.

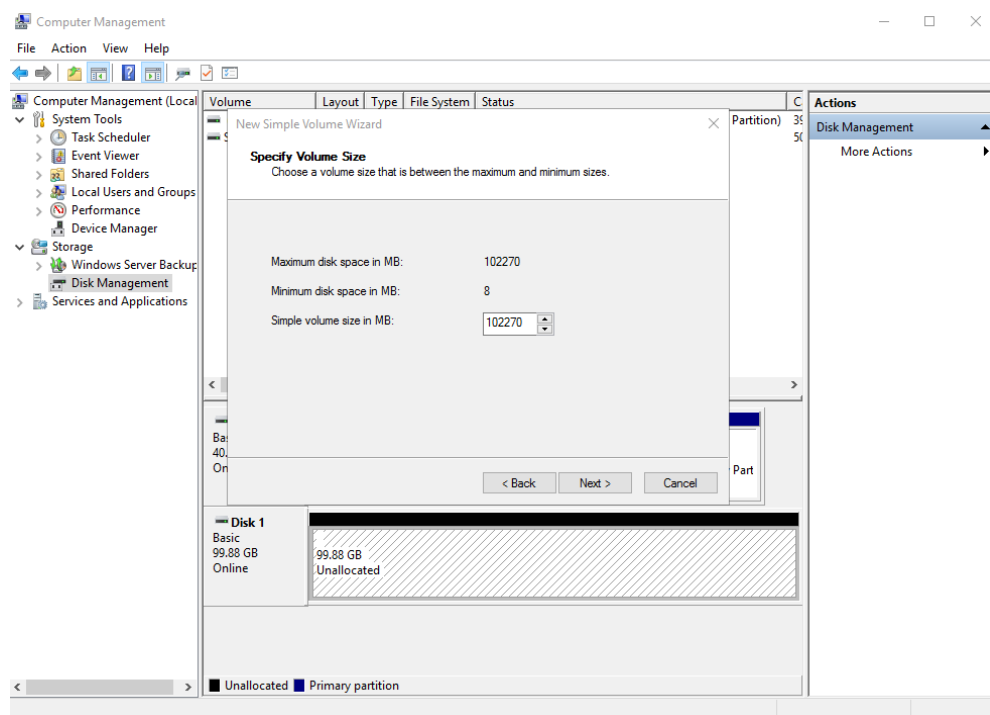
Figure 2-18 New Simple Volume Wizard (Windows Server 2016)



Step 7 Follow the prompts and click **Next**.

The **Specify Volume Size** page is displayed.

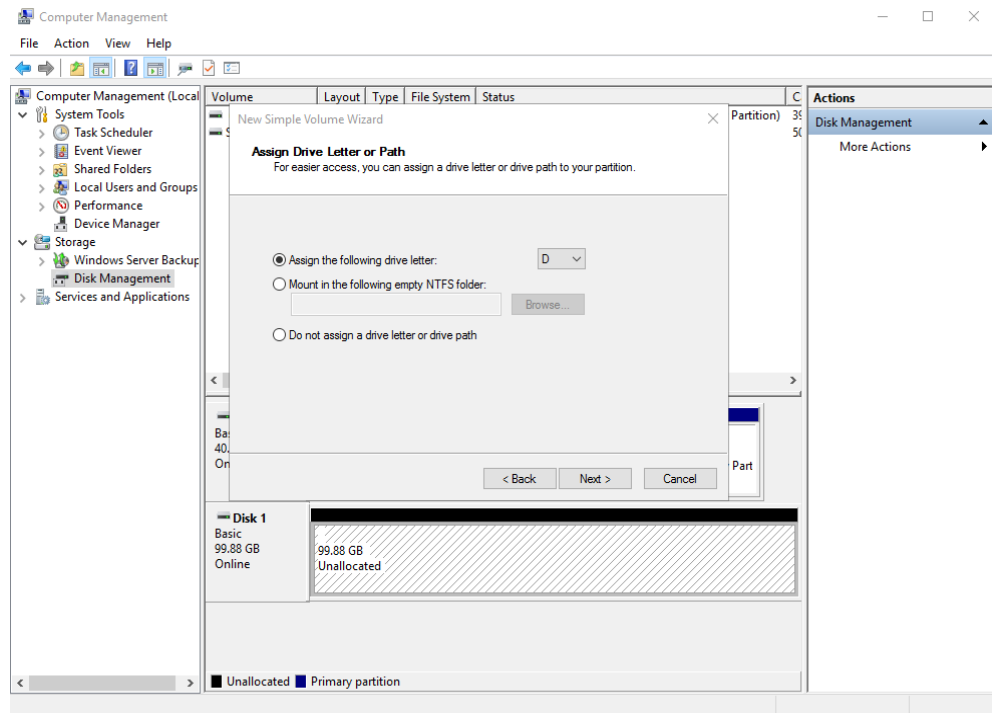
Figure 2-19 Specify Volume Size (Windows Server 2016)



Step 8 Specify the volume size and click **Next**. The system selects the maximum volume size by default. You can specify the volume size as required. In this example, the default setting is used.

The **Assign Drive Letter or Path** page is displayed.

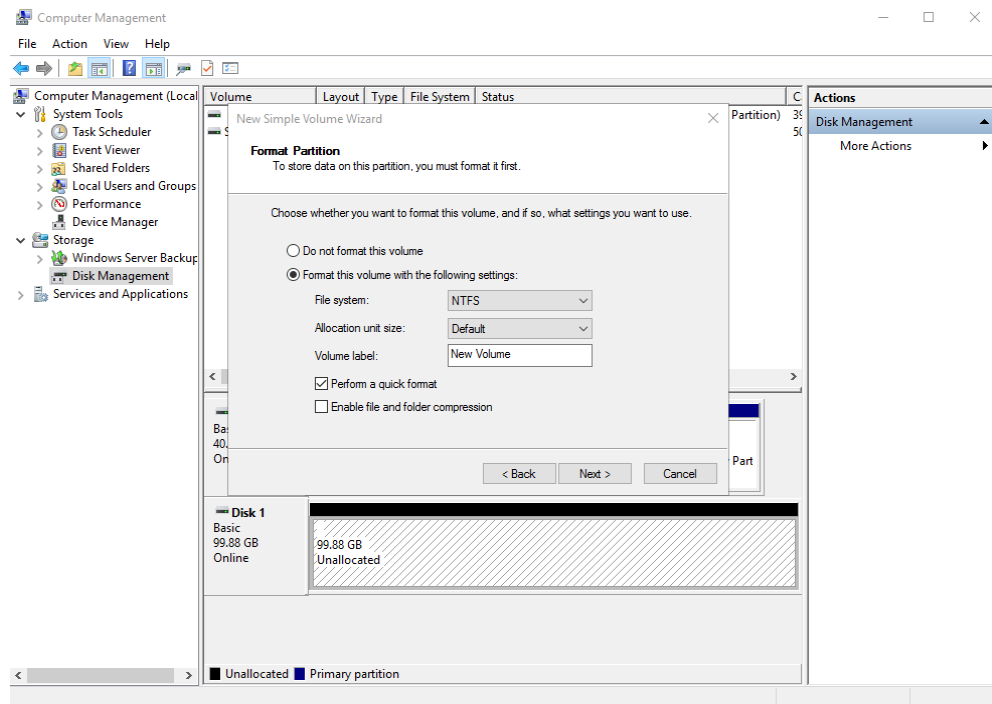
Figure 2-20 Assign Driver Letter or Path (Windows Server 2016)



Step 9 Assign a drive letter or path to your partition and click **Next**. The system assigns drive letter D by default. In this example, the default setting is used.

The **Format Partition** page is displayed.

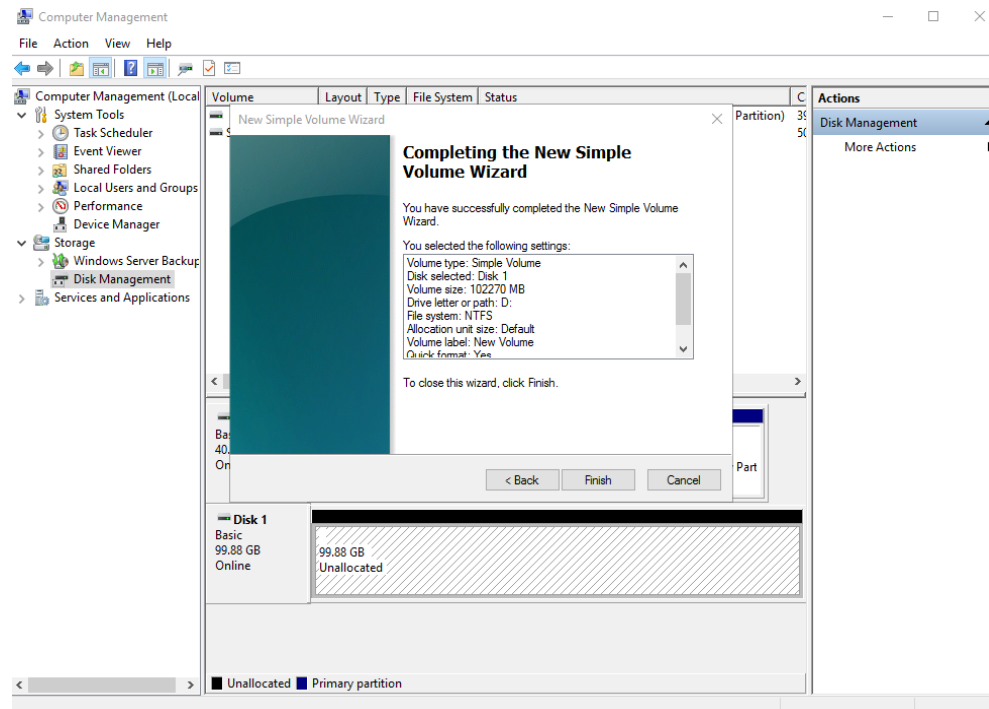
Figure 2-21 Format Partition (Windows Server 2016)



Step 10 Specify format settings and click **Next**. The system selects the NTFS file system by default. You can specify the file system type as required. In this example, the default setting is used.

The **Completing the New Simple Volume Wizard** page is displayed.

Figure 2-22 Completing the New Simple Volume Wizard (Windows Server 2016)



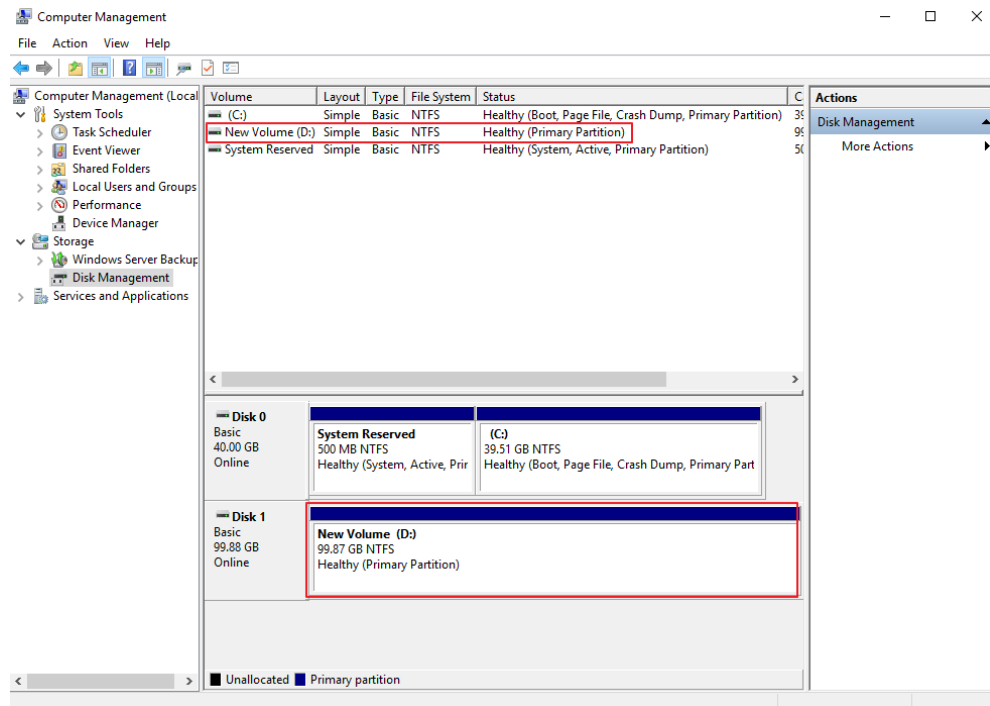
NOTICE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

Step 11 Click **Finish**.

Wait for the initialization to complete. When the volume status changes to **Healthy**, the initialization has finished successfully, as shown in [Figure 2-23](#).

Figure 2-23 Disk initialization succeeded (Windows Server 2016)




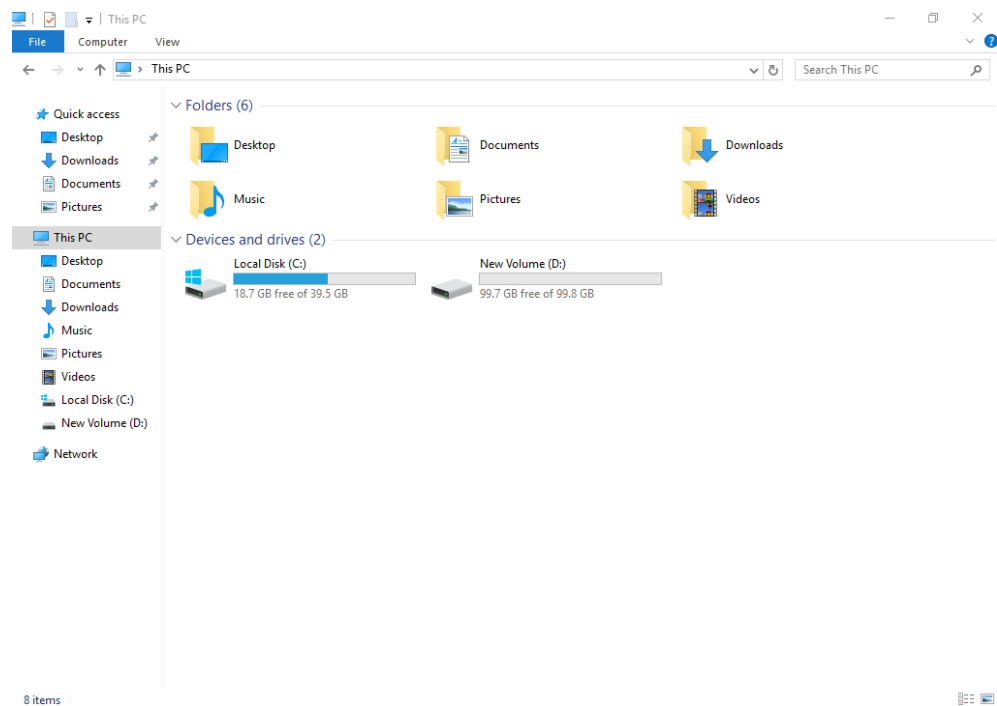
Step 12 After the volume is created, click  on the task bar and check whether a new volume appears in **This PC**. In this example, New Volume (D:) is the new volume. If New Volume (D:) appears, the disk is successfully initialized and no further action is required.

Figure 2-24 This PC (Windows Server 2016)

----End

2.3.4 Initializing a Linux Data Disk (fdisk)

Scenarios

This topic uses CentOS 7.4 64bit to describe how to initialize a data disk attached to a server running Linux and use fdisk to partition the data disk.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is larger than 2 TB. In Linux, if you choose to use the GPT partition style, the fdisk partitioning tool cannot be used. Use the parted partitioning tool instead. For details about disk partition styles, see [2.3.1 Scenarios and Disk Partitions](#).

The method for initializing a disk varies depending on the OS running on the server. This document is used for reference only. For the detailed operations and differences, see the product documents of the corresponding OS.

Prerequisites

- A data disk has been attached to a server and has not been initialized.
- You have logged in to the server.
 - For how to log in to an ECS, see the *Elastic Cloud Server User Guide*.
 - For how to log in to a BMS, see the *Bare Metal Server User Guide*.

Creating and Mounting a Partition

The following example shows you how a new primary partition can be created on a new data disk that has been attached to a server. The primary partition will be

created using fdisk, and MBR is the default partition style. Furthermore, the partition will be formatted using the ext4 file system, mounted on **/mnt/sdc**, and configured automatic mounting at system start.

Step 1 Run the following command to query information about the new data disk:

fdisk -l

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# fdisk -l

Disk /dev/vda: 42.9 GB, 42949672960 bytes, 83886080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000bcb4e

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1 *        2048     83886079     41942016   83  Linux

Disk /dev/vdb: 107.4 GB, 107374182400 bytes, 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

In the command output, the server contains two disks. **/dev/vda** is the system disk, and **/dev/vdb** is the new data disk.

Step 2 Run the following command to enter fdisk to partition the new data disk:

fdisk *New data disk*

In this example, run the following command:

fdisk /dev/vdb

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# fdisk /dev/vdb
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.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0x38717fc1.

Command (m for help):
```

Step 3 Enter **n** and press **Enter** to create a new partition.

Information similar to the following is displayed:

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

There are two types of disk partitions:

- Choosing **p** creates a primary partition.
- Choosing **e** creates an extended partition.

 **NOTE**

If the MBR partition style is used, a maximum of 4 primary partitions, or 3 primary partitions and 1 extended partition can be created. The extended partition cannot be used directly and must be divided into logical partitions before use.

Disk partitions created using GPT are not categorized.

Step 4 In this example, a primary partition is created. Therefore, enter **p** and press **Enter** to create a primary partition.

Information similar to the following is displayed:

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

Partition number indicates the serial number of the primary partition. The value ranges from **1** to **4**.

Step 5 Enter the serial number of the primary partition and press **Enter**. Primary partition number **1** is used in this example. One usually starts with partition number **1** when partitioning an empty disk.

Information similar to the following is displayed:

```
Partition number (1-4, default 1): 1
First sector (2048-209715199, default 2048):
```

First sector indicates the start sector. The value ranges from **2048** to **209715199**, and the default value is **2048**.

Step 6 Select the default start sector **2048** and press **Enter**.

The system displays the start and end sectors of the partition's available space. You can customize the value within this range or use the default value. The start sector must be smaller than the partition's end sector.

Information similar to the following is displayed:

```
First sector (2048-209715199, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-209715199, default 209715199):
```

Last sector indicates the end sector. The value ranges from **2048** to **209715199**, and the default value is **209715199**.

Step 7 Select the default end sector **209715199** and press **Enter**.

The system displays the start and end sectors of the partition's available space. You can customize the value within this range or use the default value. The start sector must be smaller than the partition's end sector.

Information similar to the following is displayed:

```
Last sector, +sectors or +size{K,M,G} (2048-209715199, default 209715199):
Using default value 209715199
Partition 1 of type Linux and of size 100 GiB is set
Command (m for help):
```

A primary partition has been created for the new data disk.

Step 8 Enter **p** and press **Enter** to view details about the new partition.

Information similar to the following is displayed:

```
Command (m for help): p
```

```
Disk /dev/vdb: 107.4 GB, 107374182400 bytes, 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x38717fc1
```

Device	Boot	Start	End	Blocks	Id	System
/dev/vdb1		2048	209715199	104856576	83	Linux

```
Command (m for help):
```

Details about the **/dev/vdb1** partition are displayed.

Step 9 Enter **w** and press **Enter** to write the changes to the partition table.

Information similar to the following is displayed:

```
Command (m for help): w
The partition table has been altered!
```

```
Calling ioctl() to re-read partition table.
Syncing disks.
```

The partition is created.

NOTE

In case that you want to discard the changes made before, you can exit fdisk by entering **q**.

Step 10 Run the following command to synchronize the new partition table to the OS:

```
partprobe
```

Step 11 Run the following command to set the file system format for the new partition:

```
mkfs -t File system format /dev/vdb1
```

In this example, run the following command to set the **ext4** file system for the new partition:

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

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# mkfs -t ext4 /dev/vdb1
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
6553600 inodes, 26214144 blocks
1310707 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2174746624
800 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872
```

```
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

The formatting takes a period of time. Observe the system running status and do not exit.

NOTICE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

Step 12 Run the following command to create a mount point:

```
mkdir Mount point
```

In this example, run the following command to create the **/mnt/sdc** mount point:

```
mkdir /mnt/sdc
```

Step 13 Run the following command to mount the new partition on the created mount point:

```
mount Disk partition Mount point
```

In this example, run the following command to mount the new partition **/dev/vdb1** on **/mnt/sdc**:

```
mount /dev/vdb1 /mnt/sdc
```

Step 14 Run the following command to view the mount result:

```
df -TH
```

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/vda1       ext4      43G  1.9G  39G   5% /
devtmpfs        devtmpfs  2.0G   0  2.0G   0% /dev
tmpfs           tmpfs     2.0G   0  2.0G   0% /dev/shm
tmpfs           tmpfs     2.0G  9.1M  2.0G   1% /run
tmpfs           tmpfs     2.0G   0  2.0G   0% /sys/fs/cgroup
tmpfs           tmpfs     398M   0  398M   0% /run/user/0
/dev/vdb1       ext4     106G  63M 101G   1% /mnt/sdc
```

New partition **/dev/vdb1** is mounted on **/mnt/sdc**.

NOTE

If the server is restarted, the mounting will become invalid. You can set automatic mounting for partitions at system start by modifying the **/etc/fstab** file. For details, see [Setting Automatic Mounting at System Start](#).

----End

Setting Automatic Mounting at System Start

To automatically mount disk partitions at system start, do not specify partitions, for example **/dev/vdb1**, in **/etc/fstab** because the sequence of cloud devices, and therefore their names may change during the server stop and start. You are advised to use the universally unique identifier (UUID) in **/etc/fstab** to set automatic mounting at system start.

NOTE

UUID is the unique character string for disk partitions in a Linux system.

Step 1 Run the following command to query the partition UUID:

blkid *Disk partition*

In this example, run the following command to query the UUID of the **/dev/vdb1** partition:

blkid /dev/vdb1

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# blkid /dev/vdb1
/dev/vdb1: UUID="0b3040e2-1367-4abb-841d-ddb0b92693df" TYPE="ext4"
```

The UUID of the **/dev/vdb1** partition is displayed.

Step 2 Run the following command to open the **fstab** file using the vi editor:

vi /etc/fstab

Step 3 Press **i** to enter the editing mode.

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

```
UUID=0b3040e2-1367-4abb-841d-ddb0b92693df /mnt/sdc          ext4  defaults  0 2
```

The preceding content is used for reference only. Add the information that is used in the environment. The parameters are described as follows:

- The first column indicates the partition UUID obtained in [Step 1](#).
- The second column indicates the directory on which the partition is mounted. You can query the mount point using the **df -TH** command.
- The third column indicates the file system format of the partition. You can query the file system format using the **df -TH** command.
- The fourth column indicates the partition mount option. Normally, this parameter is set to **defaults**.
- The fifth column indicates the Linux dump backup option.
 - **0**: not use Linux dump backup. Normally, dump backup is not used, and you can set this parameter to **0**.
 - **1**: use Linux dump backup.
- The sixth column indicates the fsck option, that is, whether to use fsck to check the attached disk during startup.
 - **0**: not use fsck.
 - If the mount point is the root partition (**/**), this parameter must be set to **1**.

When this parameter is set to **1** for the root partition, this parameter for other partitions must start with **2** so that the system checks the partitions in the ascending order of the values.

Step 5 Press **Esc**, enter **:wq**, and press **Enter**.

The system saves the configurations and exits the vi editor.

Step 6 Perform the following operations to verify the automatic mounting function:

1. Run the following command to unmount the partition:

umount *Disk partition*

In this example, run the following command:

```
umount /dev/vdb1
```

2. Run the following command to reload all the content in the `/etc/fstab` file:

```
mount -a
```

3. Run the following command to query the file system mounting information:

```
mount | grep Mount point
```

In this example, run the following command:

```
mount | grep /mnt/sdc
```

If information similar to the following is displayed, the automatic mounting function takes effect:

```
root@ecs-test-0001 ~]# mount | grep /mnt/sdc  
/dev/vdb1 on /mnt/sdc type ext4 (rw,relatime,data=ordered)
```

----End

2.3.5 Initializing a Linux Data Disk (parted)

Scenarios

This topic uses CentOS 7.4 64bit to describe how to initialize a data disk attached to a server running Linux and use parted to partition the data disk.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is larger than 2 TB. In Linux, if you choose to use the GPT partition style, the fdisk partitioning tool cannot be used. Use the parted partitioning tool instead. For details about disk partition styles, see [2.3.1 Scenarios and Disk Partitions](#).

The method for initializing a disk varies depending on the OS running on the server. This document is used for reference only. For the detailed operations and differences, see the product documents of the corresponding OS.

Prerequisites

- A data disk has been attached to a server and has not been initialized.
- You have logged in to the server.
 - For how to log in to an ECS, see the *Elastic Cloud Server User Guide*.
 - For how to log in to a BMS, see the *Bare Metal Server User Guide*.

Creating and Mounting a Partition

The following example shows you how a new partition can be created on a new data disk that has been attached to a server. The partition will be created using parted, and GPT is used as the partition style. Furthermore, the partition will be formatted using the ext4 file system, mounted on `/mnt/sdc`, and configured automatic mounting at system start.

- Step 1** Run the following command to query information about the new data disk:

```
lsblk
```

Information similar to the following is displayed:

```
root@ecs-test-0001 ~]# lsblk
NAME MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda   253:0   0  40G  0 disk
└─vda1 253:1   0  40G  0 part /
vdb   253:16  0 100G  0 disk
```

In the command output, the server contains two disks. **/dev/vda** is the system disk, and **/dev/vdb** is the new data disk.

Step 2 Run the following command to enter parted to partition the new data disk:

```
parted New data disk
```

In this example, run the following command:

```
parted /dev/vdb
```

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# parted /dev/vdb
GNU Parted 3.1
Using /dev/vdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted)
```

Step 3 Enter **p** and press **Enter** to view the current disk partition style.

Information similar to the following is displayed:

```
(parted) p
Error: /dev/vdb: unrecognised disk label
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 107GB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:
(parted)
```

In the command output, the **Partition Table** value is **unknown**, indicating that no partition style is set for the new disk.

Step 4 Run the following command to set the disk partition style:

```
mklabel Disk partition style
```

In this example, run the following command to set the partition style to GPT:
(Disk partition styles can be MBR or GPT.)

```
mklabel gpt
```

NOTICE

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Because a data disk currently supports up to 32 TB, use the GPT partition style if your disk capacity is larger than 2 TB.

If you change the disk partition style after the disk has been used, the data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

Step 5 Enter **p** and press **Enter** to view the disk partition style.

Information similar to the following is displayed:

```
(parted) mklabel gpt
(parted) p
```

```
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 107GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number Start End Size File system Name Flags
(parted)
```

In the command output, the **Partition Table** value is **gpt**, indicating that the disk partition style is GPT.

Step 6 Enter **unit s** and press **Enter** to set the measurement unit of the disk to sector.

Step 7 Run the following command and press **Enter**:

```
mkpart Partition name Start sector End sector
```

In this example, run the following command:

```
mkpart test 2048s 100%
```

In this example, one partition is created for the new data disk. Variable *2048s* indicates the disk start sector, and variable *100%* indicates the disk end sector. The two values are used for reference only. You can determine the number of partitions and the partition size based on your service requirements.

Information similar to the following is displayed:

```
(parted) mkpart opt 2048s 100%
(parted)
```

Step 8 Enter **p** and press **Enter** to view details about the new partition.

Information similar to the following is displayed:

```
(parted) p
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 209715200s
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number Start End Size File system Name Flags
1 2048s 209713151s 209711104s test

(parted)
```

Step 9 Enter **q** and press **Enter** to exit parted.

Information similar to the following is displayed:

```
(parted) q
Information: You may need to update /etc/fstab.
```

You can set automatic disk mounting by updating the **/etc/fstab** file. Before updating the file, set the file system format for the partition and mount the partition on the mount point.

Step 10 Run the following command to view the disk partition information:

```
lsblk
```

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda 253:0 0 40G 0 disk
└─vda1 253:1 0 40G 0 part /
```

```
vdb 253:16 0 100G 0 disk
└─vdb1 253:17 0 100G 0 part
```

In the command output, **/dev/vdb1** is the partition you created.

Step 11 Run the following command to set the file system format for the new partition:

```
mkfs -t File system format /dev/vdb1
```

In this example, run the following command to set the **ext4** file system for the new partition:

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

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# mkfs -t ext4 /dev/vdb1
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
6553600 inodes, 26213888 blocks
1310694 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2174746624
800 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

The formatting takes a period of time. Observe the system running status and do not exit.

NOTICE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

Step 12 Run the following command to create a mount point:

```
mkdir Mount point
```

In this example, run the following command to create the **/mnt/sdc** mount point:

```
mkdir /mnt/sdc
```

Step 13 Run the following command to mount the new partition on the created mount point:

```
mount Disk partition Mount point
```

In this example, run the following command to mount the new partition **/dev/vdb1** on **/mnt/sdc**:

```
mount /dev/vdb1 /mnt/sdc
```

Step 14 Run the following command to view the mount result:

```
df -TH
```

Information similar to the following is displayed:

New partition **/dev/vdb1** is mounted on **/mnt/sdc**.

 **NOTE**

If the server is restarted, the mounting will become invalid. You can set automatic mounting for partitions at system start by modifying the **/etc/fstab** file. For details, see [Setting Automatic Mounting at System Start](#).

----End

Setting Automatic Mounting at System Start

To automatically mount disk partitions at system start, do not specify partitions, for example **/dev/vdb1**, in **/etc/fstab** because the sequence of cloud devices, and therefore their names may change during the server stop and start. You are advised to use the universally unique identifier (UUID) in **/etc/fstab** to set automatic mounting at system start.

 **NOTE**

UUID is the unique character string for disk partitions in a Linux system.

Step 1 Run the following command to query the partition UUID:

```
blkid Disk partition
```

In this example, run the following command to query the UUID of the **/dev/vdb1** partition:

```
blkid /dev/vdb1
```

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# blkid /dev/vdb1
/dev/vdb1: UUID="0b3040e2-1367-4abb-841d-ddb0b92693df" TYPE="ext4"
```

The UUID of the **/dev/vdb1** partition is displayed.

Step 2 Run the following command to open the **fstab** file using the vi editor:

```
vi /etc/fstab
```

Step 3 Press **i** to enter the editing mode.

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

```
UUID=0b3040e2-1367-4abb-841d-ddb0b92693df /mnt/sdc          ext4 defaults      0 2
```

The preceding content is used for reference only. Add the information that is used in the environment. The parameters are described as follows:

- The first column indicates the partition UUID obtained in [Step 1](#).
- The second column indicates the directory on which the partition is mounted. You can query the mount point using the **df -TH** command.

- The third column indicates the file system format of the partition. You can query the file system format using the **df -TH** command.
- The fourth column indicates the partition mount option. Normally, this parameter is set to **defaults**.
- The fifth column indicates the Linux dump backup option.
 - **0**: not use Linux dump backup. Normally, dump backup is not used, and you can set this parameter to **0**.
 - **1**: use Linux dump backup.
- The sixth column indicates the fsck option, that is, whether to use fsck to check the attached disk during startup.
 - **0**: not use fsck.
 - If the mount point is the root partition (**/**), this parameter must be set to **1**.
When this parameter is set to **1** for the root partition, this parameter for other partitions must start with **2** so that the system checks the partitions in the ascending order of the values.

Step 5 Press **Esc**, enter **:wq**, and press **Enter**.

The system saves the configurations and exits the vi editor.

Step 6 Perform the following operations to verify the automatic mounting function:

1. Run the following command to unmount the partition:

```
umount Disk partition
```

In this example, run the following command:

```
umount /dev/vdb1
```

2. Run the following command to reload all the content in the **/etc/fstab** file:

```
mount -a
```

3. Run the following command to query the file system mounting information:

```
mount | grep Mount point
```

In this example, run the following command:

```
mount | grep /mnt/sdc
```

If information similar to the following is displayed, the automatic mounting function takes effect:

```
root@ecs-test-0001 ~]# mount | grep /mnt/sdc  
/dev/vdb1 on /mnt/sdc type ext4 (rw,relatime,data=ordered)
```

----End

2.3.6 Initializing a Windows Data Disk Larger Than 2 TB (Windows Server 2008)

Scenarios

This topic uses Windows Server 2008 R2 Standard 64bit to describe how to initialize a data disk whose capacity is larger than 2 TB. In the following operations, the capacity of the example disk is 3 TB.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is larger than 2 TB. For details, see [2.3.6 Initializing a Windows Data Disk Larger Than 2 TB \(Windows Server 2008\)](#). For details about disk partition styles, see [2.3.1 Scenarios and Disk Partitions](#).

The method for initializing a disk varies depending on the OS running on the server. This document is used for reference only. For the detailed operations and differences, see the product documents of the corresponding OS.

Prerequisites

- A data disk has been attached to a server and has not been initialized.
- You have logged in to the server.
 - For how to log in to an ECS, see the *Elastic Cloud Server User Guide*.
 - For how to log in to a BMS, see the *Bare Metal Server User Guide*.

Procedure

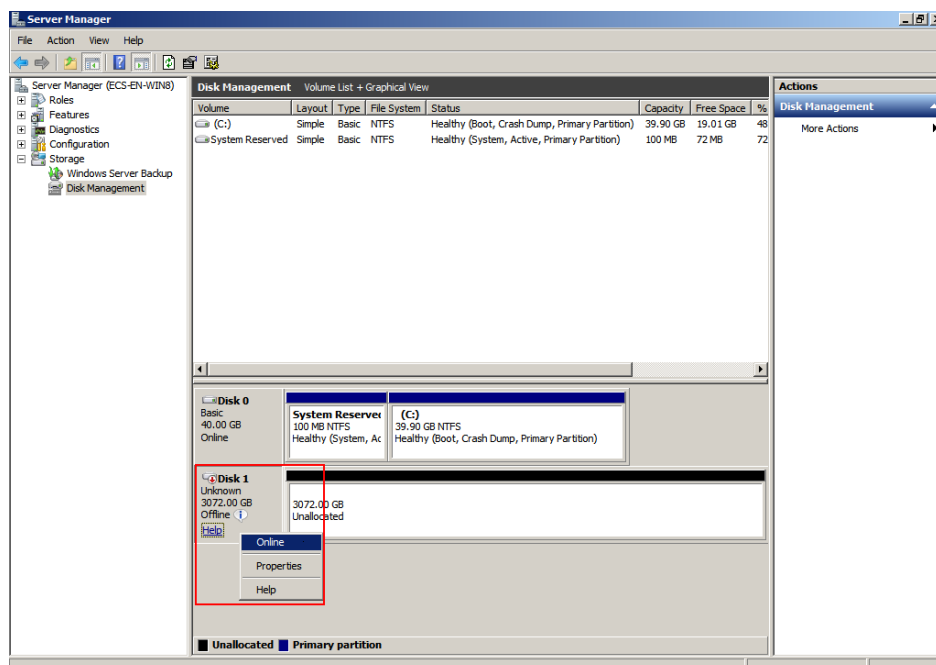
Step 1 On the desktop of the server, click **Start**.

The **Start** window is displayed.

Step 2 Right-click **Computer** and choose **Manage** from the short-cut menu.

The **Server Manager** window is displayed.

Figure 2-25 Server Manager (Windows Server 2008)

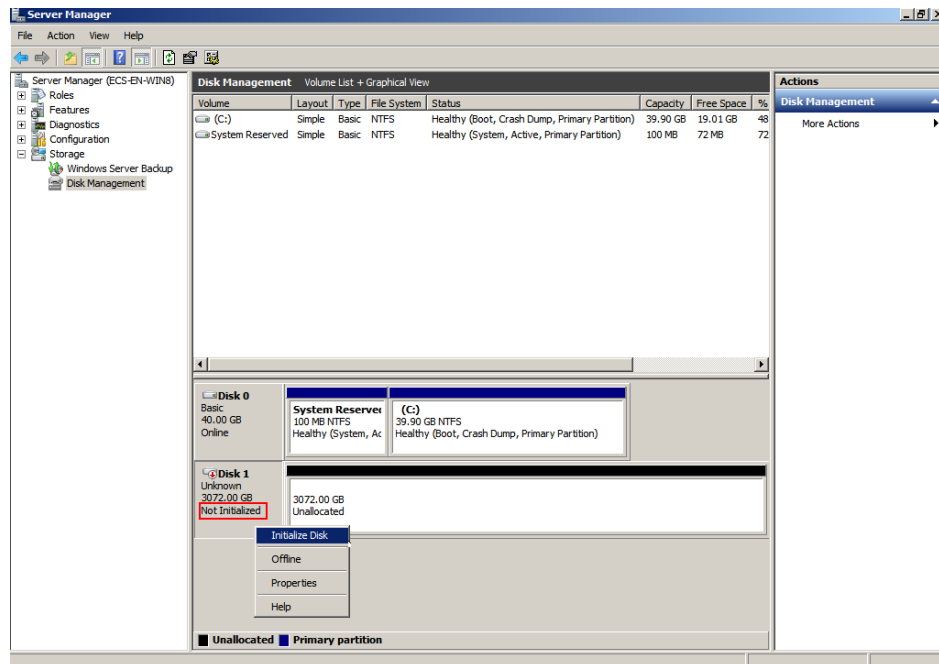


Step 3 Disks are listed in the right pane. If the new disk is in the offline state, bring it online before initialize it.

In the **Disk 1** area, right-click and choose **Online** from the shortcut menu.

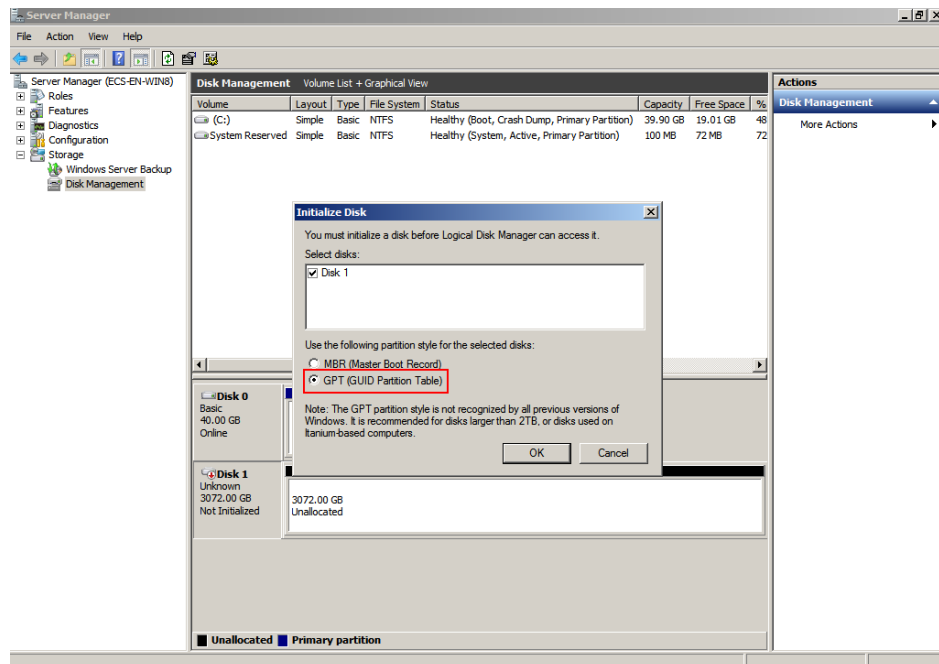
When the Disk 1 status changes from **Offline** to **Not Initialized**, the disk has been brought online.

Figure 2-26 Bring online succeeded (Windows Server 2008)



Step 4 In the **Disk 1** area, right-click and choose **Initialize Disk** from the shortcut menu. The **Initialize Disk** dialog box is displayed.

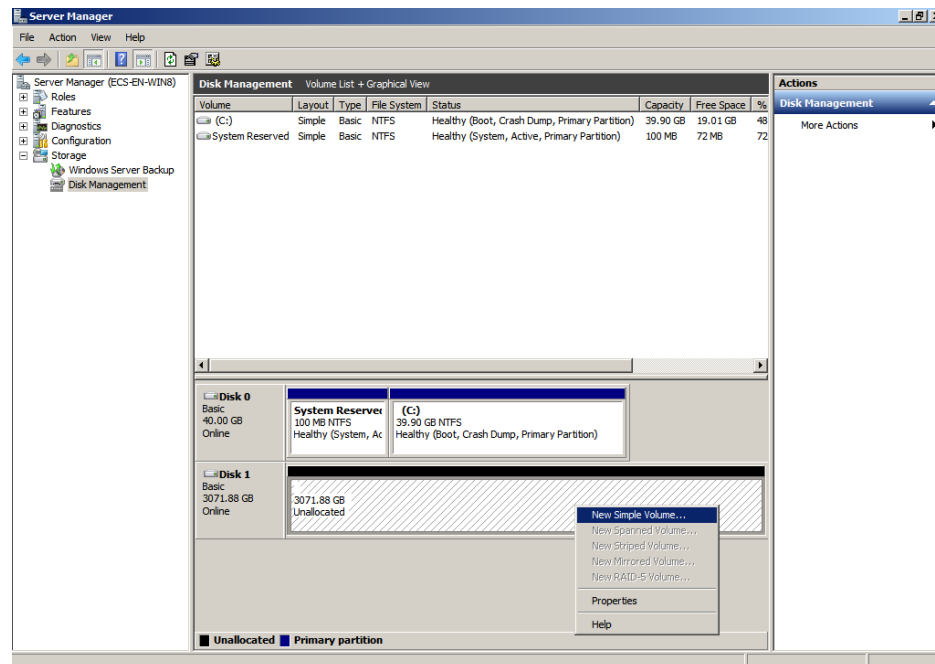
Figure 2-27 Initialize Disk (Windows Server 2008)



Step 5 In the **Initialize Disk** dialog box, the to-be-initialized disk is selected. In this example, the disk capacity is larger than 2 TB. Therefore, select **GPT (GUID Partition Table)** and click **OK**.

The **Server Manager** window is displayed.

Figure 2-28 Server Manager (Windows Server 2008)



NOTICE

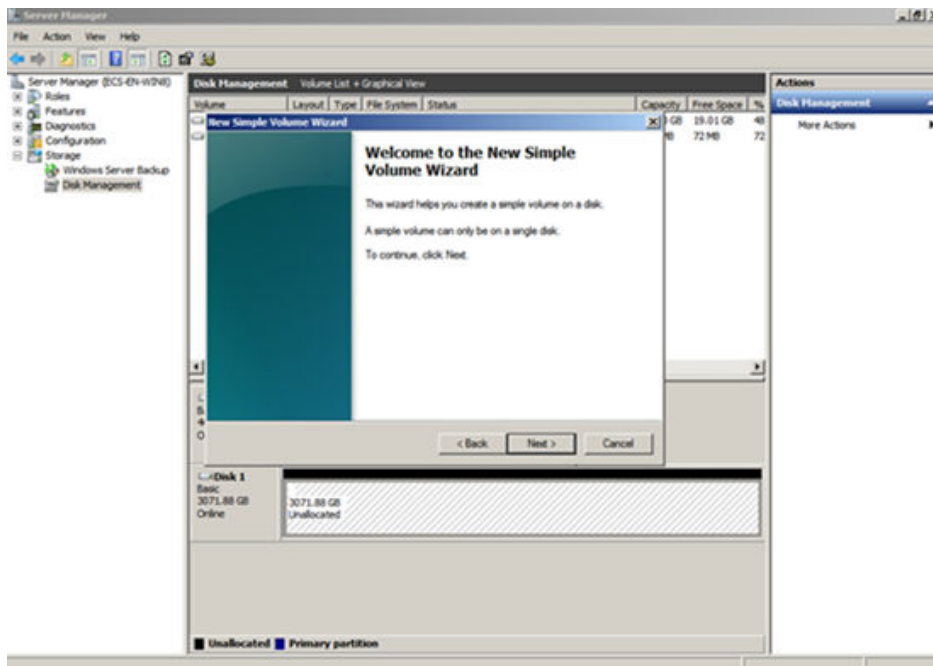
The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Because a data disk currently supports up to 32 TB, use the GPT partition style if your disk capacity is larger than 2 TB.

If you change the disk partition style after the disk has been used, the data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

Step 6 Right-click at the unallocated disk space and choose **New Simple Volume** from the shortcut menu.

The **New Simple Volume Wizard** window is displayed.

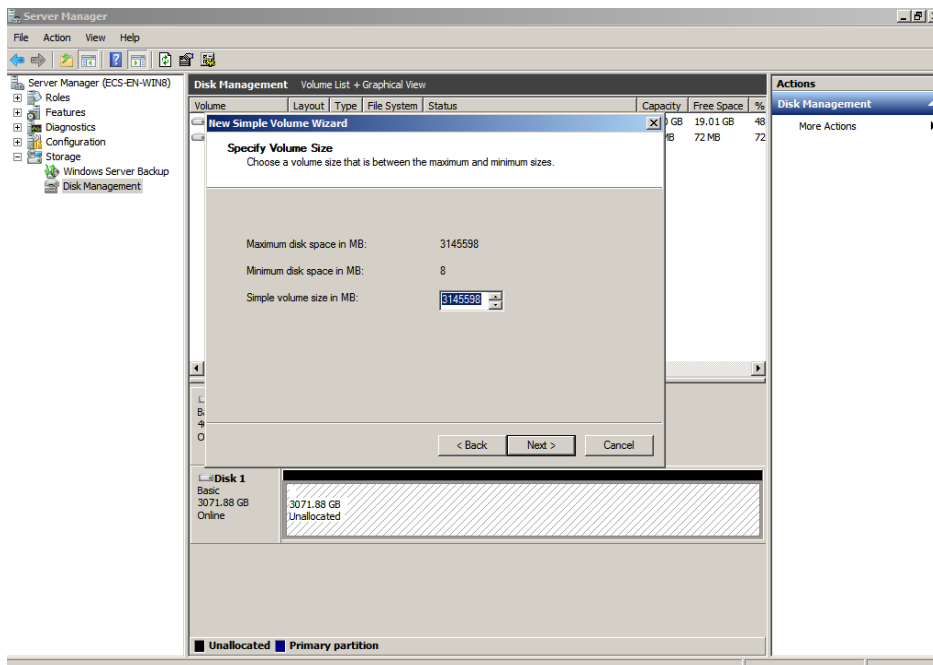
Figure 2-29 New Simple Volume Wizard (Windows Server 2008)



Step 7 Follow the prompts and click **Next**.

The **Specify Volume Size** page is displayed.

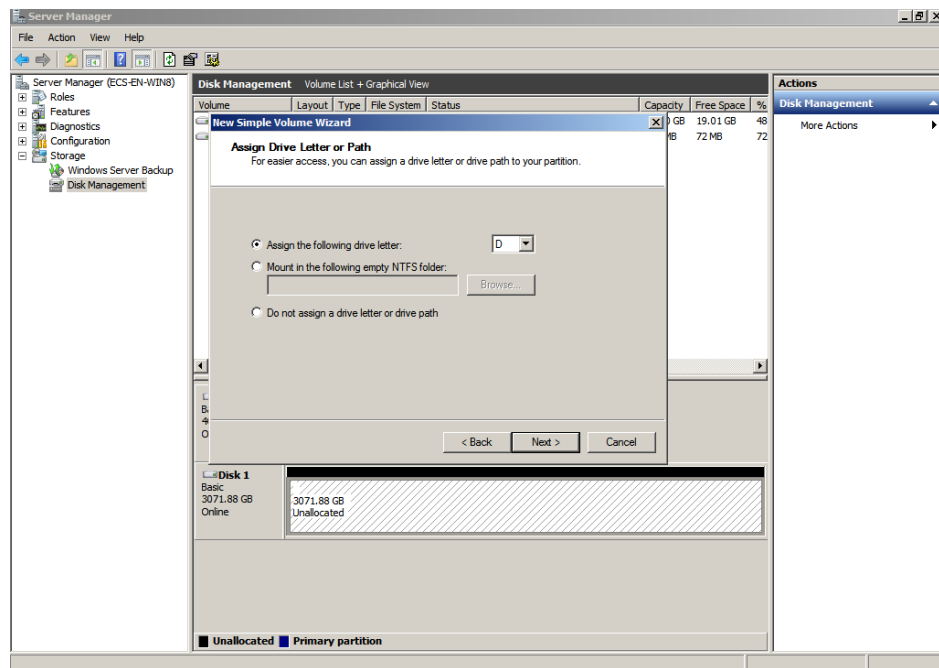
Figure 2-30 Specify Volume Size (Windows Server 2008)



Step 8 Specify the volume size and click **Next**. The system selects the maximum volume size by default. You can specify the volume size as required. In this example, the default setting is used.

The **Assign Drive Letter or Path** page is displayed.

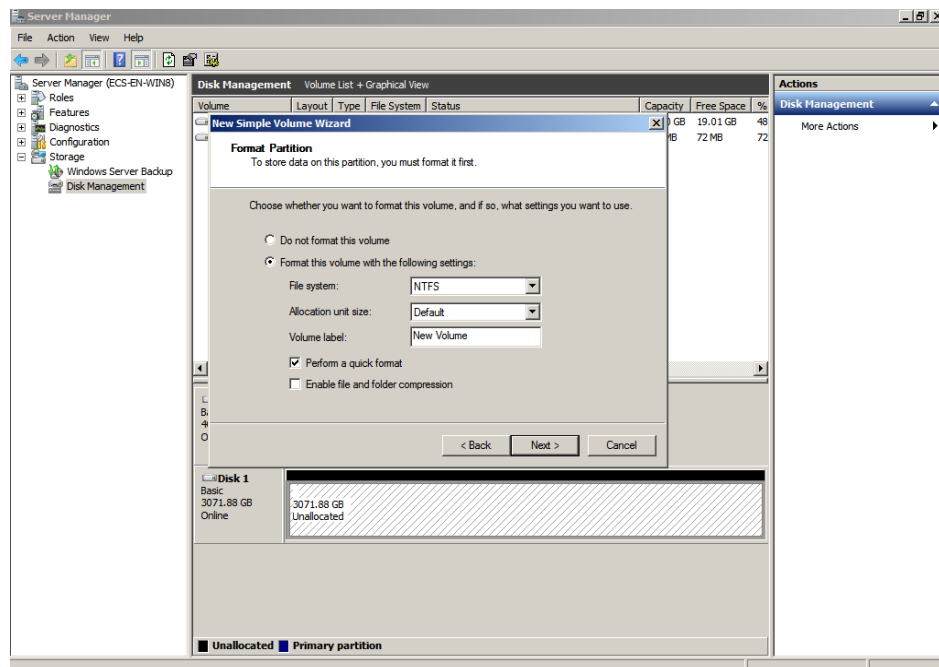
Figure 2-31 Assign Driver Letter or Path (Windows Server 2008)



Step 9 Assign a drive letter or path to your partition and click **Next**. The system assigns drive letter D by default. In this example, the default setting is used.

The **Format Partition** page is displayed.

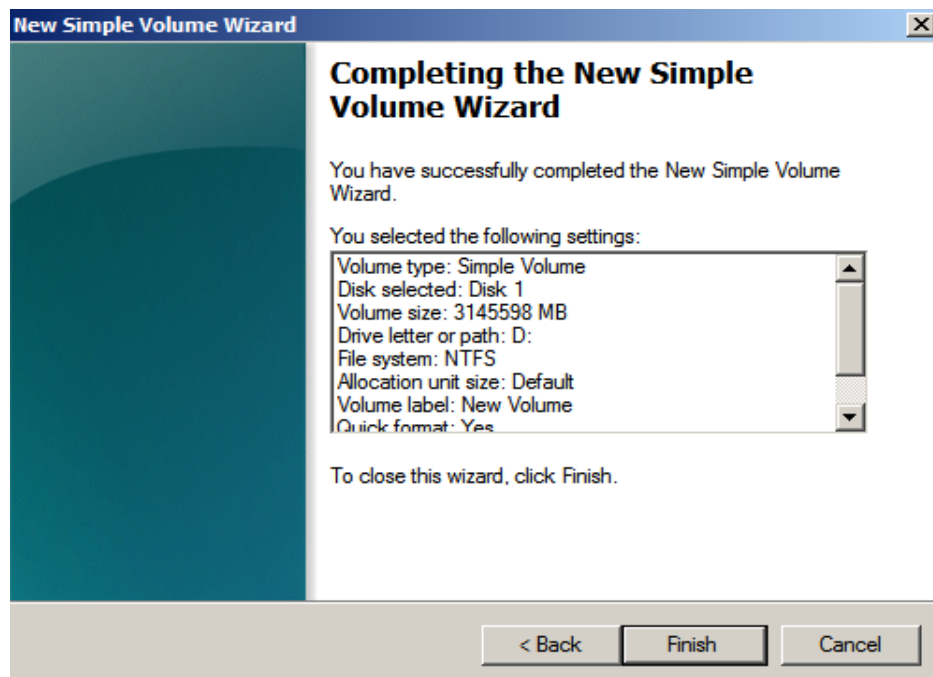
Figure 2-32 Format Partition (Windows Server 2008)



Step 10 Specify format settings and click **Next**. The system selects the NTFS file system by default. You can specify the file system type as required. In this example, the default setting is used.

The **Completing the New Simple Volume Wizard** page is displayed.

Figure 2-33 Completing the New Simple Volume Wizard



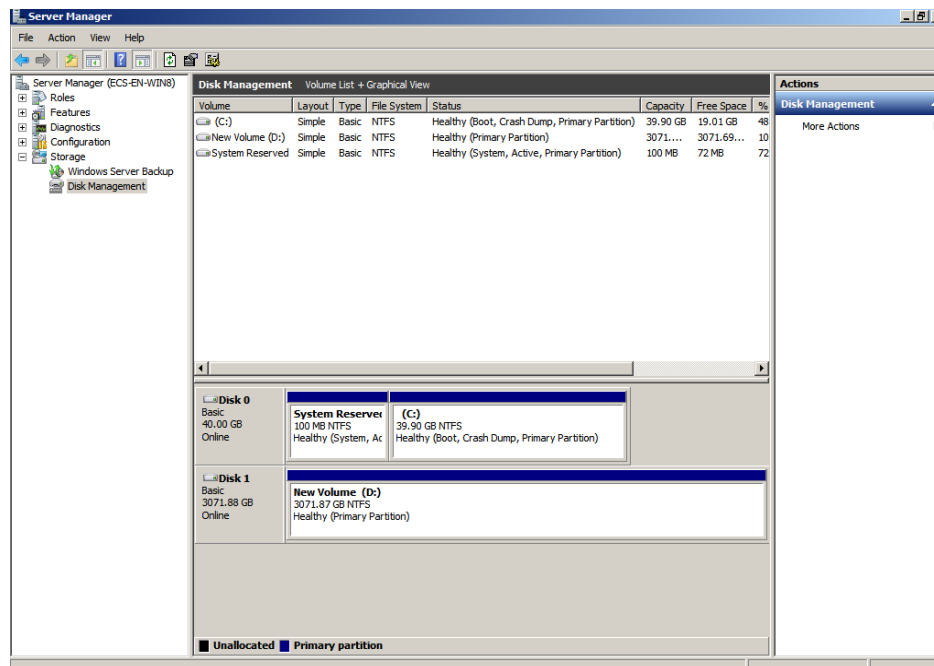
NOTICE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

Step 11 Click **Finish**.

Wait for the initialization to complete. When the volume status changes to **Healthy**, the initialization has finished successfully, as shown in [Figure 2-34](#).

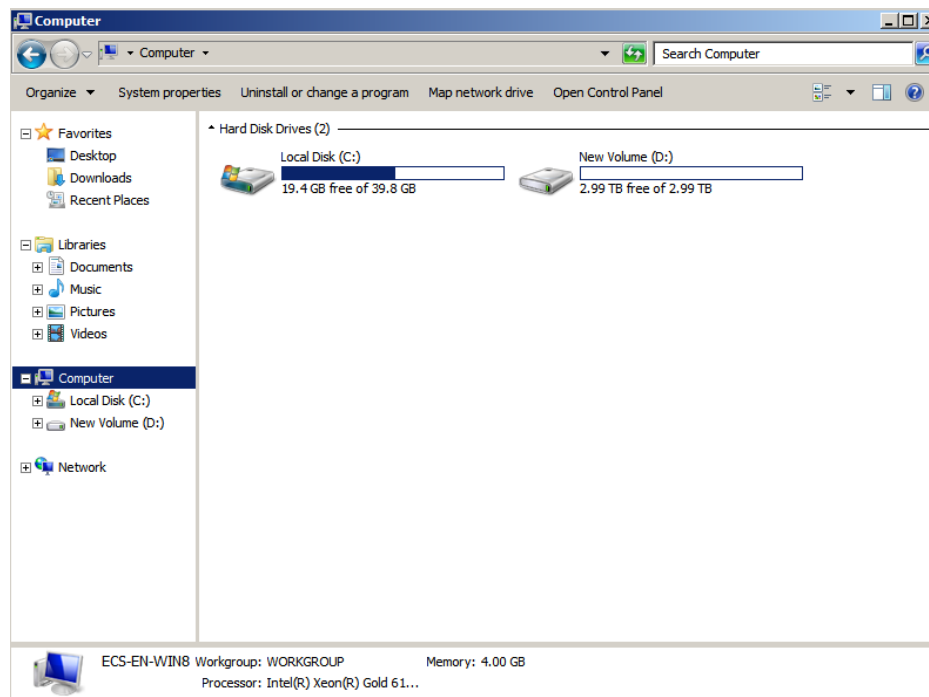
Figure 2-34 Disk initialization succeeded (Windows Server 2008)



Step 12 After the volume is created, click  and check whether a new volume appears in **Computer**. In this example, New Volume (D:) is the new volume.

If New Volume (D:) appears, the disk is successfully initialized and no further action is required.

Figure 2-35 Computer (Windows Server 2008)



----End

2.3.7 Initializing a Windows Data Disk Larger Than 2 TB (Windows Server 2012)

Scenarios

This topic uses Windows Server 2012 R2 Standard 64bit to describe how to initialize a data disk whose capacity is larger than 2 TB. In the following operations, the capacity of the sample disk is 3 TB.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is larger than 2 TB. For details, see [2.3.6 Initializing a Windows Data Disk Larger Than 2 TB \(Windows Server 2008\)](#). For details about disk partition styles, see [2.3.1 Scenarios and Disk Partitions](#).

The method for initializing a disk varies depending on the OS running on the server. This document is used for reference only. For the detailed operations and differences, see the product documents of the corresponding OS.

Prerequisites

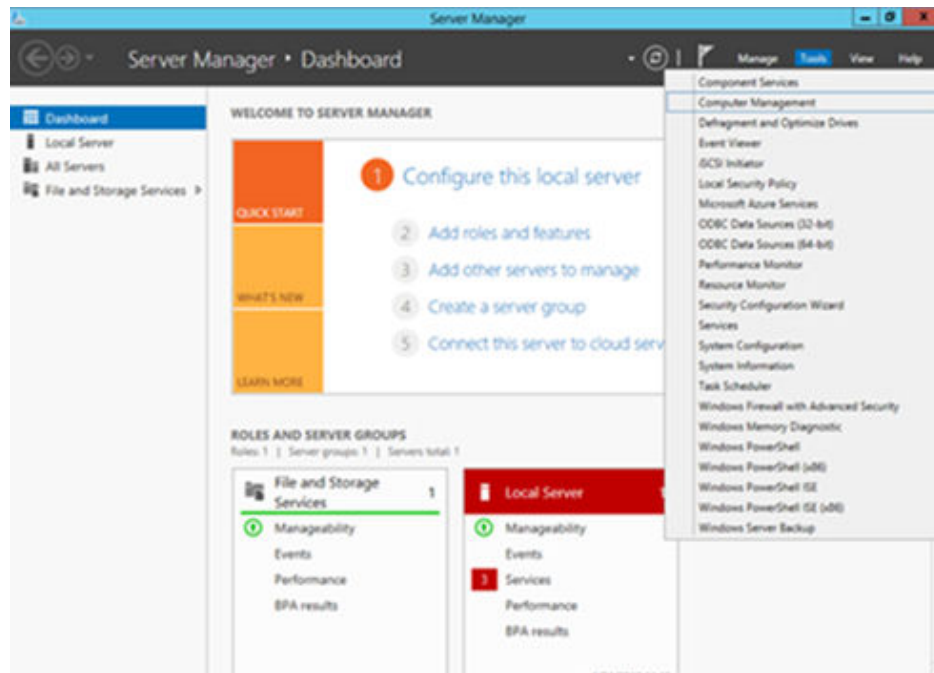
- A data disk has been attached to a server and has not been initialized.
- You have logged in to the server.
 - For how to log in to an ECS, see the *Elastic Cloud Server User Guide*.
 - For how to log in to a BMS, see the *Bare Metal Server User Guide*.

Procedure

Step 1 On the desktop of the server, click  in the lower area.

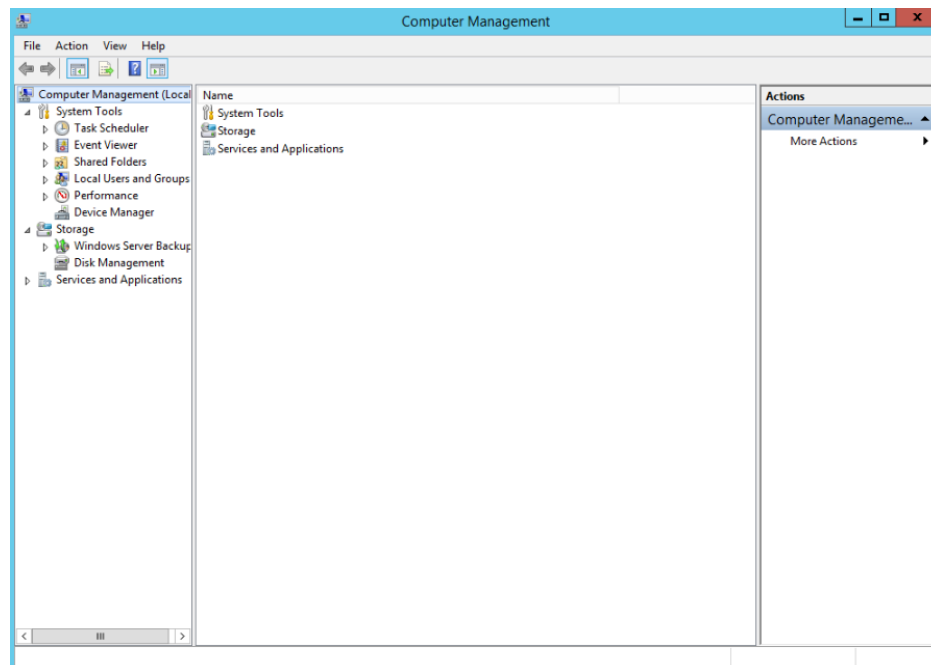
The **Server Manager** window is displayed.

Figure 2-36 Server Manager (Windows Server 2012)



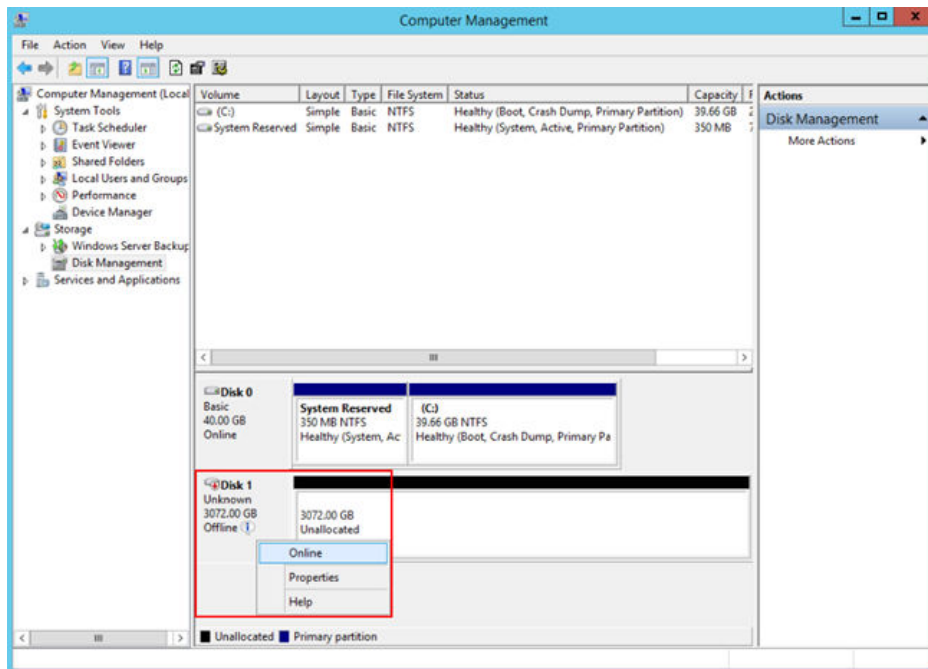
Step 2 In the upper right corner, choose **Tools > Computer Management**.
The **Computer Management** window is displayed.

Figure 2-37 Computer Management



Step 3 Choose **Storage > Disk Management**.
Disks are displayed in the right pane.

Figure 2-38 Disk list

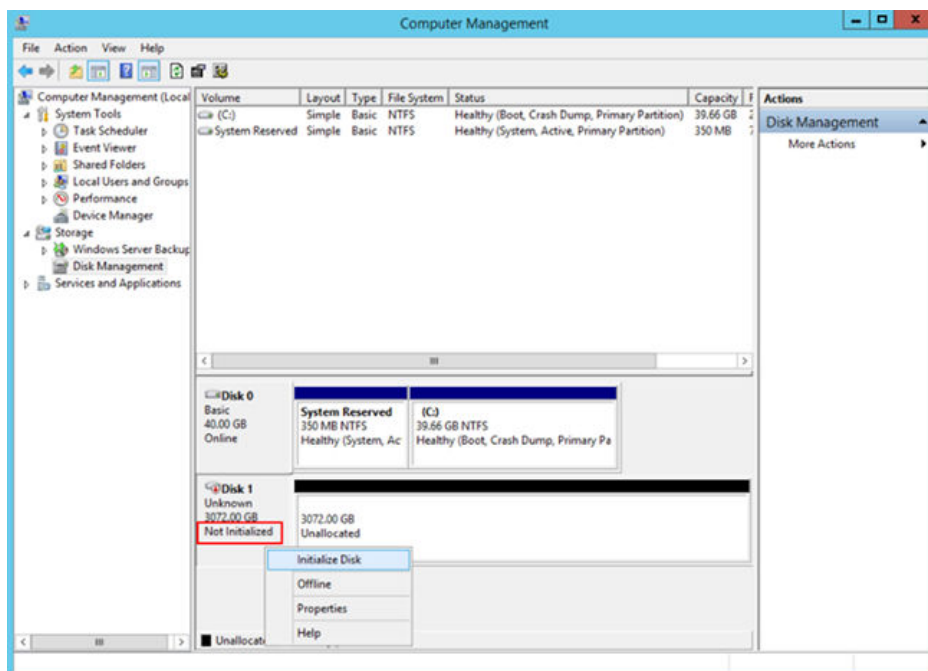


Step 4 (Optional) If the new disk is in the offline state, bring it online before initializing it.

In the **Disk 1** area, right-click and choose **Online** from the shortcut menu.

When the status of Disk 1 changes from **Offline** to **Not Initialized**, the disk has been brought online.

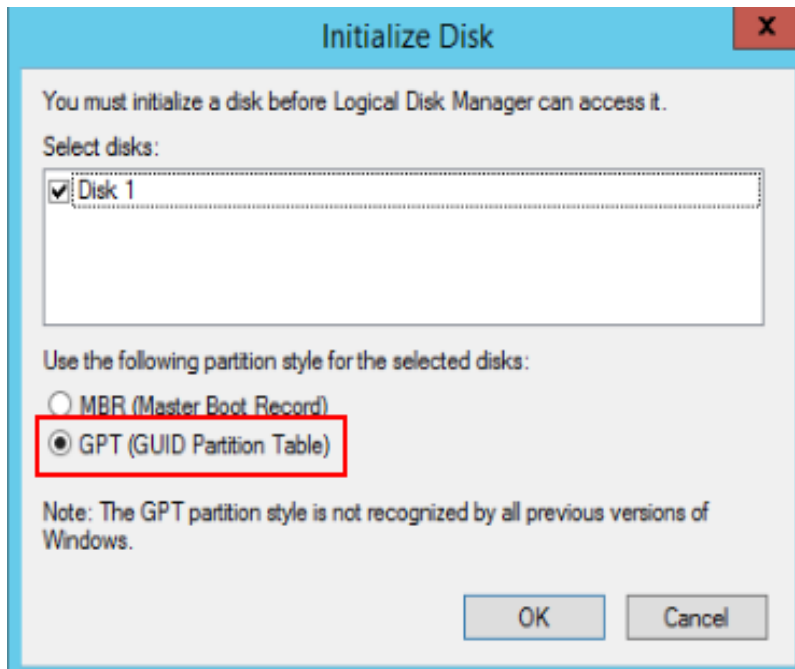
Figure 2-39 Bring online succeeded (Windows Server 2012)



Step 5 In the **Disk 1** area, right-click and choose **Initialize Disk** from the shortcut menu.

The **Initialize Disk** dialog box is displayed.

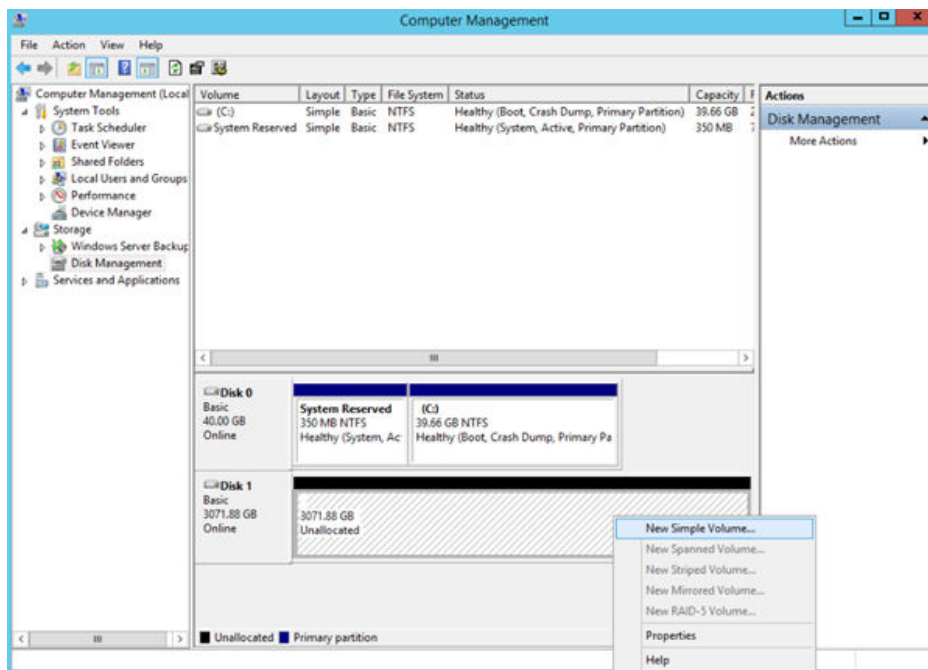
Figure 2-40 Initialize Disk (Windows Server 2012)



Step 6 In the **Initialize Disk** dialog box, the to-be-initialized disk is selected. In this example, the disk capacity is larger than 2 TB. Therefore, select **GPT (GUID Partition Table)** and click **OK**.

The **Computer Management** window is displayed.

Figure 2-41 Computer Management (Windows Server 2012)



NOTICE

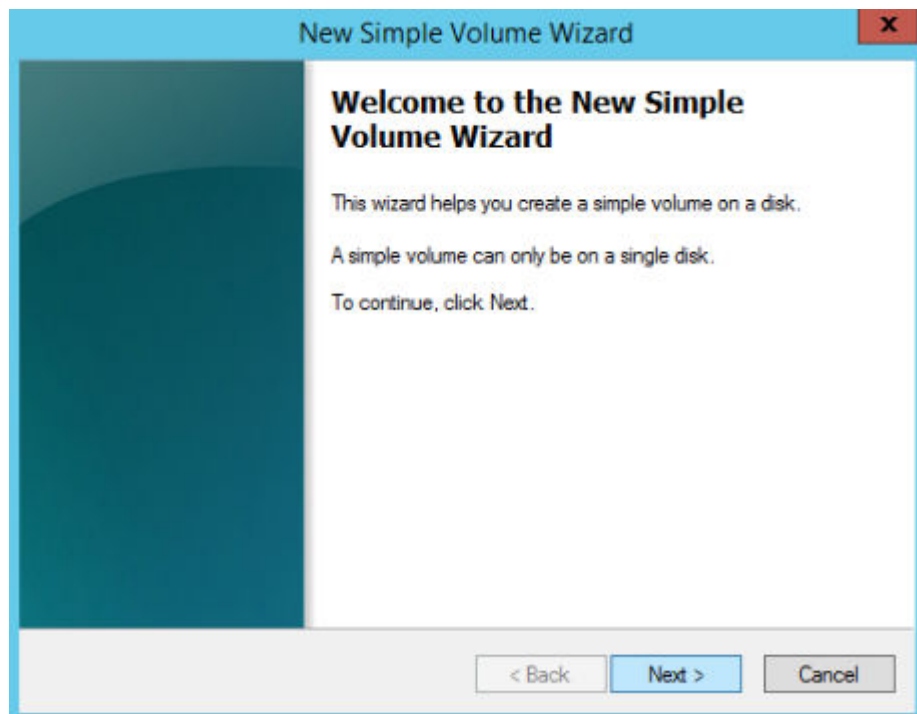
The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Because a data disk currently supports up to 32 TB, use the GPT partition style if your disk capacity is larger than 2 TB.

If you change the disk partition style after the disk has been used, the data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

Step 7 Right-click at the unallocated disk space and choose **New Simple Volume** from the shortcut menu.

The **New Simple Volume Wizard** window is displayed.

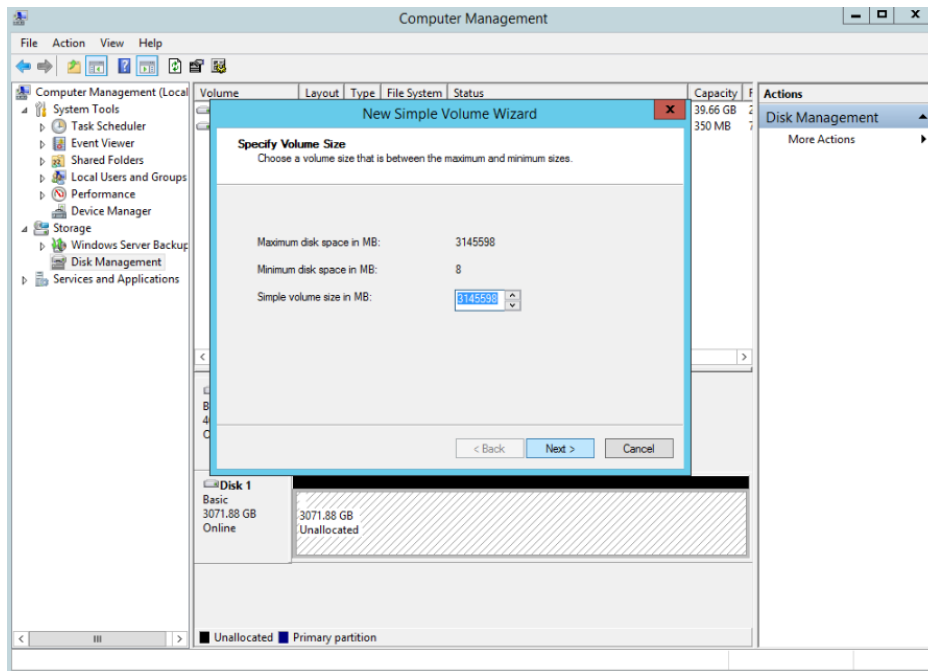
Figure 2-42 New Simple Volume Wizard (Windows Server 2012)



Step 8 Follow the prompts and click **Next**.

The **Specify Volume Size** page is displayed.

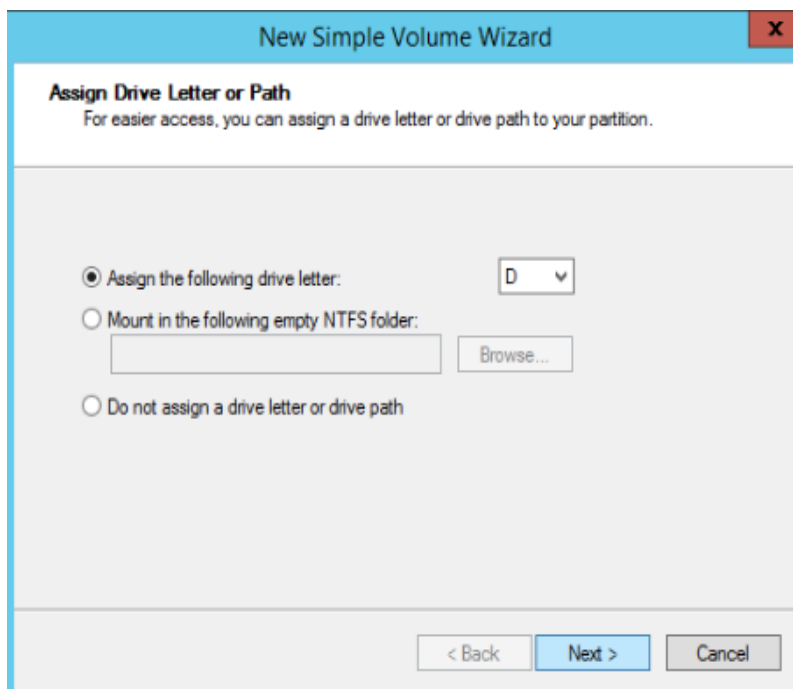
Figure 2-43 Specify Volume Size (Windows Server 2012)



Step 9 Specify the volume size and click **Next**. The system selects the maximum volume size by default. You can specify the volume size as required. In this example, the default setting is used.

The **Assign Drive Letter or Path** page is displayed.

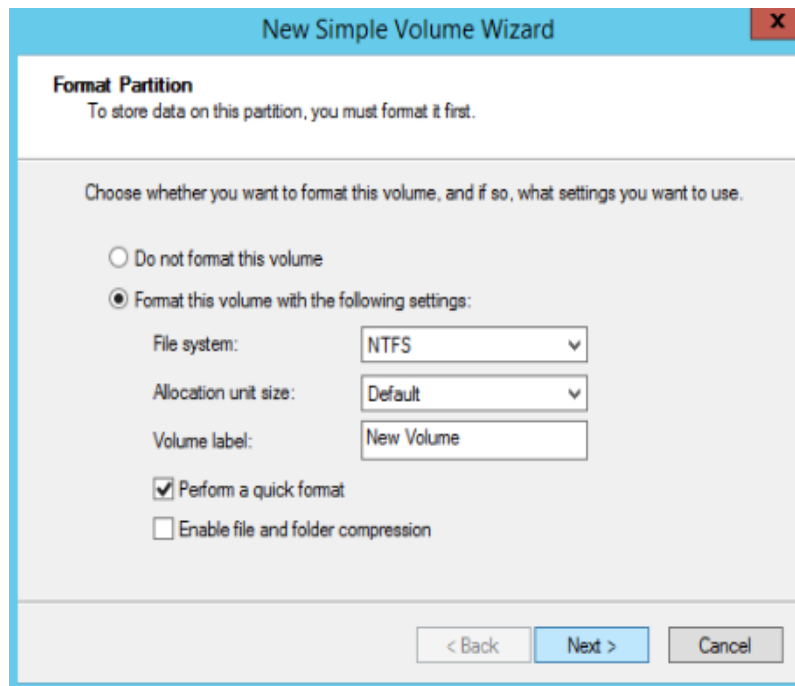
Figure 2-44 Assign Driver Letter or Path (Windows Server 2012)



Step 10 Assign a drive letter or path to your partition and click **Next**. The system assigns drive letter D by default. In this example, the default setting is used.

The **Format Partition** page is displayed.

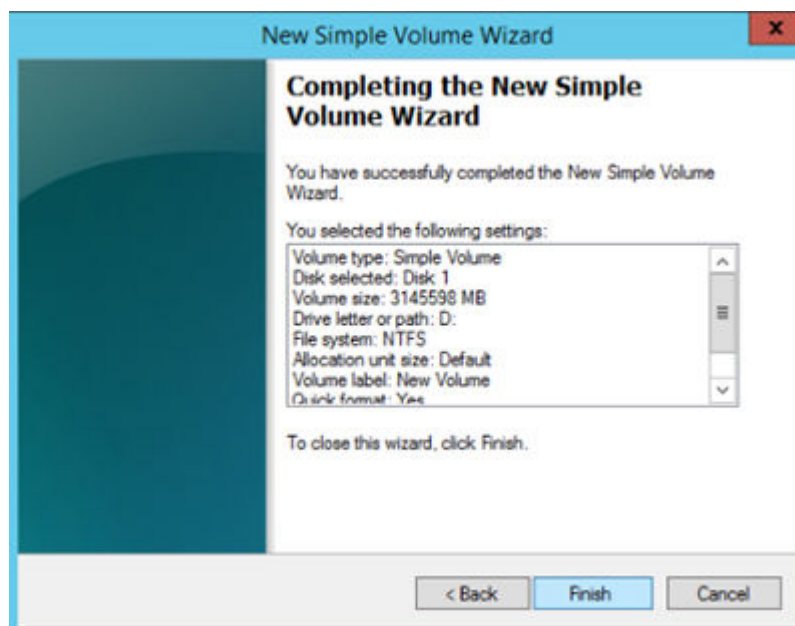
Figure 2-45 Format Partition (Windows Server 2012)



Step 11 Specify format settings and click **Next**. The system selects the NTFS file system by default. You can specify the file system type as required. In this example, the default setting is used.

The **Completing the New Simple Volume Wizard** page is displayed.

Figure 2-46 Completing the New Simple Volume Wizard (Windows Server 2012)



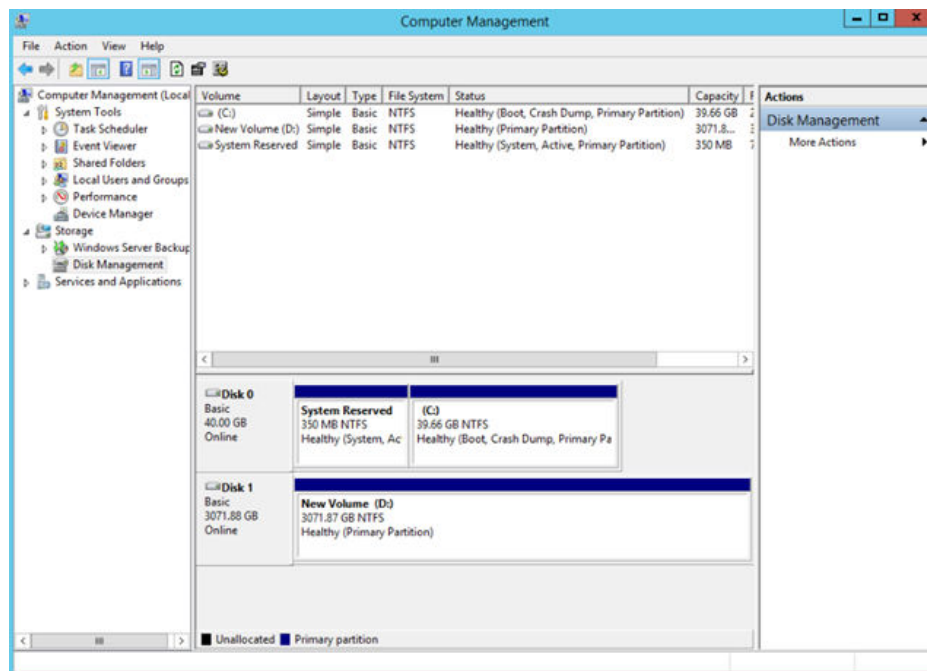
NOTICE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

Step 12 Click **Finish**.

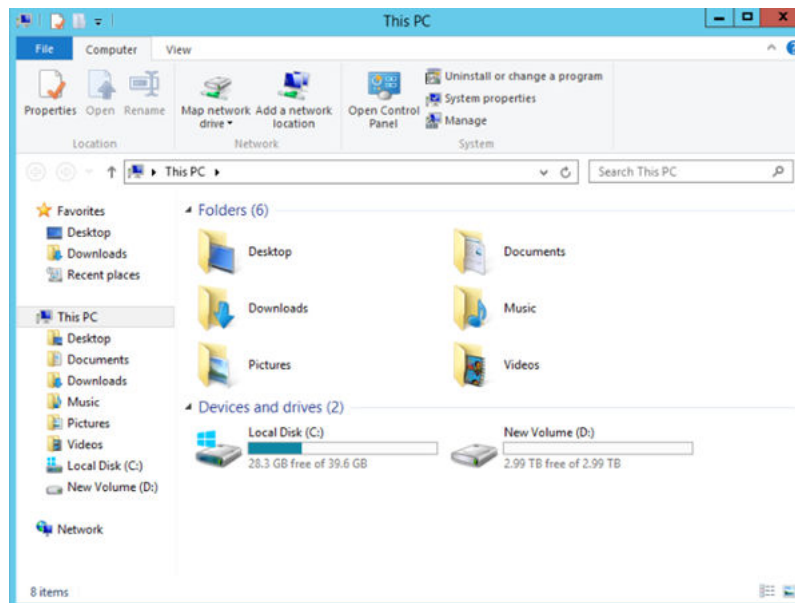
Wait for the initialization to complete. When the volume status changes to **Healthy**, the initialization has finished successfully, as shown in **Figure 2-47**.

Figure 2-47 Disk initialization succeeded (Windows Server 2012)



Step 13 After the volume is created, click  and check whether a new volume appears in **This PC**. In this example, New Volume (D:) is the new volume.

If New Volume (D:) appears, the disk is successfully initialized and no further action is required.

Figure 2-48 This PC (Windows Server 2012)

----End

2.3.8 Initializing a Linux Data Disk Larger Than 2 TB (parted)

Scenarios

This topic uses CentOS 7.4 64bit to describe how to use parted to initialize a data disk whose capacity is larger than 2 TB. In the following operations, the capacity of the sample disk is 3 TB.

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Therefore, use the GPT partition style if your disk capacity is larger than 2 TB. In Linux, if you choose to use the GPT partition style, the fdisk partitioning tool cannot be used. Use the parted partitioning tool instead. For details about disk partition styles, see [2.3.1 Scenarios and Disk Partitions](#).

The method for initializing a disk varies depending on the OS running on the server. This document is used for reference only. For the detailed operations and differences, see the product documents of the corresponding OS.

Prerequisites

- A data disk has been attached to a server and has not been initialized.
- You have logged in to the server.
 - For how to log in to an ECS, see the *Elastic Cloud Server User Guide*.
 - For how to log in to a BMS, see the *Bare Metal Server User Guide*.

Creating and Mounting a Partition

The following example shows you how a new partition can be created on a new data disk that has been attached to a server. The partition will be created using parted, and GPT is used as the partition style. Furthermore, the partition will be

formatted using the ext4 file system, mounted on **/mnt/sdc**, and configured automatic mounting at system start.

Step 1 Run the following command to query information about the new data disk:

lsblk

Information similar to the following is displayed:

```
[root@ecs-centos74 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda  253:0  0 40G 0 disk
├─vda1 253:1  0  1G 0 part /boot
├─vda2 253:2  0 39G 0 part /
└─vdb  253:16 0  3T 0 disk
```

In the command output, the server contains two disks. **/dev/vda** is the system disk, and **/dev/vdb** is the new data disk.

Step 2 Run the following command to enter parted to partition the new data disk:

parted *New data disk*

In this example, run the following command:

parted /dev/vdb

Information similar to the following is displayed:

```
[root@ecs-centos74 ~]# parted /dev/vdb
GNU Parted 3.1
Using /dev/vdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted)
```

Step 3 Enter **p** and press **Enter** to view the current disk partition style.

Information similar to the following is displayed:

```
(parted) p
Error: /dev/vdb: unrecognised disk label
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 3299GB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:
(parted)
```

In the command output, the **Partition Table** value is **unknown**, indicating that no partition style is set for the new disk.

Step 4 Run the following command to set the disk partition style:

mklabel *Disk partition style*

In this example, run the following command to set the disk partition style to GPT: (Disk partition styles can be MBR or GPT.)

mklabel gpt

NOTICE

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Because a data disk currently supports up to 32 TB, use the GPT partition style if your disk capacity is larger than 2 TB.

If you change the disk partition style after the disk has been used, the data on the disk will be cleared. Therefore, select a proper disk partition style when initializing the disk.

Step 5 Enter **p** and press **Enter** to view the disk partition style.

Information similar to the following is displayed:

```
(parted) mklabel gpt
(parted) p
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 3299GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start  End  Size  File system  Name  Flags
(parted)
```

Step 6 Enter **unit s** and press **Enter** to set the measurement unit of the disk to sector.

Step 7 Run the following command and press **Enter**:

```
mkpart Partition name Start sector End sector
```

In this example, run the following command:

```
mkpart opt 2048s 100%
```

In this example, one partition is created for the new data disk. Value **2048s** indicates the disk start sector, and **100%** indicates the disk end sector. The two values are used for reference only. You can determine the number of partitions and the partition size based on your service requirements.

Information similar to the following is displayed:

```
(parted) mkpart opt 2048s 100%
Warning: The resulting partition is not properly aligned for best performance.
Ignore/Cancel? Ignore
```

If the preceding warning message is displayed, enter **Ignore** to ignore the performance warning.

Step 8 Enter **p** and press **Enter** to view details about the new partition.

Information similar to the following is displayed:

```
(parted) p
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 6442450944s
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start  End  Size  File system  Name  Flags
1       2048s  6442448895s  6442446848s  opt
```

Details about the **dev/vdb1** partition are displayed.

Step 9 Enter **q** and press **Enter** to exit parted.

Step 10 Run the following command to view the disk partition information:

lsblk

Information similar to the following is displayed:

```
[root@ecs-centos74 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda 253:0 0 40G 0 disk
├─vda1 253:1 0 1G 0 part /boot
├─vda2 253:2 0 39G 0 part /
vdb 253:16 0 3T 0 disk
├─vdb1 253:17 0 3T 0 part
```

In the command output, **/dev/vdb1** is the partition you created.

Step 11 Run the following command to set the file system format for the new partition:

mkfs -t *File system format* /dev/vdb1

In this example, run the following command to set the **ext4** file system for the new partition:

mkfs -t ext4 /dev/vdb1

Information similar to the following is displayed:

```
[root@ecs-centos74 ~]# mkfs -t ext4 /dev/vdb1
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
201326592 inodes, 805305856 blocks
40265292 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2952790016
24576 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872, 71663616, 78675968,
    102400000, 214990848, 512000000, 550731776, 644972544

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

The formatting takes a period of time. Observe the system running status and do not exit.

NOTICE

The partition sizes supported by file systems vary. Therefore, you are advised to choose an appropriate file system based on your service requirements.

Step 12 Run the following command to create a mount point:

mkdir *Mount point*

In this example, run the following command to create the **/mnt/sdc** mount point:

```
mkdir /mnt/sdc
```

Step 13 Run the following command to mount the new partition on the created mount point:

```
mount Disk partition Mount point
```

In this example, run the following command to mount the new partition **/dev/vdb1** on **/mnt/sdc**:

```
mount /dev/vdb1 /mnt/sdc
```

Step 14 Run the following command to view the mount result:

```
df -TH
```

Information similar to the following is displayed:

```
[root@ecs-centos74 ~]# df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/vda2       ext4      42G   1.5G   38G   4% /
devtmpfs        devtmpfs  2.0G   0   2.0G   0% /dev
tmpfs           tmpfs     2.0G   0   2.0G   0% /dev/shm
tmpfs           tmpfs     2.0G   8.9M   2.0G   1% /run
tmpfs           tmpfs     2.0G   0   2.0G   0% /sys/fs/cgroup
/dev/vda1       ext4      1.1G  153M  801M  17% /boot
tmpfs           tmpfs     398M   0   398M   0% /run/user/0
/dev/vdb1       ext4      3.3T   93M   3.1T   1% /mnt/sdc
```

New partition **dev/vdb1** is mounted on **/mnt/sdc**.

----End

Setting Automatic Mounting at System Start

To automatically mount disk partitions at system start, do not specify partitions, for example **/dev/vdb1**, in **/etc/fstab** because the sequence of cloud devices, and therefore their names may change during the server stop and start. You are advised to use the universally unique identifier (UUID) in **/etc/fstab** to set automatic mounting at system start.

NOTE

UUID is the unique character string for disk partitions in a Linux system.

Step 1 Run the following command to query the partition UUID:

```
blkid Disk partition
```

In this example, run the following command to query the UUID of the **/dev/vdb1** partition:

```
blkid /dev/vdb1
```

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# blkid /dev/vdb1
/dev/vdb1: UUID="0b3040e2-1367-4abb-841d-ddb0b92693df" TYPE="ext4"
```

The UUID of the **/dev/vdb1** partition is displayed.

Step 2 Run the following command to open the **fstab** file using the vi editor:

```
vi /etc/fstab
```

Step 3 Press **i** to enter the editing mode.

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

```
UUID=0b3040e2-1367-4abb-841d-ddb0b92693df /mnt/sdc          ext4  defaults  0 2
```

The preceding content is used for reference only. Add the information that is used in the environment. The parameters are described as follows:

- The first column indicates the partition UUID obtained in [Step 1](#).
- The second column indicates the directory on which the partition is mounted. You can query the mount point using the **df -TH** command.
- The third column indicates the file system format of the partition. You can query the file system format using the **df -TH** command.
- The fourth column indicates the partition mount option. Normally, this parameter is set to **defaults**.
- The fifth column indicates the Linux dump backup option.
 - **0**: not use Linux dump backup. Normally, dump backup is not used, and you can set this parameter to **0**.
 - **1**: use Linux dump backup.
- The sixth column indicates the fsck option, that is, whether to use fsck to check the attached disk during startup.
 - **0**: not use fsck.
 - If the mount point is the root partition (**/**), this parameter must be set to **1**.

When this parameter is set to **1** for the root partition, this parameter for other partitions must start with **2** so that the system checks the partitions in the ascending order of the values.

Step 5 Press **Esc**, enter **:wq**, and press **Enter**.

The system saves the configurations and exits the vi editor.

Step 6 Perform the following operations to verify the automatic mounting function:

1. Run the following command to unmount the partition:

```
umount Disk partition
```

In this example, run the following command:

```
umount /dev/vdb1
```

2. Run the following command to reload all the content in the **/etc/fstab** file:

```
mount -a
```

3. Run the following command to query the file system mounting information:

```
mount | grep Mount point
```

In this example, run the following command:

```
mount | grep /mnt/sdc
```

If information similar to the following is displayed, the automatic mounting function takes effect:

```
root@ecs-test-0001 ~]# mount | grep /mnt/sdc  
/dev/vdb1 on /mnt/sdc type ext4 (rw,relatime,data=ordered)
```

----End

3 Instances

3.1 Creating an ECS

3.1.1 Creating the Same ECS


Scenarios

If you have created an ECS and want to create new ones with the same configuration, you are advised to use "Create Same ECS" provided on the public cloud platform to rapidly create the new ECSs.

Notes

Large-memory ECSs and the ECSs created using full-ECS images do not support "Create Same ECS".

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. Select the target ECS, click **More** in the **Operation** column, and select **Create Same ECS**.

The system switches to the **Create ECS** page and automatically copies the parameter settings of the selected ECS.

 **NOTE**

For security purposes, you must manually configure the new ECSs in the following scenarios:

- Add the remaining quantity of data disks if the quantity of desired data disks exceeds 10.
 - Add the remaining quantity of NICs if the quantity of desired NICs exceeds 5.
 - Add the remaining quantity of security groups if the quantity of desired security groups exceeds 5.
 - Select a new data disk image if the disks of the source ECS are created using a data disk image.
 - Select **Encryption** if the disks of the source ECS have been encrypted.
 - Configure the functions in **Advanced Settings**.
 - Configure **EIP** if required because it is not required by default.
5. Adjust the parameter settings of the new ECSs as required, confirm the configuration, and click **Create Now**.


3.2 Viewing ECS Information

3.2.1 Viewing ECS Creation Statuses

Scenarios

After submitting the request for creating an ECS, you can view the creation status. This section describes how to view the creation status of an ECS.

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. After creating an ECS, view the creation status in the task status area on the right side of common operations, such as **Start**, **Stop**, and **More**.
5. Click the number displayed above **Creating** and view details about the tasks.

 **NOTE**

- An ECS that is being created is in one of the following states:
 - **Creating**: The ECS is being created.
 - **Failures**: Creating the ECS failed. In such a case, the system automatically rolls the task back and displays an error code on the GUI, for example, **Ecs.0013 Insufficient EIP quota**.
 - **Running**: The request of creating the ECS has been processed, and the ECS is running properly. An ECS in this state can provide services for you.
- If you find that the task status area shows an ECS creation failure but the ECS list displays the created ECS, see [13.2.1 Why Does the Failures Area Show an ECS Creation Failure But the ECS List Displays the Created ECS?](#)

3.2.2 Viewing Failures

Scenarios

The **Failures** area shows the tasks that failed to process due to an error, including the task name and status. **Failures** is displayed on the management console if a task failed. This section describes how to view failures.


Failure Types

Table 3-1 lists the types of failures that can be recorded in the **Failures** area.

Table 3-1 Failure types

Failure Type	Description
Creation failures	A task failed to process. For a failed task, the system rolls back and displays an error code, for example, Ecs.0013 Insufficient EIP quota .
Operation failures	<ul style="list-style-type: none">Modifying ECS specifications If an ECS specifications modification failed, this operation is recorded in Failures.

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. View **Failures** on the right side of common operations.
5. Click the number displayed in the **Failures** area to view details about the tasks.
 - **Creation Failures**: show the tasks that are being created and those failed to create.
 - **Operation Failures**: show the tasks with errors, including the operations performed on the tasks and error codes. Such information can be used for rapid fault locating.



3.2.3 Viewing Details About an ECS

Scenarios

After obtaining ECSs, you can view and manage them on the management console. This section describes how to view detailed ECS configurations, including its name, image, system disk, data disks, VPC, NIC, security group, and EIP.

To view the private IP address of an ECS, view it on the **Elastic Cloud Server** page.

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**.
The **Elastic Cloud Server** page is displayed. On this page, you can view your ECSs and the basic information about the ECSs, such as their private IP addresses.
4. In the search box above the ECS list, enter the ECS name, IP address, or ID, and click  for search.
5. Click the name of the target ECS.
The page providing details about the ECS is displayed.
6. View the ECS details.
You can modify ECS configurations, for example, change its security group, add a NIC to it, or bind an EIP to it, by clicking corresponding links or buttons.

3.2.4 Exporting ECS Information


Scenarios

The information of all ECSs under your account can be exported in CSV format to a local directory. The file records the IDs, private IP addresses, and EIPs of your ECSs.

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. In the upper right corner of the ECS list, click .
The system will automatically export all ECSs in the current region under your account to a local directory.

NOTE

- To export certain ECSs, select the target ECSs and click  in the upper right corner of the page.
5. In the lower left corner of your local computer desktop, obtain the exported file **servers.csv**.

3.3 Logging In to a Windows ECS

3.3.1 Login Overview

Constraints

- Only a running ECS can be logged in.
- The username for logging in to a Windows ECS is **Administrator**.
- If an ECS uses key pair authentication, use the password obtaining function available on the management console to decrypt the private key used during ECS creation to obtain a password.
- If you log in to a GPU-accelerated ECS using MSTSC, GPU acceleration will fail. This is because MSTSC replaces the WDDM GPU driver with a non-accelerated remote desktop display driver. In such a case, you must use other methods to log in to the ECS, such as VNC. If the remote login function available on the management console fails to meet your service requirements, you must install a suitable remote login tool on the ECS, such as TightVNC. To download TightVNC, log in at <https://www.tightvnc.com/download.php>.

Login Modes

Select a login mode as required and log in to the target ECS.

Table 3-2 Windows login modes

ECS OS	Local OS	Connection Method	Requirement
Windows	Windows	Use MSTSC. Click Start on the local computer. In the Search programs and files text box, enter mstsc to open the Remote Desktop Connection dialog box. For details, see 3.3.3 Login Using MSTSC .	The target ECS has had an EIP bound.
	Linux	Install a remote connection tool, for example, rdesktop. For details, see 3.3.4 Logging In to a Windows ECS from a Linux Computer .	
	Mac	Install a remote connection tool, for example, Microsoft Remote Desktop for Mac. For details, see 3.3.6 Logging In to Windows ECS from a Mac .	

ECS OS	Local OS	Connection Method	Requirement
	Mobile terminal	Install a remote connection tool, for example, Microsoft Remote Desktop. For details, see 3.3.5 Logging In to a Windows ECS from a Mobile Terminal .	
	Windows	Through the management console. For details, see 3.3.2 Login Using VNC .	No EIP is required.

3.3.2 Login Using VNC

Scenarios

This section describes how to use VNC provided on the management console to log in to an ECS.

Prerequisites

If an ECS uses key pair authentication, make sure that the key file has been used to resolve the login password before logging in to the ECS. For details, see [6.4 Obtaining the Password for Logging In to a Windows ECS](#).

Logging In to a Windows ECS


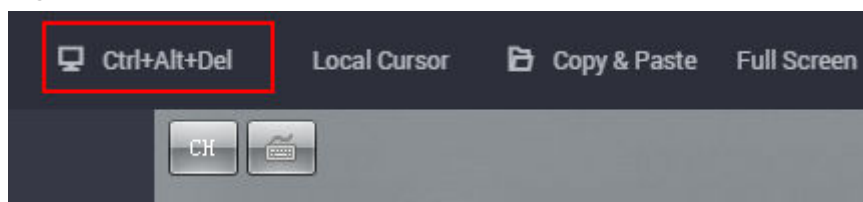
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Elastic Cloud Server**.
4. Obtain the password for logging in to the ECS.
Before logging in to the ECS, you must have the login password.
 - If your ECS uses password authentication, log in to the ECS using the password configured when you created this ECS.
 - If your ECS uses key pair authentication, obtain the password by following the instructions provided in [6.4 Obtaining the Password for Logging In to a Windows ECS](#).
5. In the **Operation** column of the target ECS, click **Remote Login**.
6. (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 3-1 Ctrl+Alt+Del



7. Enter the ECS password as prompted.

3.3.3 Login Using MSTSC

Scenarios

This section describes how to use the remote login tool MSTSC to log in to a Windows ECS from a local computer.

Prerequisites

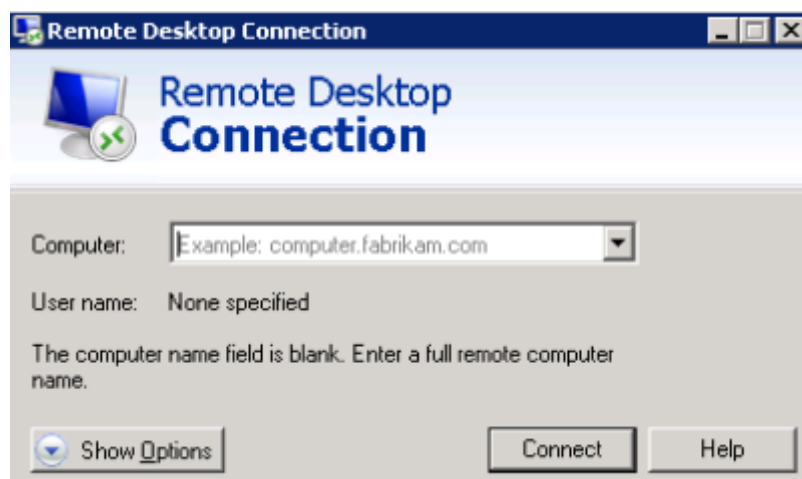
- The target ECS is running.
- If your ECS uses key pair authentication, you have obtained the password for logging in to the Windows ECS. For details, see [6.4 Obtaining the Password for Logging In to a Windows ECS](#).
- You have bound an EIP to the ECS. For details, see [9.1 Binding an EIP](#).
- Access to port 3389 is allowed in the inbound direction of the security group to which the ECS belongs. For details, see [8.1.4 Configuring Security Group Rules](#).
- The network connection between the login tool and the target ECS is normal. For example, the default port 3389 is not blocked by the firewall.
- RDP has been enabled on the target ECS. By default, RDP has been enabled on the ECSs created using a public image. For instructions about how to enable RDP, see [Enabling RDP](#).

Logging In to a Windows ECS Using MSTSC

If your local server runs Windows, you can use the remote desktop connection tool MSTSC delivered with the Windows OS to log in to a Windows ECS.

1. Click the start menu on the local server.
2. In the **Search programs and files** text box, enter **mstsc**.
3. In the **Remote Desktop Connection** dialog box, click **Show Options**.

Figure 3-2 Show Options

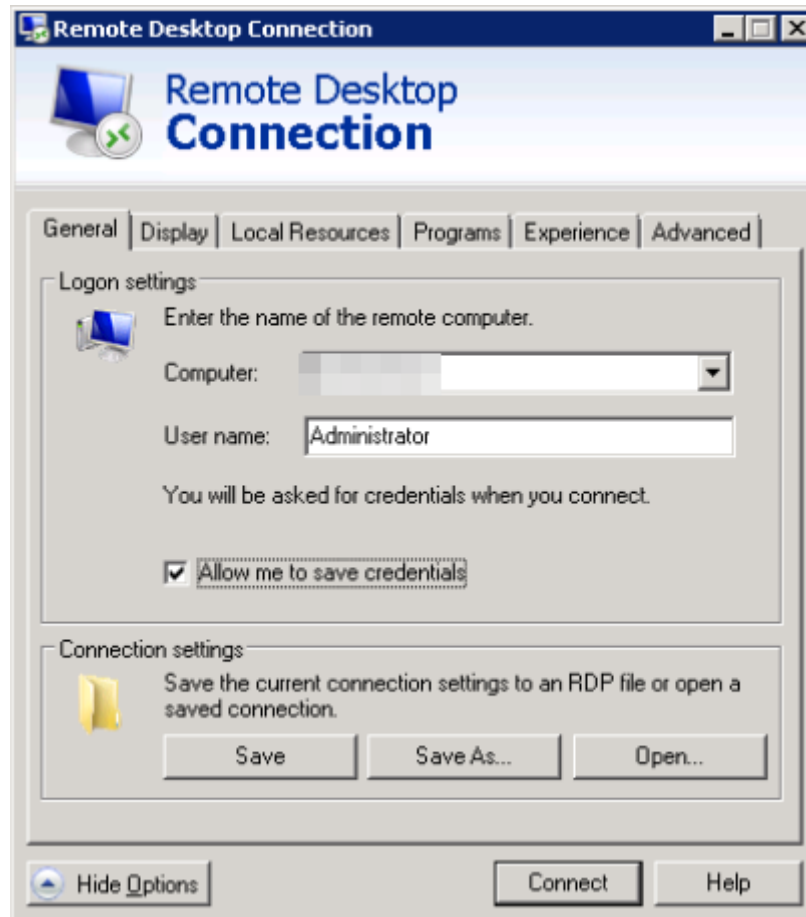


4. Enter the EIP and username (**Administrator** by default) of the target ECS.

 **NOTE**

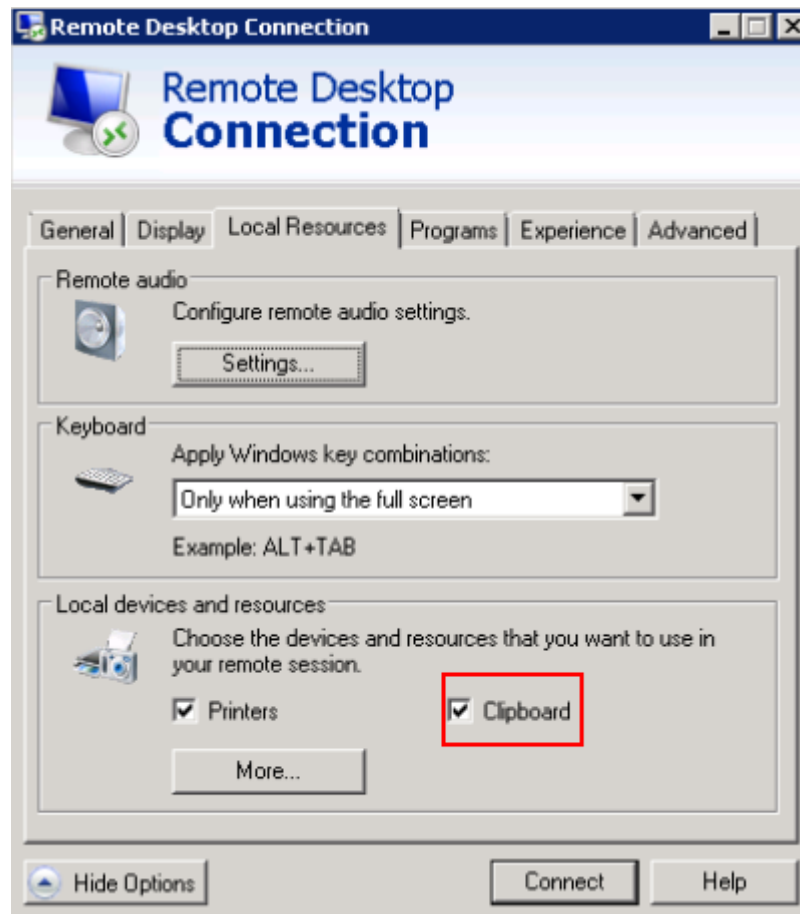
If you do not want to enter the username and password in follow-up logins, select **Allow me to save credentials**.

Figure 3-3 Remote Desktop Connection



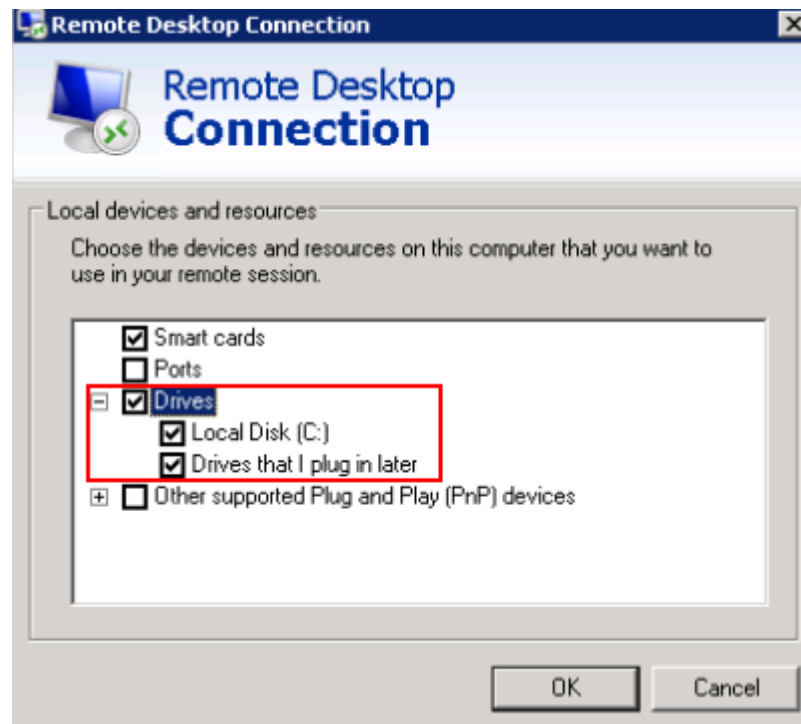
5. (Optional) To use local server resources in a remote session, configure parameters on the **Local Resources** tab.
 - To copy data from the local server to your ECS, select **Clipboard**.

Figure 3-4 Clipboard



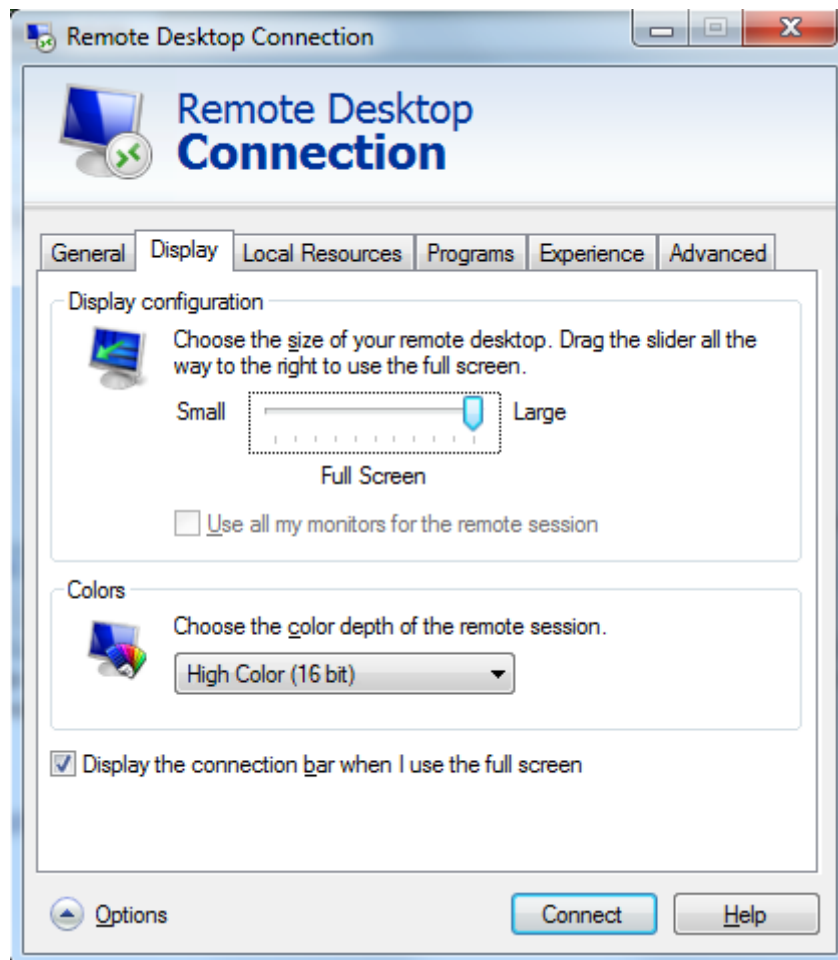
- To copy files from the local server to your ECS, click **More** and select **Drives** and your desired disks.

Figure 3-5 Drives



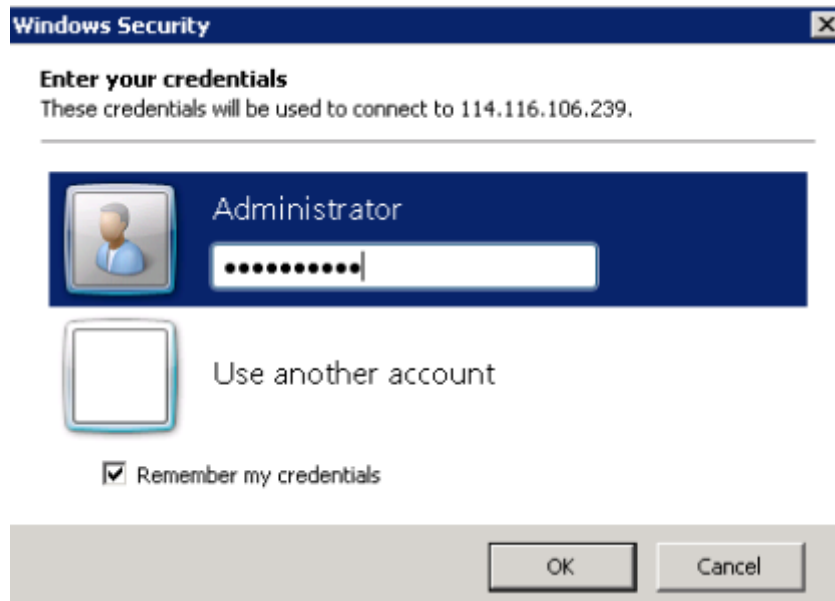
6. (Optional) Click the **Display** tab and then adjust the size of the remote desktop.

Figure 3-6 Adjusting the size of the desktop



7. Click **OK** and enter the login password as prompted to log in to the ECS. To ensure system security, change the login password after you log in to the ECS for the first time.

Figure 3-7 Entering the login password



8. (Optional) After logging in to the ECS using RDP, handle the issue that local files larger than 2 GB cannot be copied to a remote Windows ECS. For details, see [troubleshooting cases](#).

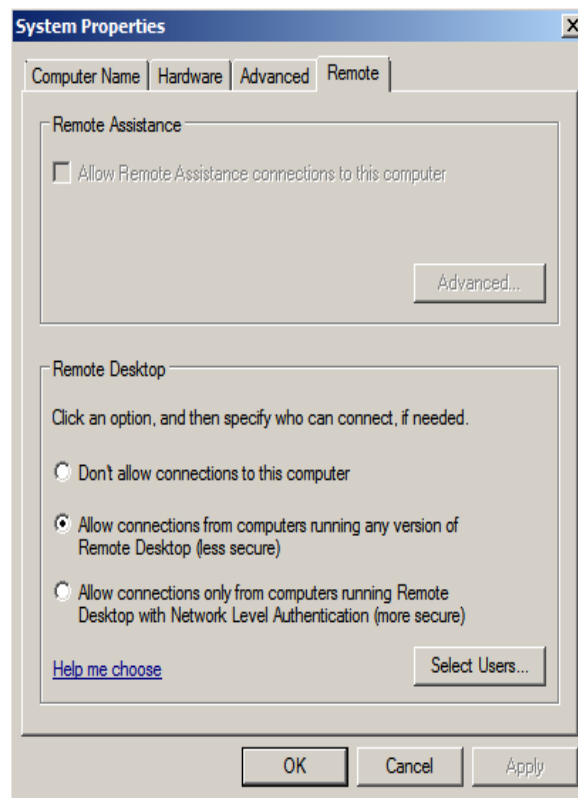
Enabling RDP

When you log in to an ECS for the first time, log in to it using VNC, enable RDP, and access the ECS using MSTSC.

NOTE

By default, RDP has been enabled on the ECSs created using a public image.

1. Log in to the Windows ECS using VNC. For details, see [3.3.2 Login Using VNC](#).
2. Click **Start** in the task bar and choose **Control Panel > System and Security > System > Remote settings**. The **System Properties** dialog box is displayed.

Figure 3-8 System Properties

3. Click the **Remote** tab and select **Allow connections from computers running any version of Remote Desktop (less secure)**.
4. Click **OK**.

3.3.4 Logging In to a Windows ECS from a Linux Computer

Scenarios

This section describes how to log in to a Windows ECS from a Linux computer.

Prerequisites

- The target ECS is running.
- You have bound an EIP to the ECS.
- Access to port 3389 is allowed in the inbound direction of the security group to which the ECS belongs.
- Data can be exchanged between the login tool and the target ECS. For example, the default port 3389 is not blocked by the firewall.
- RDP has been enabled on the target ECS. By default, RDP has been enabled on the ECSs created using a public image. For instructions about how to enable RDP, see [Enabling RDP](#).

Procedure

To log in to a Windows ECS from a local Linux computer, use a remote access tool, such as rdesktop.

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

rdesktop

If the message "command not found" is displayed, rdesktop is not installed. In such a case, obtain the rdesktop installation package at the [official rdesktop website](#).

2. Run the following command to log in to the ECS:

```
rdesktop -u Username -p Password -g Resolution EIP
```

For example, run **rdesktop -u administrator -p password -g 1024*720 192.168.x.x**.

Table 3-3 Parameters in the remote login command

Parameter	Description
-u	Username, which defaults to Administrator for Windows ECSs
-p	Password for logging in to the Windows ECS
-f	Full screen by default, which can be switched using Ctrl+Alt+Enter
-g	Resolution, which uses an asterisk (*) to separate numbers. This parameter is optional. If it is not specified, the remote desktop is displayed in full screen by default, for example, 1024*720 .
EIP	EIP of the Windows ECS to be remotely logged in. Replace it with the EIP bound to your Windows ECS.

Enabling RDP

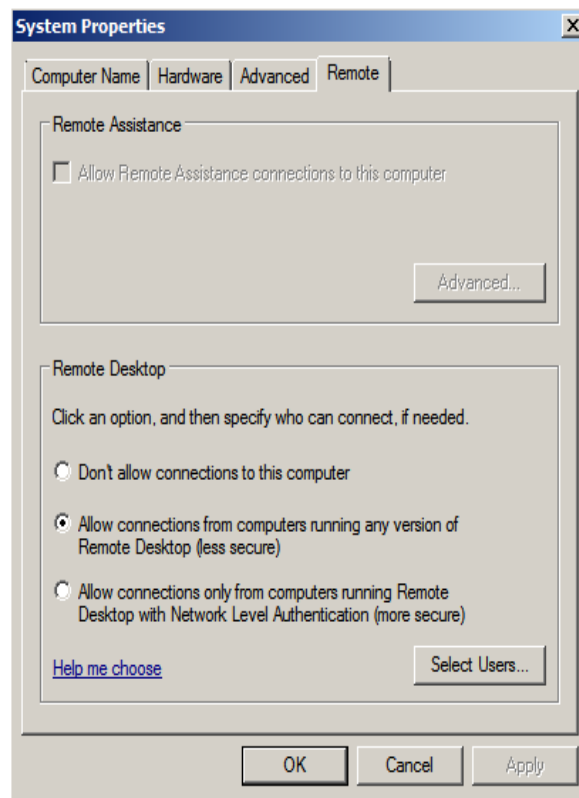
When you log in to an ECS for the first time, log in to it using VNC, enable RDP, and access the ECS using MSTSC.

 **NOTE**

By default, RDP has been enabled on the ECSs created using a public image.

1. Log in to the Windows ECS using VNC.
For details, see [3.3.2 Login Using VNC](#).
2. Click **Start** in the task bar and choose **Control Panel > System and Security > System > Remote settings**.

The **System Properties** dialog box is displayed.

Figure 3-9 System Properties

3. Click the **Remote** tab and select **Allow connections from computers running any version of Remote Desktop (less secure)**.
4. Click **OK**.

3.3.5 Logging In to a Windows ECS from a Mobile Terminal

Scenarios

This section describes how to log in to an ECS running Windows Server 2012 R2 DataCenter 64bit from the Microsoft Remote Desktop client.

Prerequisites

- The target ECS is running.
- You have obtained the username and password for logging in to the ECS.
- You have bound an EIP to the ECS. For details, see [9.1 Binding an EIP](#).
- Access to port 3389 is allowed in the inbound direction of the security group to which the ECS belongs. For details, see [8.1.4 Configuring Security Group Rules](#).
- Microsoft Remote Desktop has been installed on the mobile terminal.

Procedure


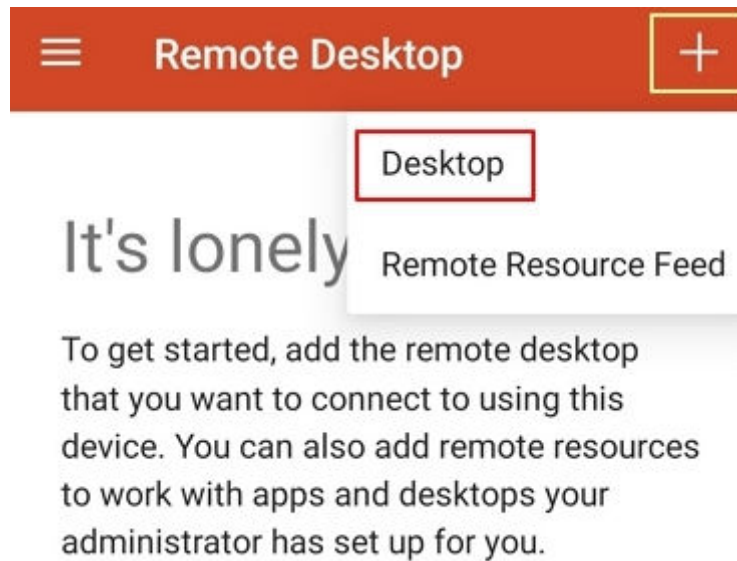
1. Start the Microsoft Remote Desktop client.
2. In the upper right corner of the **Remote Desktop** page, tap  and select **Desktop**.

Figure 3-10 Remote Desktop



3. On the **Add desktop** page, set login information and tap **SAVE**.
 - **PC name:** Enter the EIP bound to the target Windows ECS.
 - Perform the following operations to set **User name:**
 - i. Tap **User name** and select **Add user account** from the drop-down list.
The **Add user account** dialog box is displayed.
 - ii. Enter username **administrator** and password for logging in to the Windows ECS and tap **SAVE**.

Figure 3-11 Setting the login information

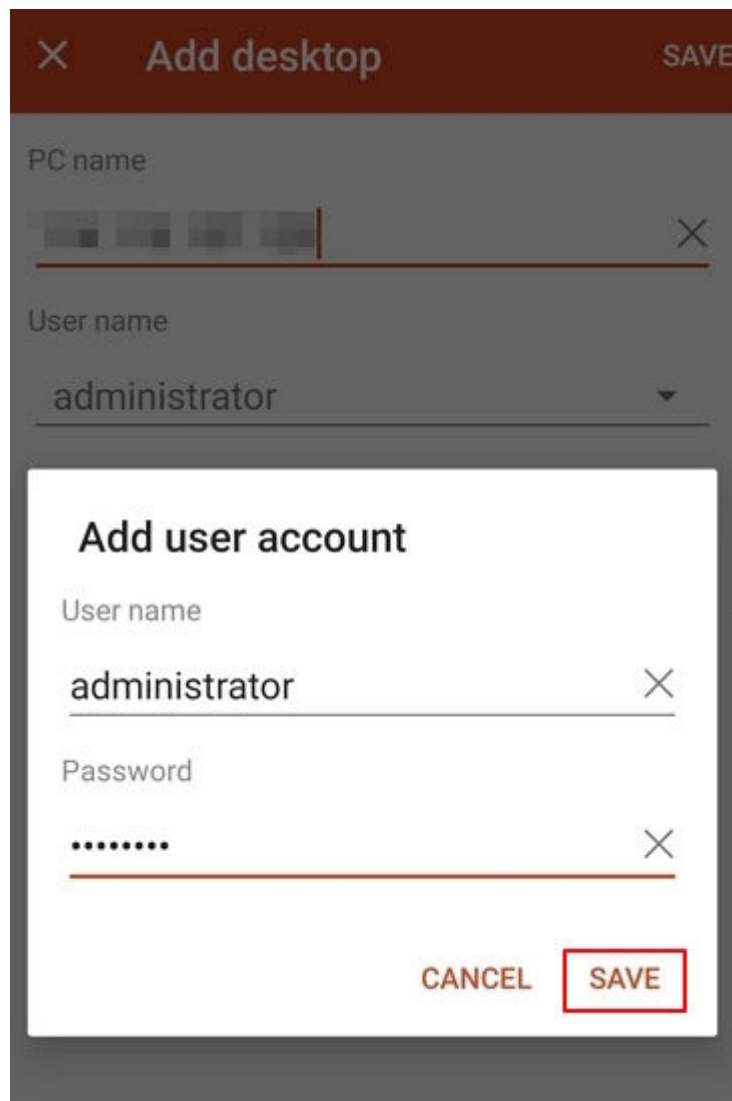
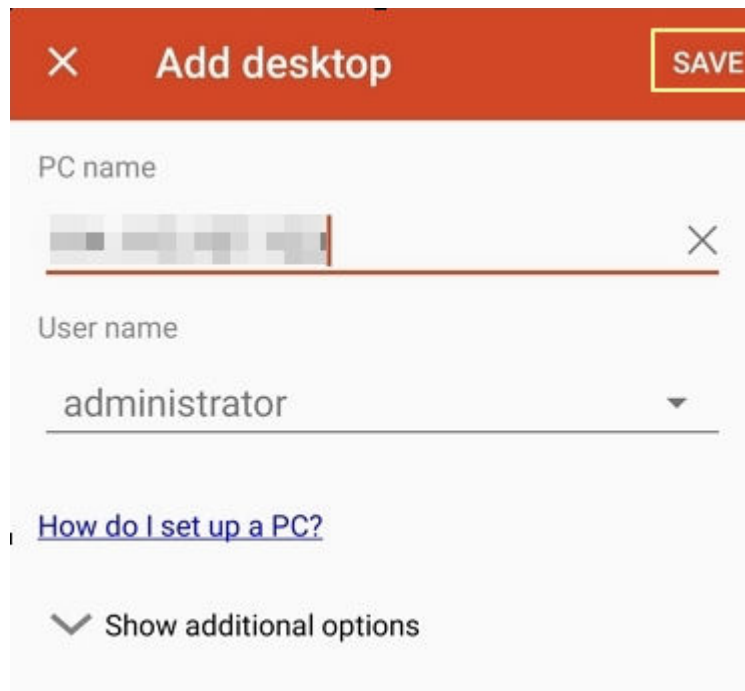


Figure 3-12 Saving the settings



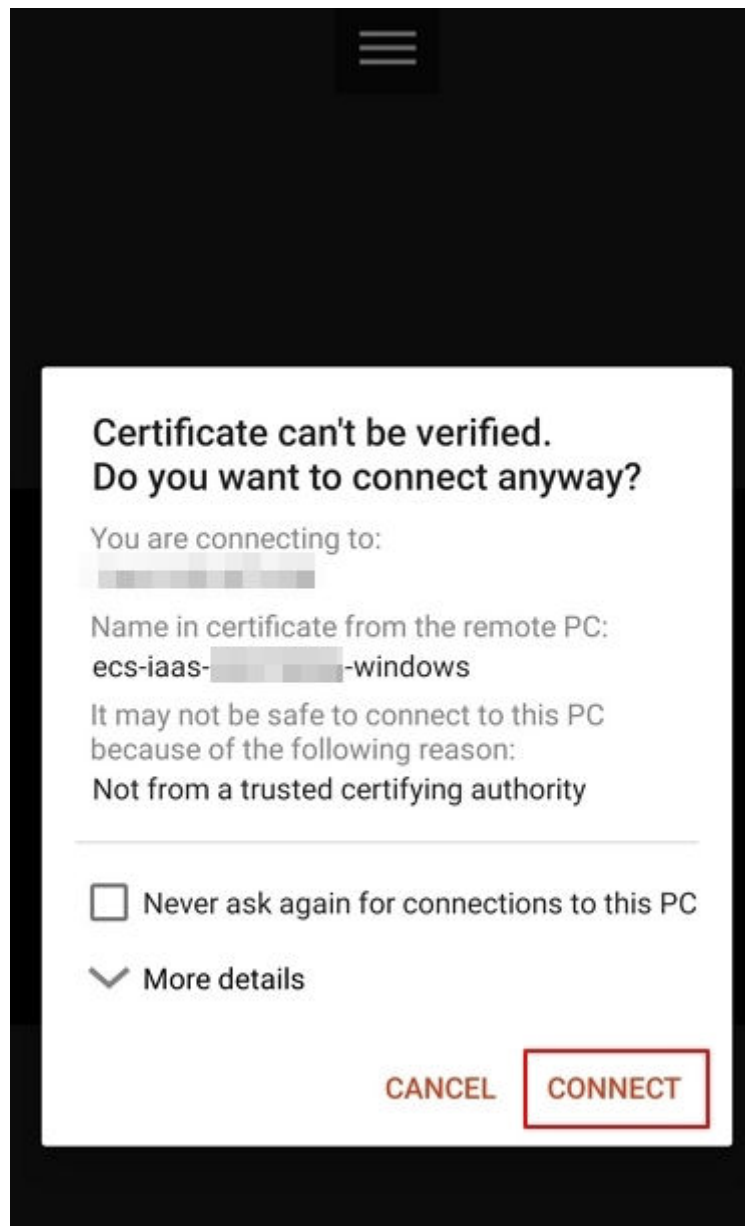
4. On the **Remote Desktop** page, tap the icon of the target Windows ECS.

Figure 3-13 Logging in to the Windows ECS

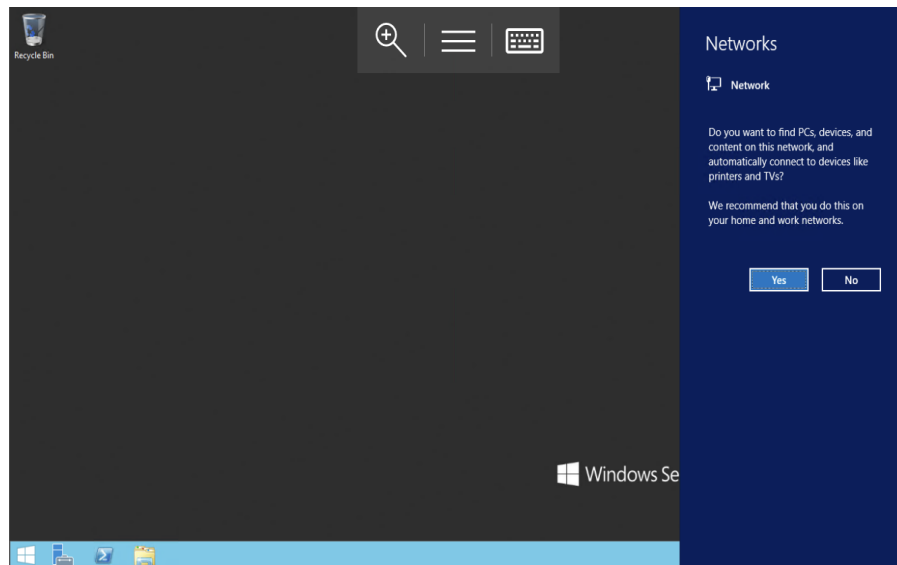


5. Confirm the information and tap **CONNECT**.

Figure 3-14 CONNECT



You have logged in to the Windows ECS.

Figure 3-15 Successful login

3.3.6 Logging In to Windows ECS from a Mac

Scenarios

This section describes how to use a remote login tool to log in to a Windows ECS from a Mac. In this section, the remote login tool Microsoft Remote Desktop for Mac and the ECS running Windows Server 2012 R2 Data Center 64bit are used as an example.

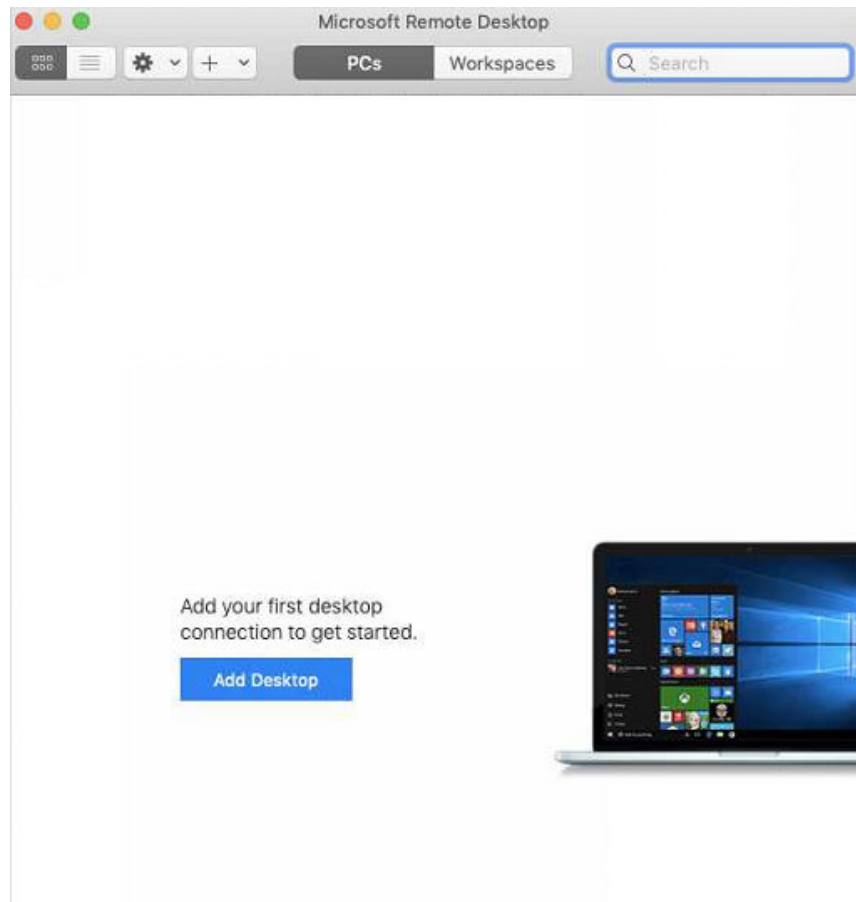
Prerequisites

- The target ECS is running.
- You have obtained the username and password for logging in to the ECS.
- You have bound an EIP to the ECS. For details, see [9.1 Binding an EIP](#).
- Access to port 3389 is allowed in the inbound direction of the security group to which the ECS belongs. For details, see [8.1.4 Configuring Security Group Rules](#).
- The remote access tool supported by Mac, such as Microsoft Remote Desktop for Mac has been installed. For details, see [Download Microsoft Remote Desktop for Mac](#).

Procedure

1. Start Microsoft Remote Desktop.
2. Click **Add Desktop**.

Figure 3-16 Add Desktop



3. On the **Add PC** page, set login information.
 - **PC name:** Enter the EIP bound to the target Windows ECS.
 - **User account:** Select **Add user account** from the drop-down list. The **Add user account** dialog box is displayed.
 - i. Enter username **administrator** and password for logging in to the Windows ECS and click **Add**.

Figure 3-17 Add user account

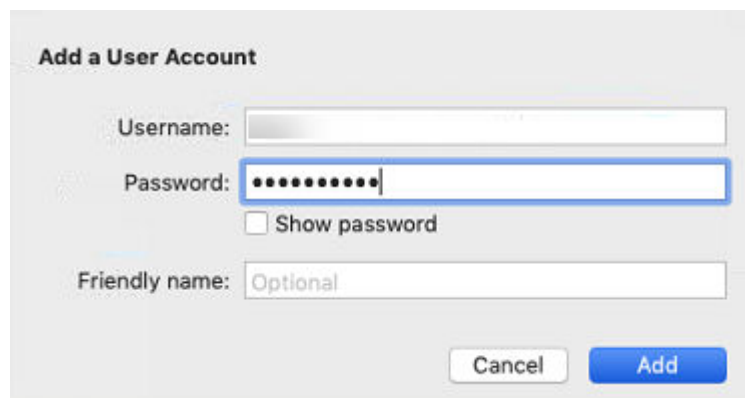
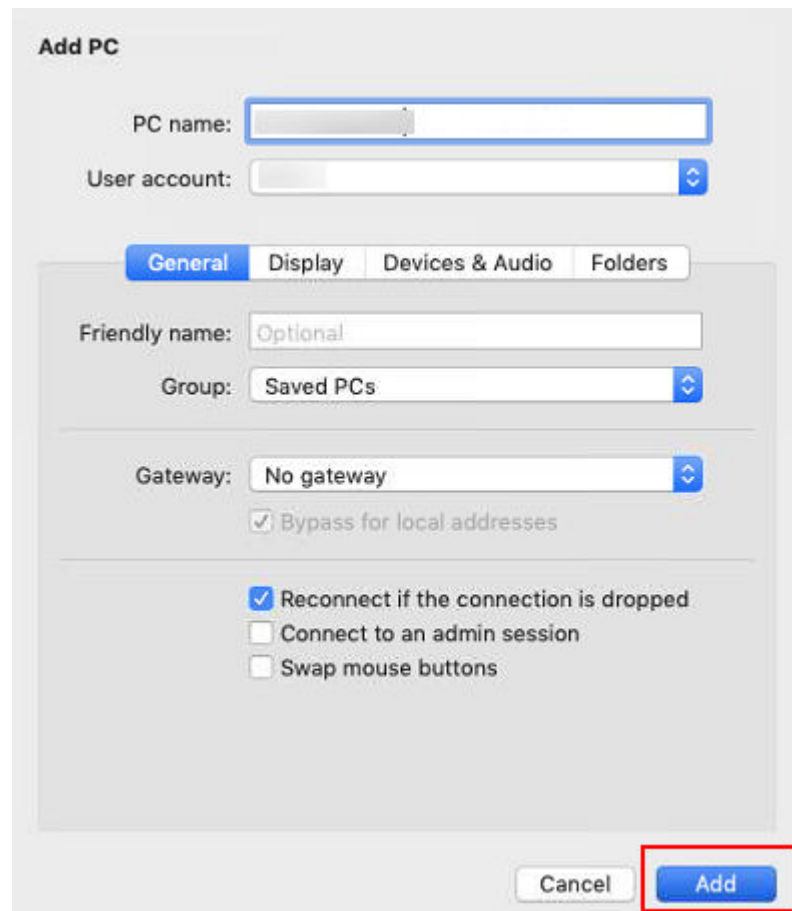
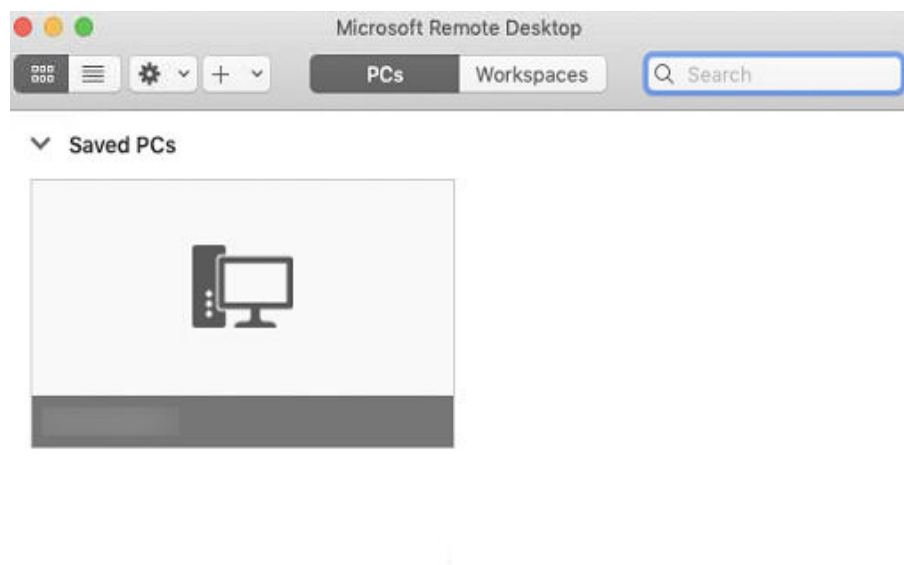


Figure 3-18 Add PC



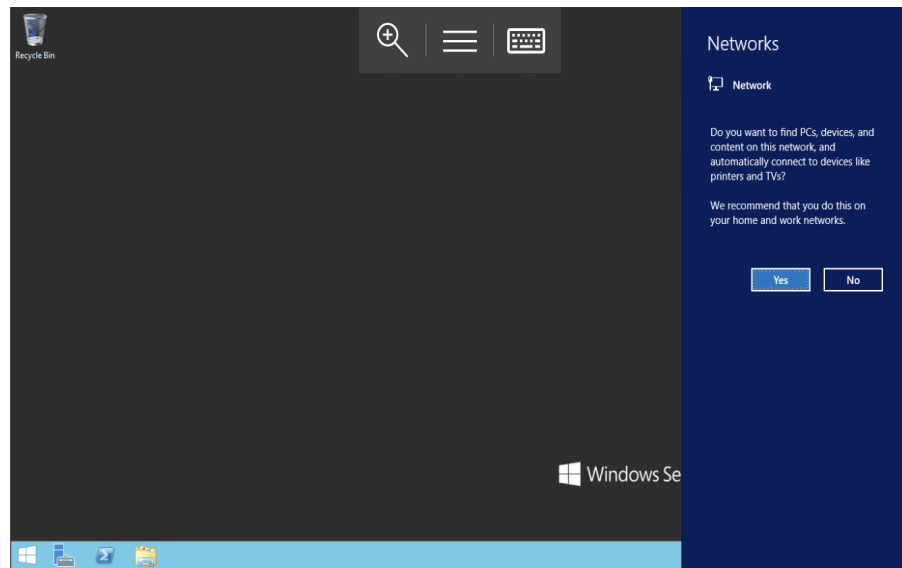
4. On the **Remote Desktop** page, double-click the icon of the target Windows ECS.

Figure 3-19 Double-click for login



5. Confirm the information and click **CONNECT**.
You have logged in to the Windows ECS.

Figure 3-20 Successful login



3.4 Logging In to a Linux ECS

3.4.1 Login Overview

Constraints

- Only a running ECS can be logged in.
- The username for logging in to a Linux ECS is **root**.

Login Modes

Select a login mode as required and log in to the target ECS.

Table 3-4 Linux ECS login modes

ECS OS	Local OS	Connection Method	Requirement
Linux	Windows	Use a remote login tool, such as PuTTY or Xshell. <ul style="list-style-type: none"> • Password-authenticated: Logging In to the Linux ECS from Local Windows • Key-pair-authenticated: Logging In to the Linux ECS from Local Windows 	The target ECS has had an EIP bound.

ECS OS	Local OS	Connection Method	Requirement
	Linux	Run commands. <ul style="list-style-type: none">• Password-authenticated: Logging In to the Linux ECS from Local Linux• Key-pair-authenticated: Logging In to the Linux ECS from Local Linux	
	Mobile terminal	Use an SSH client tool, such as Termius or JuiceSSH, to log in to the ECS. 3.4.5 Logging In to a Linux ECS from a Mobile Terminal	
	Windows	Use the remote login function available on the management console. For details, see 3.4.2 Login Using VNC .	No EIP is required.

3.4.2 Login Using VNC

Scenarios

This section describes how to use VNC provided on the management console to log in to an ECS.

For instructions about how to copy and paste data on VNC pages after the ECS login, see [Follow-up Procedure](#).


NOTE

Before using remote login (VNC) provided on the management console to log in to a Linux ECS authenticated using a key pair, log in to the ECS [using an SSH key](#) and set a login password.

Prerequisites

- You have used an SSH key to log in to the Linux ECS authenticated using a key pair and set a login password.
- An EIP has been bound to the ECS.

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. In the **Operation** column of the target ECS, click **Remote Login**.

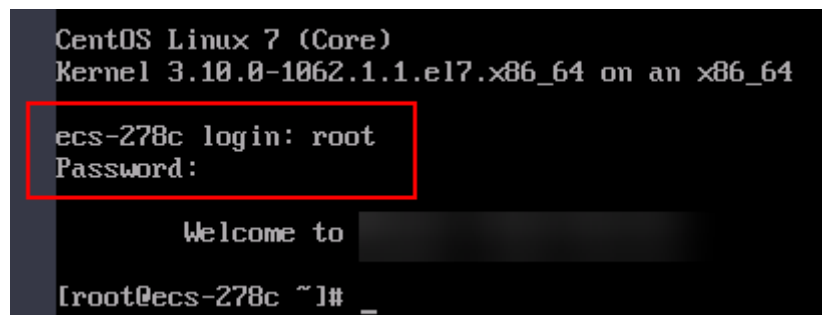
- (Optional) When the system displays "Press CTRL+ALT+DELETE to log on", click **Ctrl+Alt+Del** in the upper part of the remote login page to log in to the ECS.

 **NOTE**

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

- Enter the ECS password as prompted.

Figure 3-21 Username (root as an example) and password

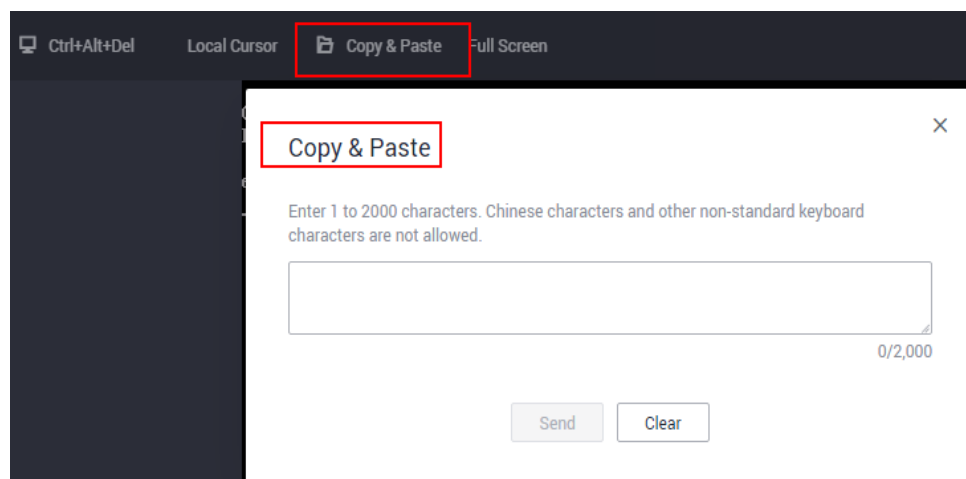


Follow-up Procedure

Local commands can be copied to an ECS. To do so, perform the following operations:

- Log in to the ECS using VNC.
- Click **Input Commands** in the upper right corner of the page.

Figure 3-22 Copy & Paste



- Press **Ctrl+C** to copy data from the local computer.
- Press **Ctrl+V** to paste the local data to the **Copy Commands** window.
- Click **Send**.
Send the copied data to the CLI.

 NOTE

There is a low probability that data is lost when you use Input Commands on the VNC page of a GUI-based Linux ECS. This is because the number of ECS vCPUs fails to meet GUI requirements. In such a case, you are advised to send a maximum of 5 characters at a time or switch from GUI to CLI (also called text interface), and then use the command input function.

3.4.3 Login Using an SSH Key

Scenarios

This section describes how to remotely log in to a Linux ECS using an SSH key pair from Windows and Linux, respectively.

Prerequisites

- You have obtained the private key file used during ECS creation.
- You have bound an EIP to the ECS. For details, see [3.2.3 Viewing Details About an ECS](#).
- You have configured the inbound rules of the security group. For details, see [8.1.4 Configuring Security Group Rules](#).
- The network connection between the login tool (PuTTY) and the target ECS is normal. For example, the default port 22 is not blocked by the firewall.

Logging In to the Linux ECS from Local Windows

To log in to the Linux ECS from local Windows, perform the operations described in this section.

Method 1: Use PuTTY to log in to the ECS.

The following operations use PuTTY as an example. Before logging in to the ECS using PuTTY, make sure that the private key file has been converted to .ppk format.

1. Check whether the private key file has been converted to .ppk format.
 - If yes, go to step [7](#).
 - If no, go to step [2](#).
2. Visit the following website and download PuTTY and PuTTYgen:
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

 NOTE

PuTTYgen is a key generator, which is used to create a key pair that consists of a public key and a private key for PuTTY.

3. Run PuTTYgen.
4. In the **Actions** pane, click **Load** and import the private key file that you stored during ECS creation.
Ensure that the format of **All files (*.*)** is selected.
5. Click **Save private key**.

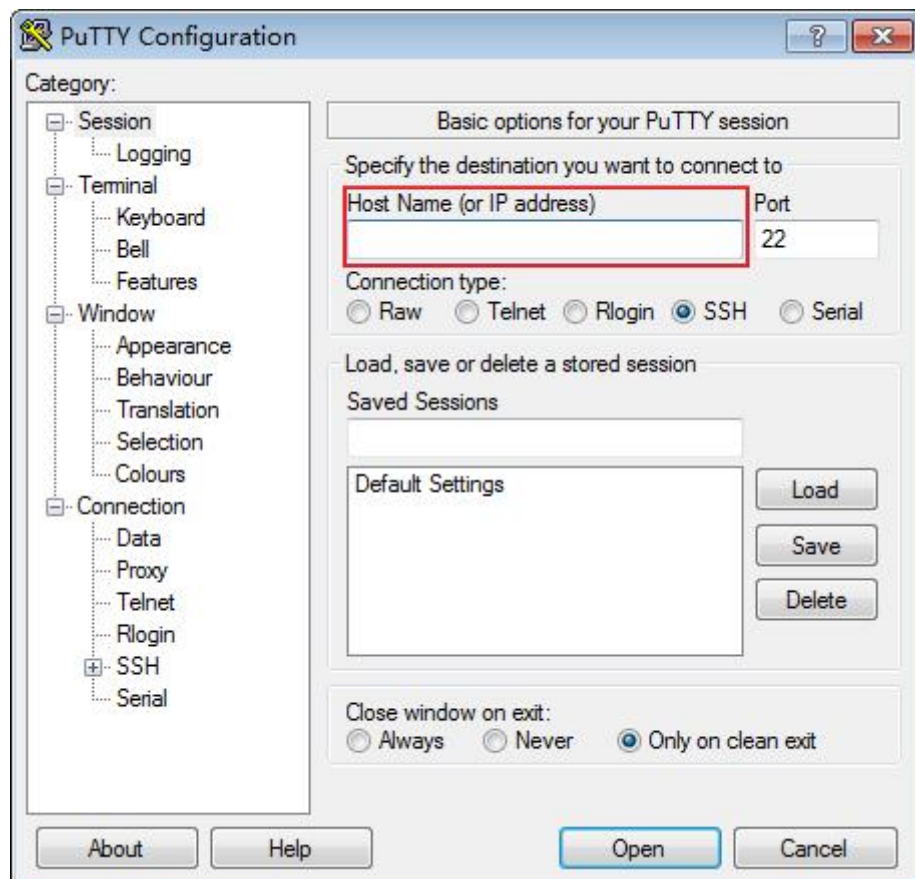
6. Save the converted private key, for example, **kp-123.ppk**, to the local computer.
7. Double-click **PuTTY.EXE**. The **PuTTY Configuration** page is displayed.
8. Choose **Connection > Data**. Enter the image username in **Auto-login username**.

NOTE

When you log in to an ECS using an SSH key:

- The image username is **core** for a CoreOS public image.
 - The image username is **root** for a non-CoreOS public image.
9. Choose **Connection > SSH > Auth**. In the last configuration item **Private key file for authentication**, click **Browse** and select the private key converted in step 6.
 10. Choose **Session** and enter the EIP of the ECS under **Host Name (or IP address)**.

Figure 3-23 Configuring the EIP



11. Click **Open**.
Log in to the ECS.

Method 2: Use Xshell to log in to the ECS.

1. Start the Xshell tool.
2. Run the following command using the EIP to remotely log in to the ECS through SSH:

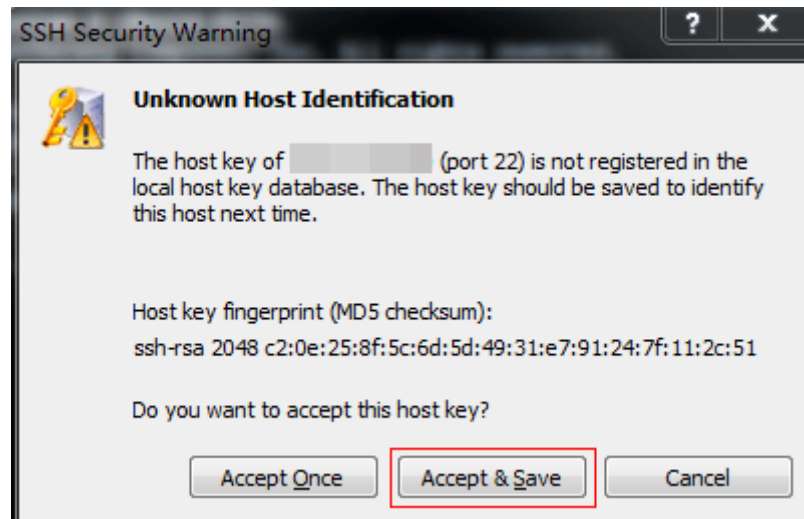
```
ssh Username@EIP
```

An example is provided as follows:

```
ssh root@192.168.0.1
```

3. (Optional) If the system displays the **SSH Security Warning** dialog box, click **Accept & Save**.

Figure 3-24 SSH Security Warning



4. Select **Public Key** and click **Browse** beside the user key text box.
5. In the user key dialog box, click **Import**.
6. Select the locally stored key file and click **Open**.
7. Click **OK** to log in to the ECS.

Logging In to the Linux ECS from Local Linux

To log in to the Linux ECS from local Linux, perform the operations described in this section. The following operations use private key file **kp-123.pem** as an example to log in to the ECS. The name of your private key file may differ.

1. On the Linux CLI, run the following command to change operation permissions:

```
chmod 400 /path/kp-123.pem
```

NOTE

In the preceding command, *path* refers to the path where the key file is saved.

2. Run the following command to log in to the ECS:

```
ssh -i /path/kp-123.pem Default username@EIP
```

For example, if the default username is **linux** and the EIP is **123.123.123.123**, run the following command:

```
ssh -i /path/kp-123.pem linux@123.123.123.123
```

 NOTE

In the preceding command:

- *path* refers to the path under which the key file is stored.
- *EIP* is the EIP bound to the ECS.

Follow-up Procedure

- After logging in to the ECS using the SSH key, you can set a password to log in to the ECS using VNC.

3.4.4 Login Using an SSH Password

Scenarios

This section describes how to remotely log in to a Linux ECS using an SSH password from Windows and Linux, respectively.

Prerequisites

- The target ECS is running.
- You have bound an EIP to the ECS. For details, see [9.1 Binding an EIP](#).
- Access to port 22 is allowed in the inbound direction of the security group to which the ECS belongs. For details, see [8.1.4 Configuring Security Group Rules](#).
- The network connection between the login tool (PuTTY) and the target ECS is normal. For example, the default port 22 is not blocked by the firewall.

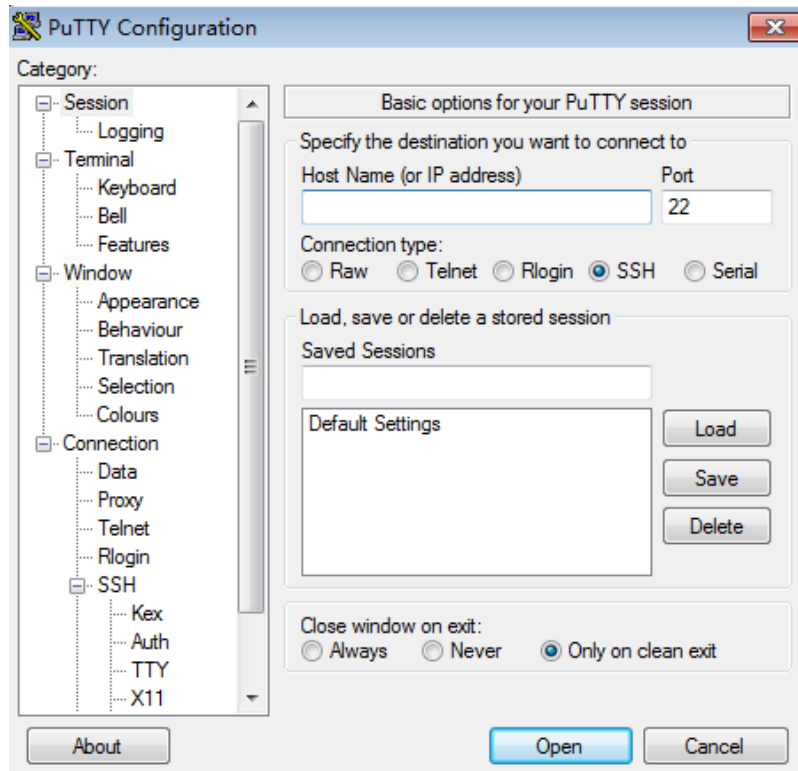
Logging In to the Linux ECS from Local Windows

To log in to the Linux ECS from local Windows, perform the operations described in this section.

The following operations use PuTTY as an example to log in to the ECS.

1. Visit the following website and download PuTTY and PuTTYgen:
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>
2. Run PuTTY.
3. Click **Session**.
 - a. **Host Name (or IP address)**: EIP bound to the ECS
 - b. **Port**: 22
 - c. **Connection type**: SSH
 - d. **Saved Sessions**: Task name, which can be clicked for remote connection when you use PuTTY next time

Figure 3-25 Session



4. Click **Window**. Then, select **UTF-8** for **Received data assumed to be in which character set:** in **Translation**.
5. Click **Open**.

If you log in to the ECS for the first time, PuTTY displays a security warning dialog box, asking you whether to accept the ECS security certificate. Click **Yes** to save the certificate to your local registry.

6. After the SSH connection to the ECS is set up, enter the username and password as prompted to log in to the ECS.

Logging In to the Linux ECS from Local Linux

To log in to the Linux ECS from local Linux, run the following command: `ssh EIP bound to the ECS`

3.4.5 Logging In to a Linux ECS from a Mobile Terminal

Scenarios

This section describes how to access a Linux ECS from a mobile terminal.

- For instructions about how to log in to a Linux ECS from an iOS terminal through iTerminal-SSH Telnet, see [Logging In to a Linux ECS from an iOS Terminal](#).
- For instructions about how to log in to a Linux ECS from an Android terminal through JuiceSSH, see [Logging In to a Linux ECS from an Android Terminal](#).

Prerequisites

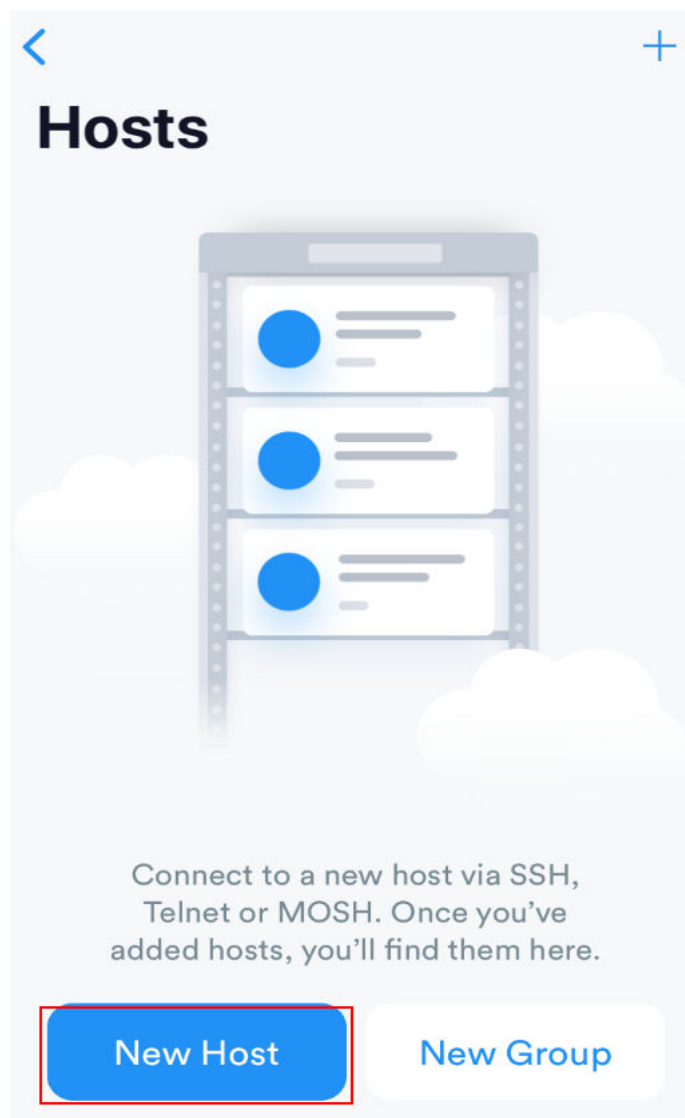
- The target ECS is running.
- You have obtained the username and password for logging in to the ECS.
- You have bound an EIP to the ECS. For details, see [9.1 Binding an EIP](#).
- Access to port 22 is allowed in the inbound direction of the security group to which the ECS belongs. For details, see [8.1.4 Configuring Security Group Rules](#).

Logging In to a Linux ECS from an iOS Terminal

Before performing the operation, make sure that you have installed an SSH client tool, taking Termius as an example, on the iOS terminal. In this example, the Linux ECS runs CentOS 7.6, and it is authenticated using a username and password.

1. Start Termius and tap **New Host**.

Figure 3-26 New Host



2. On the **New Host** page, set the following parameters:
 - **Alias:** Enter the hostname. In this example, set this parameter to **ecs01**.
 - **Hostname:** Enter the EIP bound to the target ECS.
 - **Use SSH:** Enable it.
 - **Host:** Enter the EIP bound to the target ECS.
 - **Port:** Enter port number **22**.
 - **Username:** Enter **root**.
 - **Password:** Enter the login password.

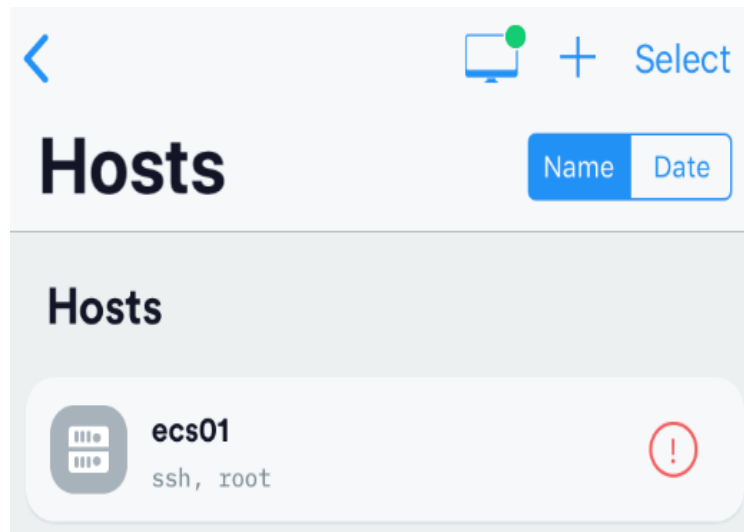
Figure 3-27 Setting parameters

The screenshot shows the 'New Host' configuration page with the following elements:

- Buttons: Cancel, New Host, Save
- Field 1: Alias (highlighted with a red box and number 1)
- Field 2: Hostname (highlighted with a red box and number 2)
- Field 3: Use SSH (highlighted with a red box and number 3, with a blue toggle switch)
- Field 4: Port (highlighted with a red box and number 4, with value 22 and 'Default' below it)
- Field 5: Username (highlighted with a red box and number 5, with value root and a user icon)
- Field 6: Password (highlighted with a red box and number 6, with a masked password field)

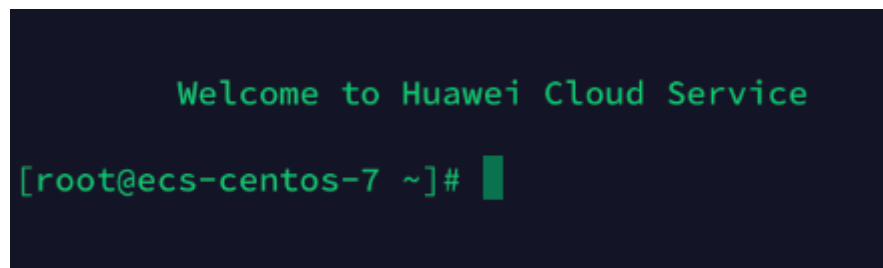
3. Tap **Save** in the upper right corner of the page to save the login settings. On the **Hosts** page, tap the name of the connection.

Figure 3-28 Login information



If the following page is displayed, you have connected to the Linux ECS.

Figure 3-29 Connected

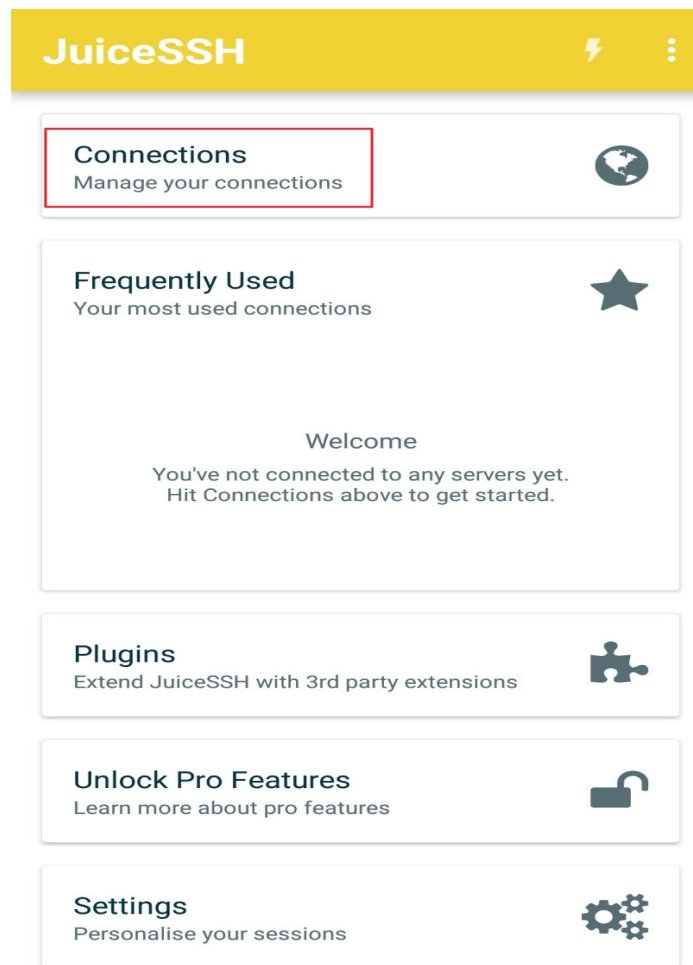


Logging In to a Linux ECS from an Android Terminal

Before performing the operation, make sure that you have installed JuiceSSH on the Android terminal. In this example, the Linux ECS runs CentOS 7.6, and it is authenticated using a username and password.

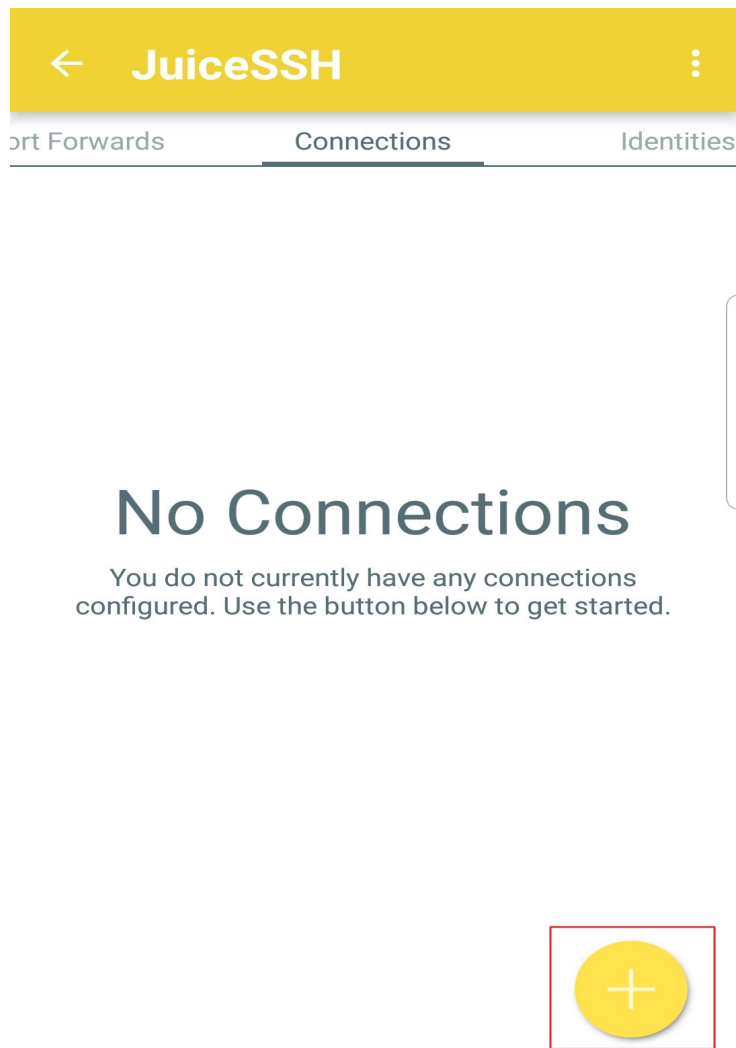
1. Start JuiceSSH and tap **Connections**.

Figure 3-30 Starting JuiceSSH



2. On the **Connections** page, tap .

Figure 3-31 Connections




3. On the **New Connection** page, add basic and advanced settings and save the settings. The parameters are as follows:
 - **Nickname:** Set the name of the login session. In this example, set this parameter to **linux_test**.
 - **Type:** Retain the default value **SSH**.
 - **Address:** Enter the EIP bound to the target Linux ECS.
 - Perform the following operations to set **Identity**:
 - i. Tap **Identity** and choose **New** from the drop-down list.
 - ii. On the **New Identity** page, set the following parameters and tap .
 - o **Nickname:** Set an identity name as required to facilitate subsequent management. This parameter is optional. In this example, set it to **linux_test**.
 - o **Username:** Enter **root**.
 - o **Password:** Tap **SET (OPTIONAL)**, enter the login password, and tap **OK**.

Figure 3-32 New Identity

← New Identity ✓

IDENTITY

Nickname:

Username:

Password:

Private Key:

SNIPPET

JuiceSSH Pro users can take advantage of an automatically generated snippet to add a public key to a servers `~/.ssh/authorized_keys` file and set the correct permissions.

- **Port:** Enter port number **22**.

Figure 3-33 Port number

← **New Connection** ✓

BASIC SETTINGS

Nickname: linux_test

Type: SSH ▼

Address: [blurred]

Identity: linux_test ▼

ADVANCED SETTINGS

Port: 22

Connect Via: (Optional) ▼

Run Snippet: (Optional) ▼

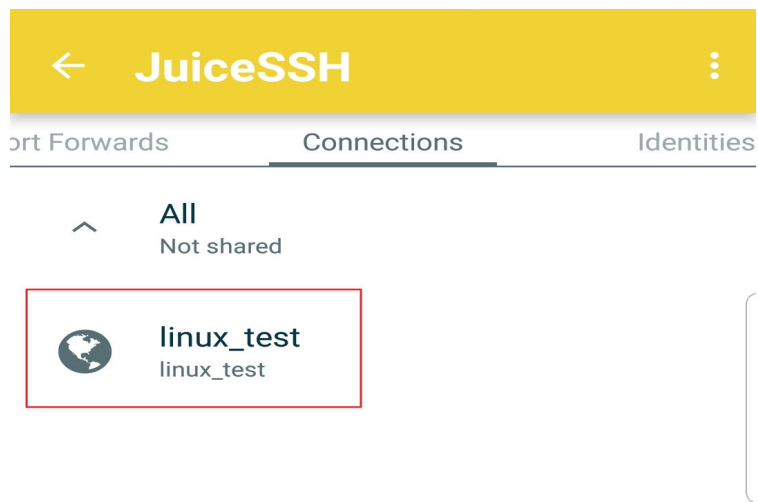
Backspace: Default (sends DEL) ▼

GROUPS

ADD TO GROUP

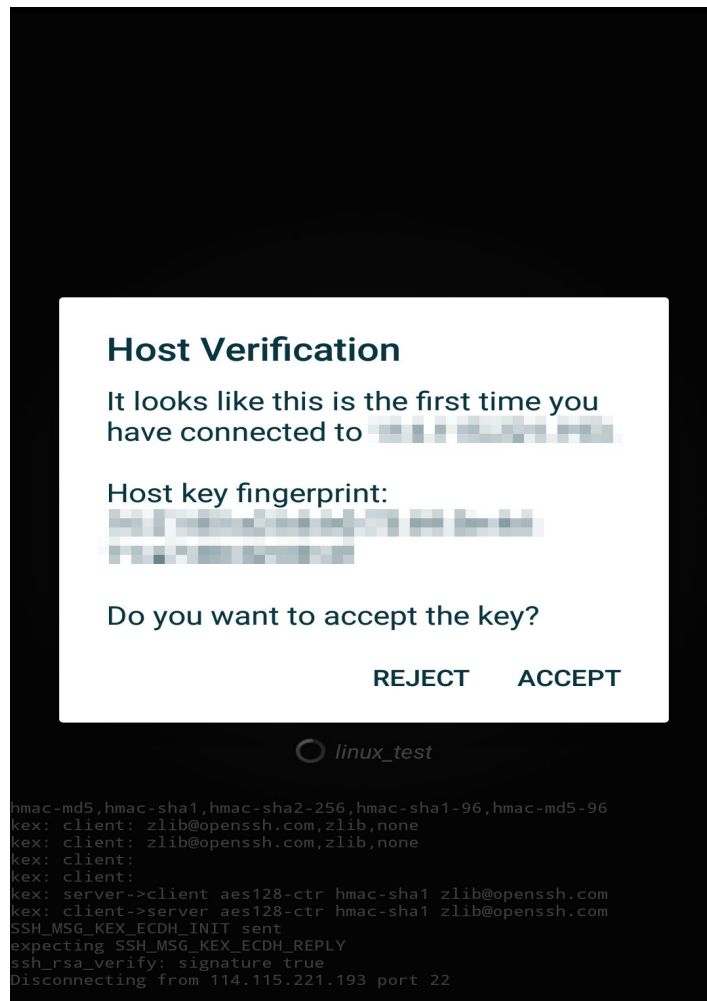
4. On the **Connections** page, tap the created connection.

Figure 3-34 Connection



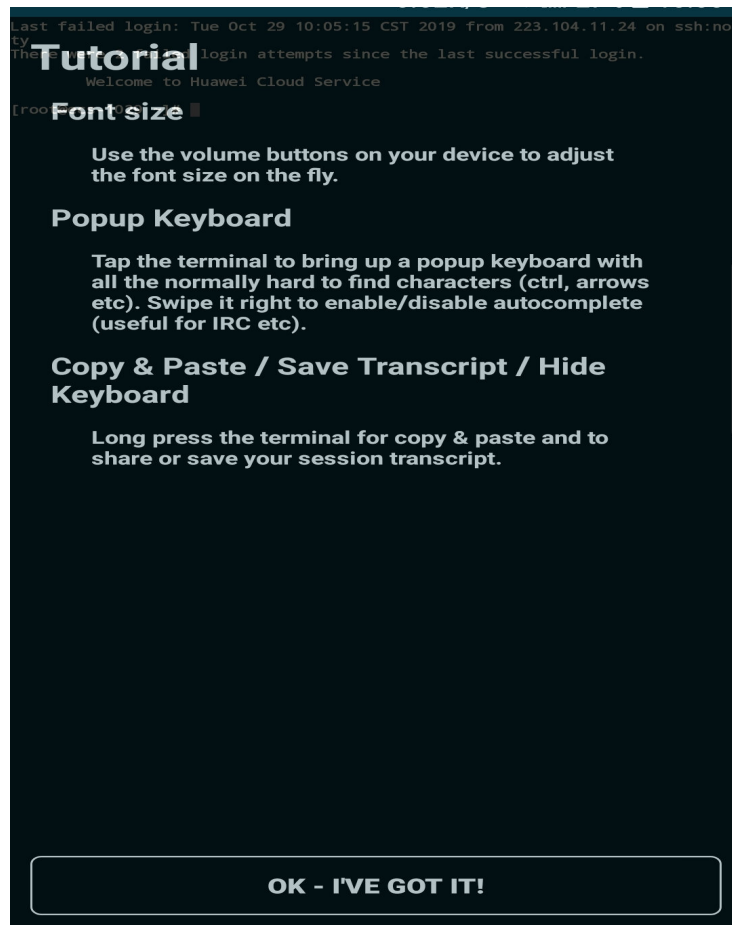
5. Confirm the information that is displayed and tap **ACCEPT**.

Figure 3-35 Confirming the information



6. (Optional) When you log in to the ECS for the first time, JuiceSSH displays a tutorial for you, including setting the font size and popping up the keyboard. Confirm the information and click **OK - I'VE GOT IT**.

Figure 3-36 Tutorial



You have logged in to the Linux ECS.

Figure 3-37 Successful login



3.5 Managing ECSs



3.5.1 Changing an ECS Name

Scenarios


The name of a created ECS can be changed to meet your service requirements.

Multiple ECS names can be changed in a batch. After the change, the ECS names are the same.

Procedure for a Single ECS

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. Click the name of the target ECS.
5. On the page providing details about the ECS, click  following the ECS name. Then, change the name as prompted.
Allow duplicate ECS name: allows ECS names to be duplicate. If **Allow duplicate ECS name** is not selected and the target name is the same as an existing ECS name, the system displays a message indicating that the name has been used and you need to change another name.
6. Click **OK**.

Procedure for Batch Operations

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. Select the target ECSs.
5. Click **More** in the upper part of the ECS list and select **Change ECS Name** from the drop-down list.
6. Enter the new name.
7. Click **OK**.
If you change ECS names in a batch, the new ECS names are the same, for example, all are **ecs-test**.

3.5.2 Reinstalling the OS

Scenarios

If the OS of an ECS fails to start or requires optimization, reinstall the OS.

Notes

- After the OS is reinstalled, the IP and MAC addresses of the ECS remain unchanged.
- Reinstalling the OS clears the data in all partitions of the EVS system disk, including the system partition. Therefore, back up data before reinstalling the OS.
- Reinstalling the OS does not affect data disks.

Constraints


- The EVS disk quota must be greater than 0.
- If the target ECS is created using a private image, ensure that the private image is available.

- H2 ECSs do not support OS reinstallation.

Prerequisites

- The target ECS is stopped.
- The target ECS has a system disk attached.

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. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Reinstall OS**.

Only stopped ECSs support OS reinstallation. If the ECS is not stopped, stop it before proceeding with reinstallation.

5. Configure the login mode.
If the target ECS uses key pair authentication, you can replace the original key pair.
6. Click **OK**.
7. On the **ECS OS Reinstallation** page, confirm the specifications and click **Submit**.

After the request is submitted, the ECS status changes to **Reinstalling**. The reinstallation has been completed when the ECS status changes to **Running**.

NOTE

A temporary ECS is created during the reinstallation process. After reinstallation, this ECS will be automatically deleted. Do not perform any operation on the temporary ECS during the reinstallation process.

Follow-up Procedure

If the reinstallation is unsuccessful, perform steps **3** to **7** again to retry reinstalling the OS again.

If the second reinstallation attempt is unsuccessful, contact customer service for manual recovery at the backend.

3.5.3 Changing the OS

Scenarios

Changing an ECS OS will change the system disk attached to the ECS. After the changing, the system disk ID of the ECS will be changed, and the original system disk will be deleted.

If the OS running on an ECS cannot meet service requirements, change the ECS OS.

The public cloud supports changing between image types (public images, private images, and shared images) and between OSs. You can change your OS to the one of a different image type.

Constraints

- The EVS disk quota must be greater than 0.
- H2 ECSs do not support OS change.
- Windows and Linux cannot be changed to each other.
- Switching between the ECSs in BIOS boot mode and in UEFI boot mode is not allowed.


Notes

- After the OS is changed, the original OS is not retained, and the original system disk is deleted, including the data in all partitions of the system disk.
- Back up data before changing the OS. For details, see *Cloud Backup and Recovery User Guide*.
- Changing the OS does not affect data in data disks.
- After the OS is changed, your service running environment must be deployed in the new OS again.
- After the OS is changed, the ECS will be automatically started.
- After the OS is changed, the system disk type of the ECS cannot be changed.
- After the OS is changed, the IP and MAC addresses of the ECS remain unchanged.
- After the OS is changed, customized configurations, such as DNS and hostname of the original OS will be reset and require reconfiguration.
- It takes about 10-20 minutes to change the OS. During this process, the ECS is in **Changing OS** state.

Prerequisites

- The target ECS is stopped.
- The target ECS has a system disk attached.
- Necessary data has been backed up. (Changing the OS clears the data in all partitions of the system disk, including the system partition.)
- If the original ECS uses password authentication while the new ECS uses key pair authentication, ensure that a key pair is available.
- If a private image is required for changing the ECS OS, create the desired private image by following the instructions provided in *Image Management Service User Guide*.
 - If an ECS image is required, make sure that a private image has been created using the ECS.
 - If a local image file is required, make sure that the image file has been imported to the cloud platform and registered as a private image.
 - If a private image from another region is required, make sure that the image has been copied.
 - If a private image from another user account is required, make sure that the image has been shared with you.

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. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Change OS**.
Only stopped ECSs support OS changing. If the ECS is not stopped, stop it before proceeding with changing.
5. Modify related ECS parameters, such as **Image Type** and **Image**, based on service requirements.
6. Configure the login mode.
If the target ECS uses key pair authentication, you can replace the original key pair.
7. Click **OK**.
8. On the **Change OS** page, confirm the specifications and click **Submit**.
After the application is submitted, the ECS status changes to **Changing OS**. The OS changing has been completed when **Changing OS** disappears.

NOTE

A temporary ECS is created during the OS changing process. After the process is complete, this ECS will be automatically deleted.

Follow-up Procedure

- If the OSs before and after the OS change are both Linux, and automatic partition mounting upon system startup has been enabled for the data disk, the data disk partition mounting information will be lost after the OS is changed. In such a case, you need to update the **/etc/fstab** configuration.
 - a. Write the new partition information into **/etc/fstab**.
You are advised to back up the **/etc/fstab** file before writing data into it.
To enable automatic partition mounting upon system startup, see [2.3.4 Initializing a Linux Data Disk \(fdisk\)](#).
 - b. Mount the partition so that you can use the data disk.
mount *Disk partition Device name*
 - c. Check the mount result.
df -TH
- If the OS change is unsuccessful, perform steps **3** to **8** again to retry changing the OS again.
- If the second OS change attempt is unsuccessful, contact customer service for manual recovery at the backend.

3.5.4 Managing ECS Groups

Scenarios

An ECS group logically groups ECSs. The ECSs in an ECS group comply with the same policy associated with the ECS group.

Only the anti-affinity policy is supported. ECSs in the same ECS group are deployed on different hosts, improving service reliability.


You can use an ECS group to deploy target ECSs on different physical servers to ensure high service availability and underlying DR capabilities.

An ECS group supports the following functions:

- [Creating an ECS Group](#)
- [Adding an ECS to an ECS Group](#)
 - Add an ECS to an ECS group during ECS creation.
 - Add a created ECS to an ECS group.
- [Removing an ECS from an ECS Group](#)
- [Deleting an ECS Group](#)

Creating an ECS Group

Create an ECS group to apply the same policy to all group members. ECS groups are independent from each other.


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. In the navigation pane on the left, choose **ECS Group**.
5. On the **ECS Group** page, click **Create ECS Group**.
6. Enter an ECS group name.
The **Anti-affinity** policy is used by default.
7. Click **OK**.

Adding an ECS to an ECS Group

After an ECS is added to an ECS group, it can be deployed on a physical server different from the physical servers accommodating other ECSs in the same ECS group.


NOTICE

- The ECS to be added must be stopped.
- After an ECS is added to an ECS group, the system reallocates the physical server accommodating the ECS so that the ECS and other ECSs in the ECS group are deployed on different physical servers. However, when the ECS is restarted, the startup may fail due to insufficient resources. In such a case, remove the ECS from the ECS group and restart the ECS.
- An ECS with local disks attached cannot be added to an ECS group after the ECS is created. To use ECS group functions, select an ECS group during ECS creation.
- An existing ECS cannot be added to an ECS group if it has a local disk attached (for example, a disk-intensive, H2, P1, or P2 ECS), a local NVMe SSD disk attached (for example, of the ultra-high I/O type), a GPU attached (for example, a G3 ECS), or an FPGA attached (for example, an FP1 or FP1c ECS). To use ECS group functions on such ECSs, select an ECS group when creating the ECS.

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. In the navigation pane on the left, choose **ECS Group**.
5. Click **Add ECS** in the **Operation** column.
6. On the **Add ECS** page, select the ECS to be added.
7. Click **OK**.

Removing an ECS from an ECS Group

After an ECS is removed from an ECS group, the ECS does not comply with the anti-affinity policy anymore.


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. In the navigation pane on the left, choose **ECS Group**.
5. Expand the ECS group information and view the ECSs in the ECS group.
6. Click **Remove** in the **Operation** column of the target ECS.
7. Click **OK**.

The ECS is removed from the ECS group.

Deleting an ECS Group

After an ECS group is deleted, the policy does not apply to the ECSs in the ECS group anymore.

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. In the navigation pane on the left, choose **ECS Group**.
5. Click **Delete** in the **Operation** column of the target ECS group.
6. Click **OK**.


3.5.5 Backing Up ECS Data

Scenarios


Cloud Backup and Recovery (CBR) backs up data for EVS disks and ECSs, and uses snapshot backups to restore the EVS disks and ECSs. In addition, CBR supports synchronizing backup data in the on-premises backup software OceanStor BCManager to the cloud. In this way, you can manage backup data on the cloud and restore data to other ECSs using the backup data. CBR maximizes the security and accuracy of your data to ensure service security.

CBR enhances data integrity and service continuity. For example, if an ECS or disk is faulty or a misoperation causes data loss, you can use backups to quickly restore data.

ECS Backup Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Choose **Storage > Cloud Backup and Recovery > Cloud Server Backup**.
4. Click **Create Server Backup Vault**.
For details, see "Create a Vault" in *Cloud Backup and Recovery User Guide*.
5. After a server backup vault is created, associate servers with the vault for backup.
For details, see "Associate a Server or Disk with the Vault" in *Cloud Backup and Recovery User Guide*.
6. Create a backup.
For details, see "Creating a Backup" in *Cloud Backup and Recovery User Guide*.

Disk Backup Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Choose **Storage > Cloud Backup and Recovery > Cloud Disk Backup**.
4. Click **Create Disk Backup Vault**.
For details, see "Create a Vault" in *Cloud Backup and Recovery User Guide*.
5. After a disk backup vault is created, associate disks with the vault for backup.
For details, see "Associate a Server or Disk with the Vault" in *Cloud Backup and Recovery User Guide*.

6. Create a backup.
For details, see "Creating a Backup" in *Cloud Backup and Recovery User Guide*.

3.5.6 Changing the Time Zone for an ECS

Scenarios

The default time zone for an ECS is the one you selected when creating the image that was used to create the ECS. This section describes how to change the time zone for an ECS to the local one or to another time zone in your network.

After you log in to your ECS, if you find that the time on the ECS is different from the local time, change the time zone for the ECS so that the time on the ECS is the same as the local time.

For Linux

The process of changing the time zone for a Linux ECS depends on the OS. In this section, the CentOS 6.x 64bit OS is used to demonstrate how to change the time zone for a Linux ECS.

1. Log in to the ECS.
2. Run the following command to switch to user **root**:
su - root
3. Run the following command to obtain the time zones supported by the ECS:

ls /usr/share/zoneinfo/

In the terminal display, the **/usr/share/zoneinfo** directory contains a hierarchy of time zone data files. Use the directory structure to obtain your desired time zone file.

The directory structure shown in **/usr/share/zoneinfo** includes both time zones and directories. The directories contain time zone files for specific cities. Locate the time zone for the city in which the ECS is located.

For example:

- If you are to use the time zone for Shanghai, China, run the **ls /usr/share/zoneinfo/Asia** command to obtain the directory **/usr/share/zoneinfo/Asia/Shanghai**.
- If you are to use the time zone for Paris, France, run the **ls /usr/share/zoneinfo/Europe** command to obtain the directory **/usr/share/zoneinfo/Europe/Paris**.

4. Set the target time zone.
 - a. Run the following command to open the **/etc/sysconfig/clock** file:
vim /etc/sysconfig/clock
 - b. Locate the **ZONE** entry and change its value to the name of the desired time zone file.

For example:

- If the target time zone is for Shanghai, China, change the **ZONE** entry value as follows:

```
ZONE="Asia/Shanghai"
```

- If the target time zone is for Paris, France, change the **ZONE** entry value as follows:

```
ZONE="Europe/Paris"
```

5. Press **Esc**. Then, run the following command to save and exit the **/etc/sysconfig/clock** file:
:wq
6. Run the following command to check whether the **/etc/localtime** file is available on the ECS:
ls /etc/localtime
 - If the file is available, go to step 7.
 - If the file is not available, go to step 8.
7. Run the following command to delete the existing **/etc/localtime** file:
rm /etc/localtime
8. Run the following command to create a symbolic link between **/etc/localtime** and your time zone file so that the ECS can find this time zone file when it references the local time:
ln -sf /usr/share/zoneinfo/Asia/Shanghai /etc/localtime
9. Run the following command to restart the ECS so that all services and applications running on the ECS use the new time zone:
reboot
10. Log in to the ECS again and run the following command as user **root** to check whether the time zone has been changed:

```
ls -lh /etc/localtime
```

The following information is displayed:

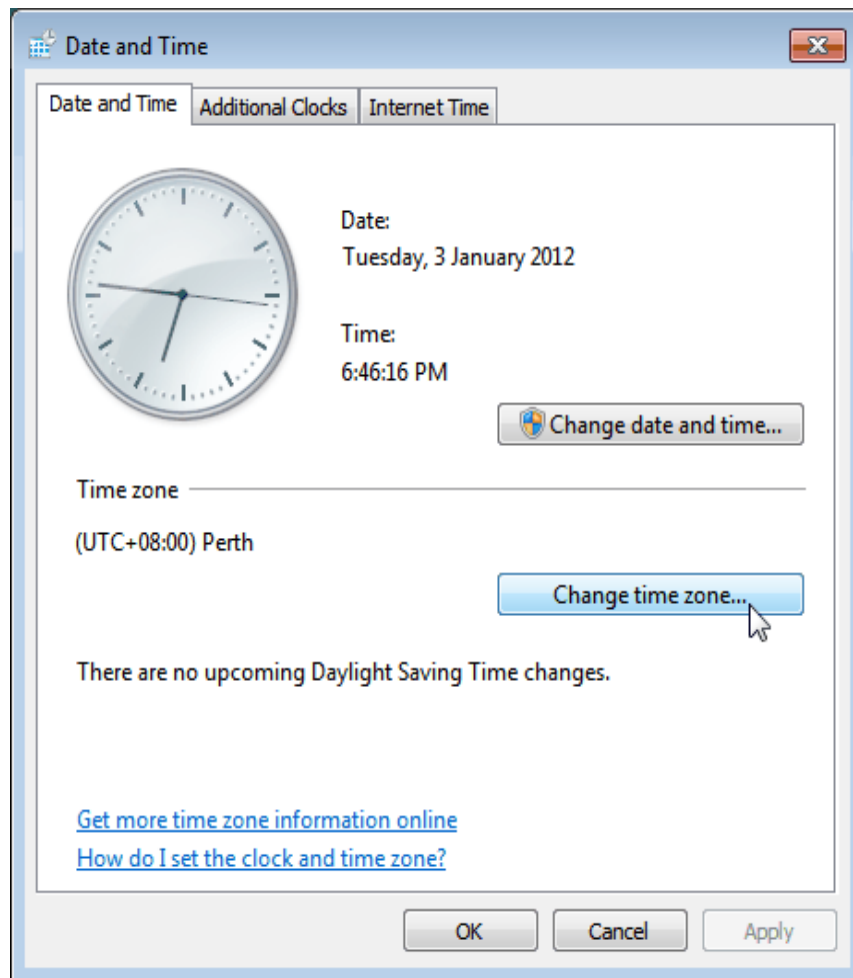
```
# ls -lh /etc/localtime  
lrwxrwxrwx 1 root root 33 Nov 27 11:01 /etc/localtime -> /usr/share/zoneinfo/Asia/Shanghai
```

For Windows

1. Log in to the ECS.
2. Click the time display on the far right side of the task bar located at the bottom of your screen. In the dialog box that is displayed, click **Change date and time settings**.

The **Date and Time** page is displayed.

Figure 3-38 Date and Time



3. Click **Change time zone**.
The **Time Zone Settings** page is displayed.
4. In the **Set the time zone** pane, choose the target time zone from the **Time zone** drop-down list.
5. Click **OK**.

3.6 Modifying ECS vCPU and Memory Specifications

3.6.1 General Operations for Modifying Specifications

Scenarios


If ECS specifications do not meet service requirements, you can modify the ECS specifications, including vCPUs and memory. Certain ECSs allow you to change their types when you modify their specifications.

Notes

- When modifying the specifications of an ECS, you are not allowed to select sold-out CPU and memory resources.

- If ECS specifications are downgraded, the ECS performance is deteriorated.
- Certain ECSs do not support specifications modification currently. For details about available ECS types as well as their functions and usage, see "Notes" in [1.5.3 ECS Types](#).
- When the disk status is **Expanding**, you are not allowed to modify the specifications of the ECS where the disk is attached.
- Before modifying the specifications of a Windows ECS, modify the SAN policy by following the instructions provided in [13.8.14 What Should I Do If a Disk Is Offline?](#) to prevent offline disks after the specifications are modified.
- Before modifying specifications, make sure that the ECS has been stopped.

Step 1: Modify Specifications

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, view the status of the target ECS.
If the ECS is not in **Stopped** state, click **More** in the **Operation** column and select **Stop**.
5. Click **More** in the **Operation** column and select **Modify Specifications**.
The **Modify ECS Specifications** page is displayed.
6. Select the new ECS type, vCPUs, and memory as prompted.
7. Click **Next**.
8. Confirm the modified configuration. Read and select the service agreement, and then click **Submit**.
9. Check whether the specifications have been modified.
After modifying the specifications, you can check whether the specifications have been modified in **Failures**.
 - a. Check whether **Failures** is displayed on the management console. For details, see [3.2.2 Viewing Failures](#).
 - If yes, go to step [9.b](#).
 - If no, the specifications have been modified.
 - b. Click **Failures**. Then, in the **Failures** dialog box, click **Operation Failures** and check whether the task is contained in the list by **Name/ID**, **Operated At**, or **Task**.
 - If yes, the specifications modification failed. See [Follow-up Procedure](#) for failure causes.
 - If no, the specifications have been modified.

Step 2: Check Disk Attachment

After specifications are modified, disk attachment may fail. Therefore, check disk attachment after specifications modification. If disks are properly attached, the specifications modification is successful.

- Windows
For details, see [13.4.3 What Should I Do If the Disk of a Windows ECS Becomes Offline After the ECS Specifications Are Modified?](#)
- Linux
For details, see [13.4.4 What Should I Do If the Disk of a Linux ECS Becomes Offline After the ECS Specifications Are Modified?](#)

Follow-up Procedure

Perform the following operations in the event of a specifications modification failure:

1. Log in to the management console.
2. Under **Management & Deployment**, click **Cloud Trace Service**.
3. In the navigation pane on the left, choose **Trace List**.
4. In the **Trace Name** column, locate the **resizeServer** event by resource ID.
The resource ID is the ID of the ECS on which the specifications modification failed.
5. Click **View Trace** in the **Operation** column to view the failure cause.
If the fault cannot be rectified based on logs, contact customer service.

3.7 Using User Data and Metadata

3.7.1 Obtaining Metadata

Scenarios

ECS metadata includes basic information of an ECS on the cloud platform, such as the ECS ID, hostname, and network information. ECS metadata can be obtained using either OpenStack APIs or EC2 APIs, as shown in [Table 3-5](#). The following describes the URI and methods of using the supported ECS metadata.

Notes

If the metadata contains sensitive data, take appropriate measures to protect the sensitive data, for example, controlling access permissions and encrypting the data.

Perform the following configuration on the firewall:

- Windows

If you need to assign permissions to only the administrator to access custom data, enable the firewall as an administrator and run the following commands in PowerShell:

```
PS C:\>$RejectPrincipal = New-Object -TypeName  
System.Security.Principal.NTAccount ("Everyone")
```

```
PS C:\>$RejectPrincipalSID =  
$RejectPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).  
Value
```

```

PS C:\>$ExceptPrincipal = New-Object -TypeName
System.Security.Principal.NTAccount ("Administrator")
PS C:\>$ExceptPrincipalSID =
$ExceptPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).
Value
PS C:\>$PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptPrincipalSID)(A;;CC;;;
$RejectPrincipalSID)"
PS C:\>New-NetFirewallRule -DisplayName "Reject metadata service for $
($RejectPrincipal.Value), exception: $($ExceptPrincipal.Value)" -Action
block -Direction out -Protocol TCP -RemoteAddress 169.254.169.254 -
LocalUser $PrincipalSDDL

```

- Linux

If you need to assign permissions to only user **root** to access custom data, run the following command as user **root**:

```

iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --
match owner ! --uid-owner root --jump REJECT

```

ECS Metadata Types

Table 3-5 ECS metadata types

Metadata Type	Metadata Item	Description
OpenStack	/meta_data.json	Displays ECS metadata. For the key fields in the ECS metadata, see Table 3-6 .
OpenStack	/password	Displays the password for logging in to an ECS. This metadata is used by Cloudbase-Init to store ciphertext passwords during initialization of key-pair-authenticated Windows ECSs.
OpenStack	/user_data	Displays ECS user data. This metadata allows you to specify scripts and configuration files for initializing ECSs. For details, see 3.7.2 Injecting User Data into ECSs . For password-authenticated Linux ECSs, this metadata is used to save password injection scripts.
OpenStack	/network_data.json	Displays ECS network information.

Metadata Type	Metadata Item	Description
OpenStack	/securitykey	Obtains temporary AKs and SKs. Before enabling an ECS to obtain a temporary AK and SK, make sure that the op_svc_ecs account has been authorized on IAM and that the desired ECS resources have been authorized for management.
EC2	/meta-data/ hostname	Displays the name of the host accommodating an ECS. To remove the suffix .novalocal from an ECS, see: 13.4.2 Is an ECS Hostname with Suffix .novalocal Normal?
EC2	/meta-data/ instance-type	Displays an ECS flavor.
EC2	/meta-data/ local-ipv4	Displays the fixed IP address of an ECS. If there are multiple NICs, only the IP address of the primary NIC is displayed.
EC2	/meta-data/ placement/ availability-zone	Displays the AZ accommodating an ECS.
EC2	/meta-data/ public-ipv4	Displays the EIP bound to an ECS. If there are multiple NICs, only the EIP of the primary NIC is displayed.
EC2	/meta-data/ public-keys/0/ openssh-key	Displays the public key of an ECS.
EC2	/user-data	Displays ECS user data.
EC2	/meta-data/ security-groups	Displays the security group to which an ECS belongs.

Table 3-6 Metadata key fields

Parameter	Type	Description
uuid	String	Specifies an ECS ID.
availability_zone	String	Specifies the AZ where an ECS locates.

Parameter	Type	Description
meta	Dict	Specifies the metadata information, including the image name, image ID, and VPC ID.
hostname	String	Specifies the name of the host accommodating an ECS. To remove the suffix .novalocal from an ECS, see: 13.4.2 Is an ECS Hostname with Suffix .novalocal Normal?
vpc_id	String	Specifies the ID of the VPC for an ECS.

Prerequisites

- The target ECS has been logged in.
- Security group rules in the outbound direction meet the following requirements:
 - **Protocol: TCP**
 - **Port Range: 80**
 - **Remote End: 169.254.0.0/16**

NOTE

If you use the default security group rules in the outbound direction, the preceding requirements are met, and the metadata can be accessed. Default security group rules in the outbound direction are as follows:

- **Protocol: ANY**
- **Port Range: ANY**
- **Remote End: 0.0.0.0/0**

Metadata (OpenStack Metadata API)

Displays ECS metadata.

- URI
`/169.254.169.254/openstack/latest/meta_data.json`

- Usage method
Supports GET requests.

- Example

To use cURL to view Linux ECS metadata, run the following command:

```
curl http://169.254.169.254/openstack/latest/meta_data.json
```

To use Invoke-RestMethod to view Windows ECS metadata, run the following command:

```
Invoke-RestMethod http://169.254.169.254/openstack/latest/meta_data.json | ConvertTo-Json
```

```
{
  "random_seed": "rEocCViRS+dNwlydGlxJHUp+00poeUsAdBFkbPbYQTmpNwpoEb43k9z+96TyrekNKS
+iLYDdRny4kKGoNPEVBCC05Hg1TcDbIAPfJwgJS1okqEtlcofUHKmL3K0fto
+5KXEDU3GNuGwyZXjdVb9HQWU+E1jztAJjqsahnU+g/tawABTVySLBKlAT8fMGax1mTGgArucn/
WzDcy19DGioKPE7F8lLtSQ4Ww3VCLK5VYB/h0x+4r7IVHrPmYX/
bi1Yhm3Dc4rRYNaTjdOV5gUOsbo3oAeQkmKwQ/
NO0N8qw5Ya4l8ZUW4tMav4mOsRySOOB35v0bvaJc6p
+50DTbWNeX5A2MLiEhTP3vsPrmvk4LRF7CLz2J2TGIM14OoVBw7LARwmv9cz532zHki/c8tlhRzLmOTXh/
wL36zFW10DeuReUGmxth7IGNmRMQKV6+mil78jm/KMPpgAdK3vwYF/
GcelOFJD2HghMUUCeMbwYnvijLTejuBpwhJMNIHA/NvlEsxJDxqBCoss/Jfe+yCmUFyxovJ
+L8oNkTzkmCNzw3Ra0hiKchGhqK3BleToV/kVx5DdF081xrEA
+qyoM6CVyfJtEoz1zIRryo09bJ65Eg6Jd8dj1UCVsdqRY1pljgzE/
Mzsw6AaaCVhaMJL7u7YmVdyKzA6z65Xtvujz0Vo=",
  "uuid": "ca9e8b7c-f2be-4b6d-a639-f10b4d994d04",
  "availability_zone": "lt-test-1c",
  "hostname": "ecs-ddd4-l00349281.novalocal",
  "launch_index": 0,
  "meta": {
    "metering.image_id": "3a64bd37-955e-40cd-ab9e-129db56bc05d",
    "metering.imagetype": "gold",
    "metering.resourcespeccode": "s3.medium.1.linux",
    "image_name": "CentOS 7.6 64bit",
    "os_bit": "64",
    "vpc_id": "3b6c201f-aeb3-4bce-b841-64756e66cb49",
    "metering.resourcetype": "1",
    "cascaded.instance_extrainfo": "pcibridge:2",
    "os_type": "Linux",
    "charging_mode": "0"
  },
  "project_id": "6e8b0c94265645f39c5abbe63c4113c6",
  "name": "ecs-ddd4-l00349281"
}
```

User Data (OpenStack Metadata API)

Displays ECS user data. The value is configured only when you create an ECS. It cannot be changed after the configuration.

- URI
`/169.254.169.254/openstack/latest/user_data`
- Usage method
Supports GET requests.
- Example

Linux:

curl `http://169.254.169.254/openstack/latest/user_data`

Windows:

Invoke-RestMethod `http://169.254.169.254/openstack/latest/user_data`

```
ICAgICAgDQoiQSBjbG91ZCBkb2VzIG5vdCBrbm93IHdoeSBpdCBtb3ZlcyBpbjBqdXN0IHN1Y2ggYSBkaXJlY
3Rpb24gYW5kIGF0IHN1Y2ggYSBzcGVlZC4uLkl0IGZlZWxzIGFuIGltcHVsc2lvbi4uLnRoaXMgaXMgdGhlIH
BsYWNIHRvIGdviG5vdy4gQnV0IHRobzSBza3kga25vd3MgdGhlIHJlYXNvbnMgYW5kIHRobzSBwYXR0ZXJl
cyBiZWVhpbmQgYWxslGNsb3VkcycwYmV5kiHlvdSB3aWxslGtub3csiHRvbywgd2h1biB5b3UgbGlmdCB5b3
Vyc2VsZiBoaWd0IGVub3VnaCB0byBzZWUgYmV5b25kIGhvcml6b25zLiINCg0KLVJpY2h1cmQgQmFjaA=
=
```

NOTE

If user data was not injected during ECS creation, the query result is 404.

Figure 3-39 404 Not Found

```
[root@pythonsdktempest--server-1519783681 ~]# curl http://169.254.169.254/openstack/latest/user_data
<html>
  <head>
    <title>404 Not Found</title>
  </head>
  <body>
    <h1>404 Not Found</h1>
    The resource could not be found.<br /><br />
  </body>
</html>
```

Network Data (OpenStack Metadata API)

Displays ECS network information.

- URI
/openstack/latest/network_data.json
- Usage method
Supports GET requests.

- Example

Linux:

```
curl http://169.254.169.254/openstack/latest/network_data.json
```

Windows:

```
Invoke-RestMethod http://169.254.169.254/openstack/latest/network_data.json | ConvertTo-Json
```

```
{
  "services": [
    {
      "type": "dns",
      "address": "xxx.xx.x.x"
    },
    {
      "type": "dns",
      "address": "100.1
25.21.250"
    }
  ],
  "networks": [
    {
      "network_id": "67dc10ce-441f-4592-9a80-cc709f6436e7",
      "type": "i
pv4_dhcp",
      "link": "tap68a9272d-71",
      "id": "network0"
    },
    {
      "links": [
        {
          "type": "cascading",
          "v
f_id": "68a9272d-7152-4ae7-a138-3ef53af669e7",
          "ethernet_mac_address": "fa:16:3e:f7:c1:47",
          "id": "tap68a9272d-71",
          "mtu": null
        }
      ]
    }
  ]
}
```

Security Key (OpenStack Metadata API)

Obtains temporary AKs and SKs.

- Usage method
Supports GET requests.
- Example
Linux:
curl http://169.254.169.254/latest/meta-data/hostname
Windows:
Invoke-RestMethod http://169.254.169.254/latest/meta-data/hostname
vm-test.novalocal

Instance Type (EC2 Compatible API)

Displays an ECS flavor.

- URI
/169.254.169.254/latest/meta-data/instance-type
- Usage method
Supports GET requests.
- Example
Linux:
curl http://169.254.169.254/latest/meta-data/instance-type
Windows:
Invoke-RestMethod http://169.254.169.254/latest/meta-data/instance-type
s3.medium.1

Local IPv4 (EC2 Compatible API)

Displays the fixed IP address of an ECS. If there are multiple NICs, only the IP address of the primary NIC is displayed.

- URI
/169.254.169.254/latest/meta-data/local-ipv4
- Usage method
Supports GET requests.
- Example
Linux:
curl http://169.254.169.254/latest/meta-data/local-ipv4
Windows:
Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
192.1.1.2

Availability Zone (EC2 Compatible API)

Displays the AZ accommodating an ECS.

- URI
/169.254.169.254/latest/meta-data/placement/availability-zone

- Usage method
Supports GET requests.
- Example
Linux:
curl http://169.254.169.254/latest/meta-data/placement/availability-zone
Windows:
Invoke-RestMethod http://169.254.169.254/latest/meta-data/placement/availability-zone
az1.dc1

Public IPv4 (EC2 Compatible API)

Displays the EIP bound to an ECS. If there are multiple NICs, only the EIP of the primary NIC is displayed.

- URI
/169.254.169.254/latest/meta-data/public-ipv4
- Usage method
Supports GET requests.
- Example
Linux:
curl http://169.254.169.254/latest/meta-data/public-ipv4
Windows:
Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
46.1.1.2

Public Keys (EC2 Compatible API)

Displays the public key of an ECS.

- URI
/169.254.169.254/latest/meta-data/public-keys/0/openssh-key
- Usage method
Supports GET requests.
- Example
Linux:
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
Windows:
Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQADIA5Fw5k8Fgzajn1zJwLoV3+wMP+6CyvsSilc/hioggSnYu/AD0Yqm8vVO0kWlun1rFbdO+QUZKyVr/OPUjQSw4SRh4qsTKf/+eFoWTjplFvd1WCBZzS/WRenxlwR00KkczHSJro763+wYcwKieb4eKRxaQoQvoFgVjLBULXAJH4eKoKTVNtMXAvPP9aMy2SLgsJNtMb9ArfziAiblQynq7UIflnN3VclzPeiWrqtzjyOp6CPUXnL0lVPTvbLe8sUteBsJZwLL6K4i+Y0lf3ryqnmQgC21yW4Dzu+kwk8FVT2MgWkCwiZd8gQ/+uJzrJFyMFUOBikIOBfuUENIJUhAB
Generated-by-Nova

3.7.2 Injecting User Data into ECSs

Scenarios

Use the user data injection function to inject user data into ECSs to:

- Simplify ECS configuration.
- Initialize the ECS OS configuration.
- Upload your scripts to ECSs during ECS creation.
- Perform other tasks using scripts.

Use Restrictions

- Linux
 - The image that is used to create ECSs must have Cloud-Init installed.
 - The user data to be injected must be less than or equal to 32 KB.
 - If user data is uploaded as text, the data can contain only ASCII characters. If user data is uploaded using a file, the file can contain any characters and the file size cannot exceed 32 KB.
 - The image that is used to create ECSs must be a public image, a private image created based on a public image, or a private image with Cloud-Init installed.
 - The format of the customized scripts must be supported by Linux ECSs.
 - DHCP must be enabled on the VPC network, and port 80 must be enabled for the security group in the outbound direction.
 - When the password login mode is selected, user data injection is not supported.
- Windows
 - The image that is used to create ECSs must have Cloudbase-Init installed.
 - The user data to be injected must be less than or equal to 32 KB.
 - User data uploaded as text can contain only ASCII characters. User data uploaded as a file can contain any characters, and the file size must be less than or equal to 32 KB.
 - The image that is used to create ECSs must be a public image, a private image created based on a public image, or a private image with Cloudbase-Init installed.
 - DHCP must be enabled on the VPC network, and port 80 must be enabled for the security group in the outbound direction.

Injecting User Data

1. Create a user data script, the format of which complies with user data script specifications. For details, see [Helpful Links](#).
2. When creating an ECS, set **Advanced Options** to **Configure now**, and paste the content of the user data script to the **User Data Injection** text box or upload the user data file.

 NOTE

User data can be injected as either text or a file.

Text: Copy the content of the user data script to the text box.

File: Save the user data script to a text file and then upload the file.

- The created ECS automatically runs Cloud-Init/Cloudbase-Init and reads the user data script upon startup.

User Data Scripts of Linux ECSs

Customized user data scripts of Linux ECSs are based on the open-source Cloud-Init architecture. This architecture uses ECS metadata as the data source for automatically configuring the ECSs. The customized script types are compatible with open-source Cloud-Init. For details about Cloud-Init, see <http://cloudinit.readthedocs.io/en/latest/topics/format.html>.

- Script execution time: A customized user data script is executed after the time when the status of the target ECS changes to **Running** and before the time when `/etc/init` is executed.

 NOTE

By default, the scripts are executed as user **root**.

- Script type: Both user-data scripts and Cloud-Config data scripts are supported.

Table 3-7 Linux ECS script types

-	User-Data Script	Cloud-Config Data Script
Description	Scripts, such as Shell and Python scripts, are used for custom configurations.	Methods pre-defined in Cloud-Init, such as the Yum source and SSH key, are used for configuring certain ECS applications.
Format	A script must be started with #! , for example, #!/bin/bash and #!/usr/bin/env python . When a script is started for the first time, it will be executed at the <code>rc.local</code> -like level, indicating a low priority in the boot sequence.	The first line must be #cloud-config , and no space is allowed in front of it.
Constraint	Before Base64 encoding, the size of the script, including the first line, cannot exceed 32 KB.	Before Base64 encoding, the size of the script, including the first line, cannot exceed 32 KB.
Frequency	The script is executed only once when the ECS is started for the first time.	The execution frequency varies according to the applications configured on the ECS.

- How can I view the customized user data injected into a Linux ECS?
 - a. Log in to the ECS.
 - b. Run the following command to view the customized user data as user **root**:
curl http://169.254.169.254/openstack/latest/user_data
- Script usage examples
This section describes how to inject scripts in different formats into Linux ECSs and view script execution results.

Example 1: Inject a user-data script.

When creating an ECS, set **User Data Injection** to **As text** and enter the customized user data script.

```
#!/bin/bash
echo "Hello, the time is now $(date -R)" | tee /root/output.txt
```

After the ECS is created, start it and run the **cat [file]** command to check the script execution result.

```
[root@XXXXXXXX ~]# cat /root/output.txt
Hello, the time is now Mon, 16 Jul 2016 16:03:18+0800
```

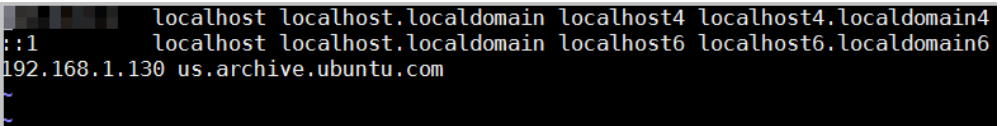
Example 2: Inject a Cloud-Config data script.

When creating an ECS, set **User Data Injection** to **As text** and enter the customized user data script.

```
#cloud-config
bootcmd:
- echo 192.168.1.130 us.archive.ubuntu.com >> /etc/hosts
```

After the ECS is created, start it and run the **cat /etc/hosts** command to check the script execution result.

Figure 3-40 Viewing operating results



```
localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.1.130 us.archive.ubuntu.com
```

User Data Scripts of Windows ECSs

Customized user data scripts of Windows ECSs are based on the open-source Cloudbase-Init architecture. This architecture uses ECS metadata as the data source for initializing and automatically configuring the ECSs. The customized script types are compatible with open-source Cloudbase-Init. For details about Cloudbase-Init, see <https://cloudbase-init.readthedocs.io/en/latest/userdata.html>.

- Script type: Both batch-processing program scripts and PowerShell scripts are supported.

Table 3-8 Windows ECS script types

-	Batch-Processing Program Script	PowerShell Script
Format	The script must be started with rem cmd , which is the first line of the script. No space is allowed at the beginning of the first line.	The script must be started with #ps1 , which is the first line of the script. No space is allowed at the beginning of the first line.
Constraint	Before Base64 encoding, the size of the script, including the first line, cannot exceed 32 KB.	Before Base64 encoding, the size of the script, including the first line, cannot exceed 32 KB.

- How can I view the customized user data injected into a Windows ECS?
 - a. Log in to the ECS.
 - b. Access the following URL in the address box of the browser and view the injected user data:

http://169.254.169.254/openstack/latest/user_data

- Script usage examples

This section describes how to inject scripts in different formats into Windows ECSs and view script execution results.

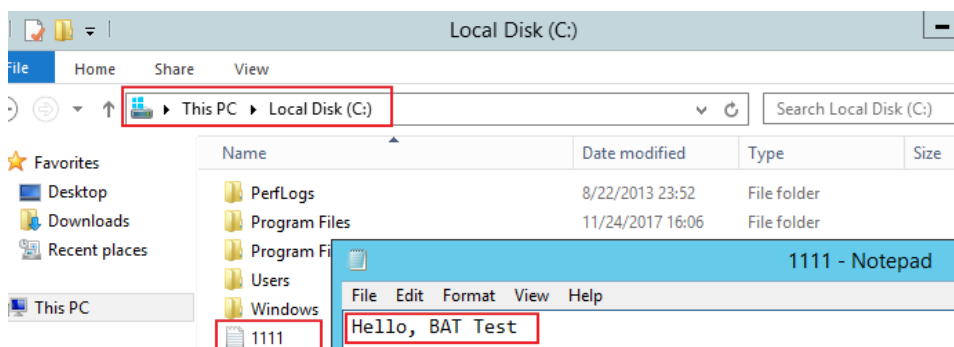
Example 1: Inject a batch-processing program script.

When creating an ECS, set **User Data Injection** to **As text** and enter the customized user data script.

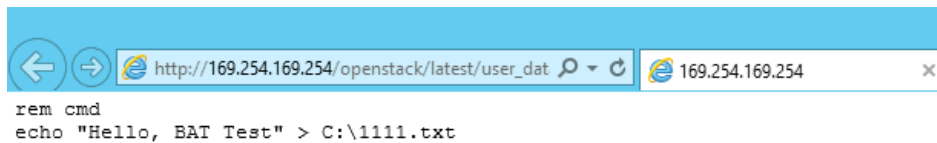
```
rem cmd
echo "Hello, BAT Test" > C:\1111.txt
```

After the ECS is created, start it and check the script execution result. In this example, a text file named **1111** is added to disk C:\.

Figure 3-41 Creating text file (Batch)



To view the user data injected into the Windows ECS, log in at http://169.254.169.254/openstack/latest/user_data.

Figure 3-42 Viewing user data (Batch)

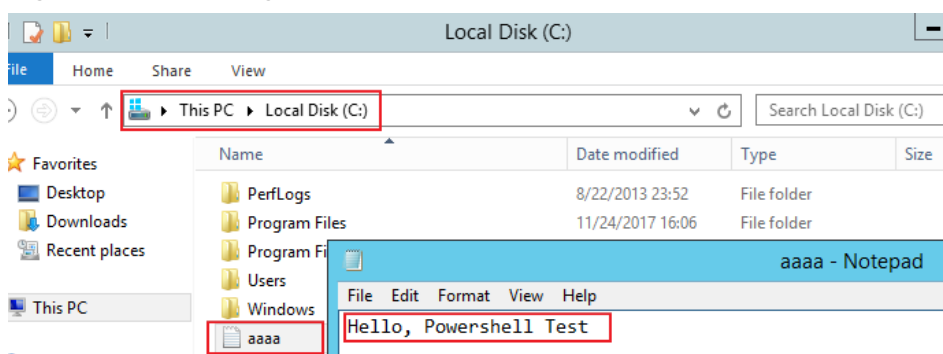
```
rem cmd
echo "Hello, BAT Test" > C:\\1111.txt
```

Example 2: Inject a PowerShell script.

When creating an ECS, set **User Data Injection** to **As text** and enter the customized user data script.

```
#ps1
echo "Hello, Powershell Test" > C:\\aaaa.txt
```

After the ECS is created, start it and check the script execution result. In this example, a text file named **aaaa** is added to disk C:\.

Figure 3-43 Creating text file (PowerShell)

To view the user data injected into the Windows ECS, log in at http://169.254.169.254/openstack/latest/user_data.

Figure 3-44 Viewing user data (PowerShell)

```
#ps1
echo "Hello, Powershell Test" > C:\\aaaa.txt
```

Case 1

This case illustrates how to use the user data injection function to simplify Linux ECS configuration.

In this example, vim is configured to enable syntax highlighting, display line numbers, and set the tab stop to 4. The `.vimrc` configuration file is created and injected into the `/root/.vimrc` directory during ECS creation. After the ECS is created, vim is automatically configured based on your requirements. This improves ECS configuration efficiency, especially in batch ECS creation scenarios.

The content of the script file to be injected is as follows:

```
#cloud-config
write_files:
  - path: /root/.vimrc
```

```
content: |
syntax on
set tabstop=4
set number
```

Case 2

This case illustrates how to use the user data injection function to set the password for logging in to a Linux ECS.

NOTE

The new password must meet the password complexity requirements listed in [Table 3-9](#).

Table 3-9 Password complexity requirements

Parameter	Requirement	Example Value
Password	<ul style="list-style-type: none"> • Consists of 8 characters to 26 characters. • Contains at least three of the following character types: <ul style="list-style-type: none"> - Uppercase letters - Lowercase letters - Digits - Special characters for Windows: \$!@%-_+=[]:./,? - Special characters for Linux: !@%-_+=[]:./^,{}? • Cannot contain the username or the username spelled backwards. • Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.) 	<p>YNbUwp! dUc9MClnv</p> <p>NOTE The example password is generated randomly. Do not copy this example password.</p>

The content of the script file to be injected is as follows:

- Using a ciphertext password (recommended)

```
#!/bin/bash
echo 'root:$6$V6azyeLwcd3CHlpY$BN3VVq18fmCkj66B4zdHLWevqcxlgi' | chpasswd -e;
```

In the preceding command output, **\$6\$V6azyeLwcd3CHlpY\$BN3VVq18fmCkj66B4zdHLWevqcxlgi** is the ciphertext password, which can be generated as follows:

- a. Run the following command to generate an encrypted ciphertext value:

```
python -c "import crypt, getpass, pwd;print crypt.mksalt()"
```

The following information is displayed:

```
$6$V6azyeLwcd3CHlpY
```

- b. Run the following command to generate a ciphertext password based on the salt value:


```
python -c "import crypt, getpass, pwd;print crypt.crypt('Cloud.1234','\
$6$V6azyeLwcD3CHlpY$BN3VVq18fmCkj66B4zdHLWevqcxlig"
```

The following information is displayed:

```
$6$V6azyeLwcD3CHlpY$BN3VVq18fmCkj66B4zdHLWevqcxlig
```

After the ECS is created, you can use the password to log in to it.

Case 3

This case illustrates how to use the user data injection function to reset the password for logging in to a Linux ECS.

In this example, the password of user **root** is reset to *********.

NOTE

The new password must meet the password complexity requirements listed in [Table 3-10](#).

Table 3-10 Password complexity requirements

Parameter	Requirement	Example Value
Password	<ul style="list-style-type: none"> • Consists of 8 characters to 26 characters. • Contains at least three of the following character types: <ul style="list-style-type: none"> - Uppercase letters - Lowercase letters - Digits - Special characters for Windows: \$!@%-_+=[]:./,? - Special characters for Linux: !@%-_+=[:./^,}{?} • Cannot contain the username or the username spelled backwards. • Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.) 	YNbUwp! dUc9MClnv NOTE The example password is generated randomly. Do not copy this example password.

The content of the script file to be injected is as follows (Retain the indentation in the following script):

```
#cloud-config
chpasswd:
  list: |
    root:*****
  expire: False
```

After the ECS is created, you can use the reset password to log in to it. To ensure system security, change the password of user **root** after logging in to the ECS for the first time.

Case 4

This case illustrates how to use the user data injection function to create a user on a Windows ECS and configure the password for the user.

In this example, the user's username is **abc**, its password is *********, and the user is added to the **administrators** user group.

NOTE

The new password must meet the password complexity requirements listed in [Table 3-10](#).

The content of the script file to be injected is as follows:

```
rem cmd
net user abc ***** /add
net localgroup administrators abc /add
```

After the ECS is created, you can use the created username and password to log in to it.

Case 5

This case illustrates how to use the user data injection function to update system software packages for a Linux ECS and enable the HTTPd service. After the user data is injected, you can use the HTTPd service.

The content of the script file to be injected is as follows:

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Case 6

This case illustrates how to use the user data injection function to assign user **root** permission for remotely logging in to a Linux ECS. After injecting the file, you can log in to the ECS as user **root** using SSH key pair authentication.

The content of the script file to be injected is as follows:

```
#cloud-config
disable_root: false
runcmd:
- sed -i 's/^PermitRootLogin.*$/PermitRootLogin without-password/' /etc/ssh/sshd_config
- sed -i '/^KexAlgorithms.*$/d' /etc/ssh/sshd_config
- service sshd restart
```

Helpful Links

For more information about user data injection cases, visit the official Cloud-init/Cloudbase-init website:

- <https://cloudinit.readthedocs.io/en/latest/>
- <https://cloudbase-init.readthedocs.io/en/latest/>

3.8 (Optional) Configuring Mapping Between Hostnames and IP Addresses

ECSs in the same VPC can communicate with each other using hostnames. In such a case, you are required to configure the mapping between hostnames and IP addresses. The communication using hostnames is more convenient than that using IP addresses.

Constraints

This method applies only to Linux ECSs.

Procedure

For example, there are two ECSs in a VPC, ecs-01 and ecs-02. Perform the following operations to enable communication using hostnames between ecs-01 and ecs-02:

Step 1 Log in to ecs-01 and ecs-02 and obtain their private IP addresses.

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. On the **Elastic Cloud Server** page, obtain the private IP address in the **IP Address** column.

For example, the obtained private IP addresses are as follows:

ecs-01: 192.168.0.1

ecs-02: 192.168.0.2

Step 2 Obtain the hostnames for the two ECSs.

1. Log in to an ECS.
2. Run the following command to view the ECS hostname:

```
sudo hostname
```

For example, the obtained hostnames are as follows:

ecs-01: hostname01

ecs-02: hostname02

Step 3 Create mapping between the hostnames and IP addresses and add information about other ECSs in the same VPC.

1. Log in to ecs-01.
2. Run the following command to switch to user **root**:

```
sudo su -
```
3. Run the following command to edit the hosts configuration file:

```
vi /etc/hosts
```
4. Press **i** to enter editing mode.
5. Add the statement in the following format to set up the mapping:

```
Private IP address hostname
```

For example, add the following statement:

```
192.168.0.1 hostname01
```

```
192.168.0.2 hostname02
```

6. Press **Esc** to exit editing mode.
7. Run the following command to save the configuration and exit:
:wq
8. Log in to ecs-02.
9. Repeat [Step 3.2](#) to [Step 3.7](#).

Step 4 Check whether the ECSs can communicate with each other using hostnames.

Log in to an ECS in the same VPC, run the following command to ping the added host, and check whether the operation is successful:

```
ping Hostname
```

```
----End
```

4 Images

4.1 Overview

Image

An image is an ECS or BMS template that contains an OS or service data and may also contain proprietary software and application software, such as database software. Images can be public, private, or shared.

Image Management Service (IMS) allows you to easily create and manage images. You can create an ECS using a public image, private image, or shared image. You can also use an existing ECS or external image file to create a private image.

Public Image

A standard, widely used image. A public image contains an OS, such as Windows, Ubuntu, CentOS, or Debian, and preinstalled public applications. This image will be available to all users. Select your desired public image. Alternatively, create a private image based on a public image to copy an existing ECS or rapidly create ECSs in a batch. You can customize a public image by configuring the application environment and software.

Private Image

A private image contains an OS or service data, preinstalled public applications, and private applications. It is available only to the user who created it.

Table 4-1 Private image types

Image Type	Description
System disk image	Contains an OS and application software for running services. You can use a system disk image to create ECSs and migrate your services to the cloud.

Image Type	Description
Data disk image	Contains only service data. You can use a data disk image to create EVS disks and migrate your service data to the cloud.
Full-ECS image	Contains an OS, application software, and data for running services. A full-ECS image contains the system disk and all data disks attached to it.

If you plan to use a private image to change the OS, ensure that the private image is available. For instructions about how to create a private image, see *Image Management Service User Guide*.

- If the image of a specified ECS is required, make sure that a private image has been created using this ECS.
- If a local image file is required, make sure that the image file has been imported to the cloud platform and registered as a private image.
- If a private image from another region is required, make sure that the image has been copied.
- If a private image from another user account is required, make sure that the image has been shared with you.

Shared Image

A shared image is a private image shared by another user and can be used as your own private image.

- Only the private images that have not been published in Marketplace can be shared.
- Images can be shared within a region only.
- Each image can be shared to a maximum of 128 tenants.
- You can stop sharing images anytime without notifying the recipient.
- You can delete shared image anytime without notifying the recipient.
- Encrypted images cannot be shared.
- Only the full-ECS images created using CBR can be shared.

4.2 Creating an Image

Scenarios


You can use an existing ECS to create a system disk image, data disk image, and full-ECS image.

- System disk image: contains an OS and application software for running services. You can use a system disk image to create ECSs and migrate your services to the cloud.

- **Data disk image:** contains only service data. You can create a data disk image from an ECS data disk. You can also use a data disk image to create EVS disks and migrate your service data to the cloud.
- **Full-ECS image:** contains the data of an ECS, including the data on the data disks attached to the ECS. A full-ECS image can be used to rapidly create ECSs with service data.

If you plan to use a private image to change the OS, ensure that the private image is available. For instructions about how to create a private image, see *Image Management Service User Guide*.

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. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Manage Image/Disk > Create Image**.
5. Configure image information as prompted.
 - **Source:** ECS
 - **ECS:** Retain default settings.
 - **Name:** Customize your image name.
6. Click **Create Now**.

5 EVS Disks

5.1 Adding a Disk to an ECS

Scenarios

The disks attached to an ECS are classified as system disk and data disk. The system disk of an ECS is automatically created and attached when the ECS is created. You do not need to add it separately.

If you add a data disk when creating an ECS, the system automatically attaches the data disk to the ECS. You can also separately add data disks after creating an ECS, and the disks will be automatically attached to the ECS then.

This section describes how to add a data disk.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Manage Image/Disk > Add Disk**.

The page for adding a disk is displayed.

4. Set parameters for the new EVS disk as prompted.
For instructions about how to set EVS disk parameters, see "Create an EVS Disk" in *Elastic Volume Service User Guide*.

NOTE

- By default, the billing mode of the new disk is the same as that of the ECS.
 - By default, the new disk is in the same region as the ECS.
 - By default, the new disk is in the same AZ as the ECS, and the AZ of the disk cannot be changed.
 - After the new disk is created, it is attached to the ECS by default.
5. Click **Create Now**.
The system automatically switches back to the **Disks** tab on the ECS management console. Then, you can view the information of the new disk.

Follow-up Procedure

The system automatically attaches the new disk to the ECS, but the disk can be used only after it is initialized. To do so, log in to the ECS and initialize the disk.

For instructions about how to initialize a data disk, see [2.3.1 Scenarios and Disk Partitions](#).

5.2 Attaching an EVS Disk to an ECS


Scenarios

If the existing disks of an ECS fail to meet service requirements, for example, due to insufficient disk space or poor disk performance, you can attach more available EVS disks to the ECS, or create more disks (**Storage > Elastic Volume Service**) and attach them to the ECS.

Prerequisites

- EVS disks are available.
For instructions about how to create an EVS disk, see "Creating an EVS Disk" in *Elastic Volume Service User Guide*.

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. In the search box above the upper right corner of the ECS list, enter the ECS name, IP address, or ID for search.
5. Click the name of the target ECS.
The page providing details about the ECS is displayed.
6. Click the **Disks** tab. Then, click **Attach Disk**.
The **Attach Disk** dialog box is displayed.
7. Select the target disk and set the device name as prompted.
Device names are as follows:
 - For Xen ECSs, you can specify the device name of a disk, such as **/dev/sdb**.
 - For KVM ECSs, you can specify a disk as a system disk or data disk but cannot specify a device name for the disk.

NOTE

- If no EVS disks are available, click **Create Disk** in the lower part of the list.
 - For details about restrictions on attaching a disk, see [13.8.10 What Are the Restrictions on Attaching an EVS Disk to an ECS?](#)
8. Click **OK**.
After the disk is attached, you can view the information about it on the **Disks** tab.

Follow-up Procedure

If the attached disk is newly created, the disk can be used only after it is initialized.

For instructions about how to initialize a data disk, see [2.3.1 Scenarios and Disk Partitions](#).

5.3 Detaching an EVS Disk from a Running ECS

Scenarios

An EVS disk attached to an ECS can function as a system disk or data disk.

- EVS disks mounted to **/dev/sda** or **/dev/vda** function as system disks. You can only detach system disks offline. Before detaching a system disk from an ECS, you must stop the ECS.
- EVS disks mounted to other locations function as data disks. In addition to offline detachment, data disks can be detached online if the OS running on the ECS supports this feature.

This section describes how to detach a disk from a running ECS.

Constraints

- The EVS disk to be detached must be mounted at a location other than **/dev/sda** or **/dev/vda**.
EVS disks mounted to **/dev/sda** or **/dev/vda** are system disks and cannot be detached from running ECSs.
- Before detaching an EVS disk from a running Windows ECS, make sure that VMTools have been installed on the ECS and that the tools are running properly.
- Before detaching an EVS disk from a running Windows ECS, ensure that no program is reading data from or writing data to the disk. Otherwise, data will be lost.
- SCSI EVS disks cannot be detached from running Windows ECSs.
- Before detaching an EVS disk from a running Linux ECS, you must log in to the ECS and run the **umount** command to cancel the association between the disk and the file system. In addition, ensure that no program is reading data from or writing data to the disk. Otherwise, detaching the disk will fail.

Notes

- On a Windows ECS, if the disk is in non-offline state, the system forcibly detaches the EVS disk. If this occurs, the system may generate a xenvbd alarm. You can ignore this alarm.

 **NOTE**

To view the status of an EVS disk, perform the following operations:

1. 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.

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

The EVS disk list is displayed in the right pane.

3. View the status of each EVS disk.

- Do not detach an EVS disk from an ECS that is being started, stopped, or restarted.
- Do not detach an EVS disk from a running ECS whose OS does not support this feature. OSs supporting EVS disk detachment from a running ECS are listed in [OSs Supporting EVS Disk Detachment from a Running ECS](#).
- For a running Linux ECS, the drive letter may be changed after an EVS disk is detached from it and then attached to it again. This is a normal case due to the drive letter allocation mechanism of the Linux system.
- For a running Linux ECS, the drive letter may be changed after an EVS disk is detached from it and the ECS is restarted. This is a normal case due to the drive letter allocation mechanism of the Linux system.

OSs Supporting EVS Disk Detachment from a Running ECS

OSs supporting EVS disk detachment from a running ECS include two parts:

- For the first part, see "Formats and OSs Supported for External Image Files" in *Image Management Service User Guide*.
- [Table 5-1](#) lists the second part of supported OSs.

Table 5-1 OSs supporting EVS disk detachment from a running ECS

OS	Version
CentOS	7.3 64bit
	7.2 64bit
	6.8 64bit
	6.7 64bit
Debian	8.6.0 64bit
	8.5.0 64bit
Fedora	25 64bit
	24 64bit
SUSE	SUSE Linux Enterprise Server 12 SP2 64bit
	SUSE Linux Enterprise Server 12 SP1 64bit
	SUSE Linux Enterprise Server 11 SP4 64bit

OS	Version
	SUSE Linux Enterprise Server 12 64bit
OpenSUSE	42.2 64bit
	42.1 64bit
Oracle Linux Server release	7.3 64bit
	7.2 64bit
	6.8 64bit
	6.7 64bit
Ubuntu Server	16.04 64bit
	14.04 64bit
	14.04.4 64bit
Windows	Windows Server 2008 R2 Enterprise 64bit
	Windows Server 2012 R2 Standard 64bit
	Windows Server 2016 R2 Standard 64bit
Red Hat Linux Enterprise	7.3 64bit
	6.8 64bit

 **NOTE**

Online detachment is not supported by the ECSs running OSs not listed in the preceding table. For such ECSs, stop the ECSs before detaching disks from them to prevent any possible problems from occurring.

Procedure

1. On the **Elastic Cloud Server** page, click the name of the ECS from which the EVS disk is to be detached. The page providing details about the ECS is displayed.
2. Click the **Disks** tab. Locate the row containing the EVS disk to be detached and click **Detach**.

5.4 Expanding the Capacity of an EVS Disk

Scenarios

When your disk capacity is insufficient, you can handle the insufficiency by expanding the disk capacity.

Procedure

The capacity of an EVS disk can be expanded in either of the following ways:

- Apply for an EVS disk and attach it to an ECS.
- Expand the capacity of an existing EVS disk. The capacities of both system disks and data disks can be expanded.

For more details, see **Expanding the Capacity of an EVS Disk** in *Elastic Volume Service User Guide*.

NOTE

After the capacity is expanded through the management console, only the storage capacity of the EVS disk is expanded. To use the expanded capacity, you also need to log in to the ECS and expand the partition and file system.

5.5 Expanding the Local Disks of a Disk-intensive ECS

Scenarios

Disk-intensive ECSs can use both local disks and EVS disks to store data. Local disks are generally used to store service data and feature higher throughput than EVS disks.

Disk-intensive ECSs do not support modifying specifications. Therefore, when the idle capacity of the local disks of such an ECS is insufficient, you must create a new disk-intensive ECS with higher specifications for capacity expansion. In such a case, the data stored in the original ECS can be migrated to the new ECS through an EVS disk.

Procedure

1. Create an EVS disk according to the volume of data to be migrated.
2. Attach the EVS disk to the disk-intensive ECS.
3. Back up the data stored in the local disks to the EVS disk that is newly attached to the disk-intensive ECS.
4. Detach the EVS disk from the ECS.
 - a. On the **Elastic Cloud Server** page, select this disk-intensive ECS and ensure that it is **Stopped**.
If the ECS is in the **Running** state, choose **More > Stop** to stop it.
 - b. Click the name of the disk-intensive ECS. The page providing details about the ECS is displayed.
 - c. Click the **Disks** tab. Locate the row containing the EVS data disk and click **Detach** to detach the disk from the ECS.
5. Ensure that a new disk-intensive ECS with higher specifications than the original one is available.
The idle local disk capacity of the new ECS must meet service requirements.
6. Attach the EVS disk to the new disk-intensive ECS.
On the **Elastic Cloud Server** page, click the name of the ECS described in step [5](#). The page providing details about the ECS is displayed.

7. Click the **Disks** tab. Then, click **Attach Disk**.
In the displayed dialog box, select the EVS disk detached in step 4 and the device name.
8. Migrate the data from the EVS disk to the local disks of the new disk-intensive ECS.


5.6 Enabling Advanced Disk

Scenarios

- Disk functions have been upgraded on the platform. Newly created ECSs can be attached with up to 60 disks. However, an existing ECS can still be attached with a maximum of 24 disks (40 for certain ECSs). To allow such ECSs to be attached with up to 60 disks, enable advanced disk.
- After advanced disk is enabled, you can view the mapping between device names and disks. For details, see [13.8.12 What Is the Mapping Between Device Names and Disks?](#)

This section describes how to enable advanced disk on an ECS.

Procedure

1. Log in to management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Elastic Cloud Server**.
4. Click the name of the target ECS. The page providing details about the ECS is displayed.
5. Click the **Disks** tab.
6. View the current number of disks that can be attached to the ECS and enable advanced disk as prompted.
The **Enable Advanced Disk** dialog box is displayed.
7. Click **OK**.
8. Stop and then start the target ECS.
This operation allows advanced disk to take effect.
9. Switch to the page providing details about the ECS again, click the **Disks** tab, and check whether the number of disks that can be attached to the ECS has been changed.
 - If yes, advanced disk has been enabled.
 - If no, enabling advanced disk failed. In such a case, try again later or contact customer service.

6 Passwords and Key Pairs

6.1 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.

Prerequisites

The ECS can be logged in.

Background

[Table 6-1](#) shows the ECS password complexity requirements.

Table 6-1 Password complexity requirements

Parameter	Requirement	Example Value
Password	<ul style="list-style-type: none"> • Consists of 8 characters to 26 characters. • Contains at least three of the following character types: <ul style="list-style-type: none"> - Uppercase letters - Lowercase letters - Digits - Special characters for Windows: \$!@%-_+=+[:./,? - Special characters for Linux: !@%-_+=+[:./^,}? • Cannot contain the username or the username spelled backwards. • Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.) 	YNbUwp! dUc9MClNv NOTE The example password is generated randomly. Do not copy this example password.

Windows

1. Log in to the ECS.
For details, see [3.3.1 Login Overview](#).
2. Press **Win+R** to start the **Run** 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 6-1](#)):
net user Administrator New password

Linux

1. Use the existing key file to log in to the ECS as user **root** through SSH.
For details, see [3.4.3 Login Using an SSH Key](#).
2. Run the following command to reset the password of user **root**:
passwd
To reset the password of another user, replace **passwd** with **passwd username**.
3. Enter the new password as prompted. Ensure that the new password meets the requirements described in [Table 6-1](#).
New password:
Retype new password:

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

6.2 Resetting a Login Password

6.2.1 Resetting the Password for Logging In to a Windows ECS

Scenarios

You can reset your ECS password if:

- The password is forgotten.
- The password has expired.

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:

```
sudo apt-get install ntfs-3g chntpw
```


Method 2:

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

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 a case, rectify the file system inconsistency.

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


Back up the disk data, run the following command to rectify the NTFS file system inconsistency, and attach the system disk:
ntfsfix /dev/*Result obtained in step 2.a*
For example, if the result obtained in step 2.a is **xvde2**, run the following command:
ntfsfix /dev/xvde2
3. Change the password and clear the original password.
 - a. Run the following command to back up the SAM file:
cp /mnt/Windows/System32/config/SAM /mnt/Windows/System32/config/SAM.bak
 - b. Run the following command to change the password of a specified user:
chntpw -u Administrator /mnt/Windows/System32/config/SAM
 - c. Enter **1**, **q**, and **y** as prompted, and press **Enter**
The password has been reset if the following information is displayed:

```
Select: [q] > 1
Password cleared!
Select: [q] > q
Hives that have changed:
#Name
0<SAM>
Write hive files? (y/n) [n] : y
0<SAM> - OK
```
4. Stop the temporary ECS, detach the system disk, and attach the system disk to the original Windows ECS.

- a. Stop the temporary ECS, switch to the page providing details about the ECS, and click the **Disks** tab.
 - b. Click **Detach** to detach the data disk temporarily attached in step **1.g**.
 - c. On the page providing details about the original Windows 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**.
5. Start the original Windows ECS and set a new login password.
- a. Click **Start** to start the original Windows ECS. After the status becomes **Running**, click **Remote Login** in the **Operation** column.
 - b. Click **Start**. Enter **CMD** in the search box and press **Enter**.
 - c. Run the following command to change the password (the new password must meet the requirements described in **Table 6-2**):
net user Administrator New password

Table 6-2 Password complexity requirements

Parameter	Requirement	Example Value
Password	<ul style="list-style-type: none"> • Consists of 8 characters to 26 characters. • Contains at least three of the following character types: <ul style="list-style-type: none"> - Uppercase letters - Lowercase letters - Digits - Special characters for Windows: \$!@%_-=+[]:./,? - Special characters for Linux: !@%_-=+[]:./^,{}? • Cannot contain the username or the username spelled backwards. • Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.) 	YNbUwp! dUc9MClnv NOTE The example password is generated randomly. Do not copy this example password.

6.2.2 Resetting the Password for Logging In to a Linux ECS

Scenarios

Keep your password secure. Reset the password if:

- The password is forgotten.

- The password has expired.

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

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.

Contact customer service to obtain the password reset script. Use a connection tool, such as WinSCP, to upload the obtained **changepasswd.sh** script to the temporary ECS.

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

2. Stop the original Linux ECS, detach the system disk, 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.

NOTICE

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

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

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

4. For a non-**root** user, perform the following operations to enable the login permission of user **root**:
vi /etc/ssh/sshd_config
Modify the following parameters:
 - Change **PasswordAuthentication no** to **PasswordAuthentication yes**.
Alternatively, delete the comment tag (#) before **PasswordAuthentication yes**.
 - Change **PermitRootLogin no** to **PermitRootLogin yes**.
Alternatively, delete the comment tag (#) before **PermitRootLogin yes**.
 - Change the **AllowUsers** value to **AllowUsers root**.
Search for **AllowUsers** in the file. If **AllowUsers** is unavailable, add it at the end of the file.
5. Stop the temporary 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 5.b and device name **/dev/sda**.
 - e. Restart the original Linux ECS.

6.3 Creating a Key Pair

Overview

To ensure system security, you are recommended to use key pair authentication to authorize the user who attempts to log in to an ECS. Therefore, you must use an existing key pair or create a new one for remote login authentication.

- Creating a key pair
If no key pair is available, create one, in which the private key is used for login authentication. You can use either of the following methods to create a key pair:

- (Recommended) Create a key pair through the management console. After the creation, the public key is automatically stored in the system, and the private key is manually stored in a local directory. For details, see [Creating a Key Pair Through the Management Console](#).
- Create a key pair using **puttygen.exe**. After the creation, both the public key and private key are stored locally. For details, see [Creating a Key Pair Using puttygen.exe](#). After the creation, import the key pair by following the instructions provided in [Importing a Key Pair](#). Then, the key pair can be used.
- Using an existing key pair
If a key pair is available locally, for example, generated using PuTTYgen, you can import the public key on the management console so that the system maintains the public key file. For details, see [Importing a Key Pair](#).

NOTE


If the public key of the existing key pair is stored by clicking **Save public key** of **puttygen.exe**, the public key cannot be imported to the management console.

If this key pair must be used for remote authentication, see [13.9.5 What Should I Do If a Key Pair Created Using puttygen.exe Cannot Be Imported to the Management Console?](#) for troubleshooting.

Constraints

- ECSs support the following encryption algorithms:
 - SSH-2 (RSA, 1024)
 - SSH-2 (RSA, 2048)
 - SSH-2 (RSA, 4096)
- The private key is one of the most important functions for protecting your ECS during remote login. To ensure ECS security, you are limited to downloading the private key only once.

Creating a Key Pair Through the Management Console

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. In the navigation pane on the left, choose **Key Pair**.
5. On the right side of the page, click **Create Key Pair**.
6. Enter the key name and click **OK**.

An automatically allocated key name consists of **KeyPair-** and a 4-digit random number. Change it to an easy-to-remember one, for example, **KeyPair-xxxx_ecs**.

7. Manually or automatically download the private key file. The file name is the specified key pair name with a suffix of **.pem**. Securely store the private key file. In the displayed dialog box, click **OK**.

NOTICE

This is the only opportunity for you to save the private key file. Keep it secure. When creating an ECS, provide the name of your desired key pair. Each time you log in to the ECS using SSH, provide the private key.

Creating a Key Pair Using puttygen.exe

Step 1 Download and install PuTTY and PuTTYgen.

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

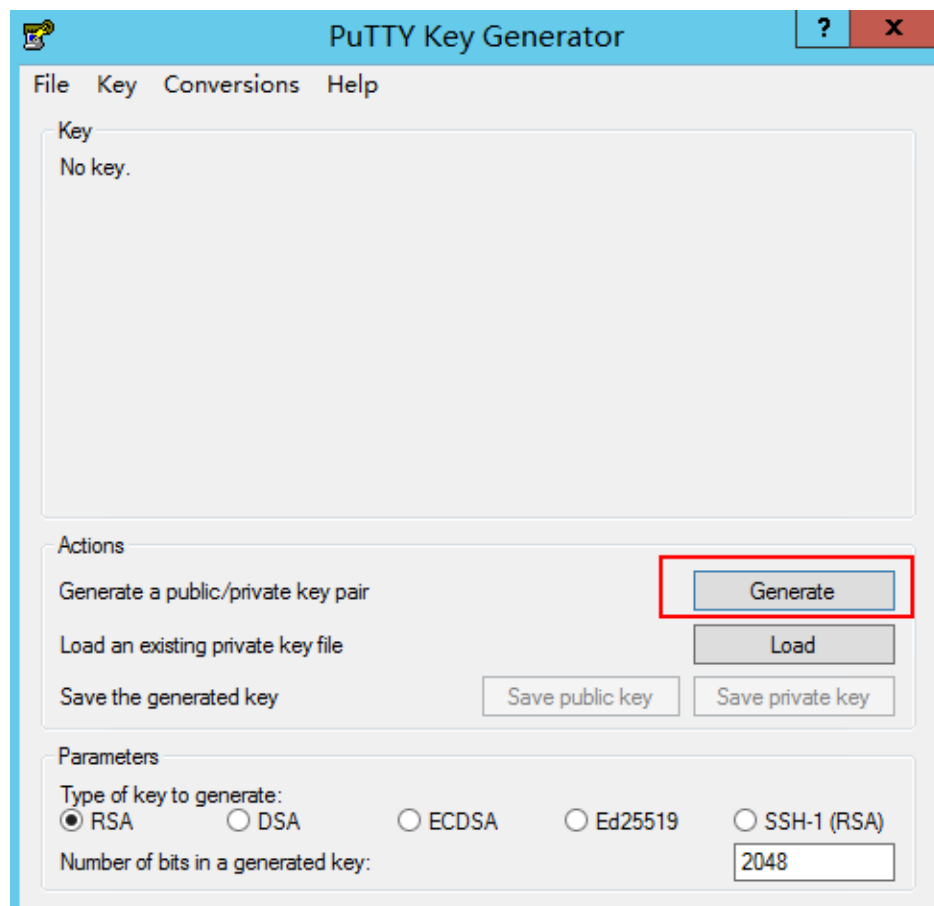
NOTE

PuTTYgen is a key generator, which is used to create a key pair that consists of a public key and a private key for PuTTY.

Step 2 Obtain the public and private keys.

1. Double-click **puttygen.exe** to switch to the **PuTTY Key Generator** page.

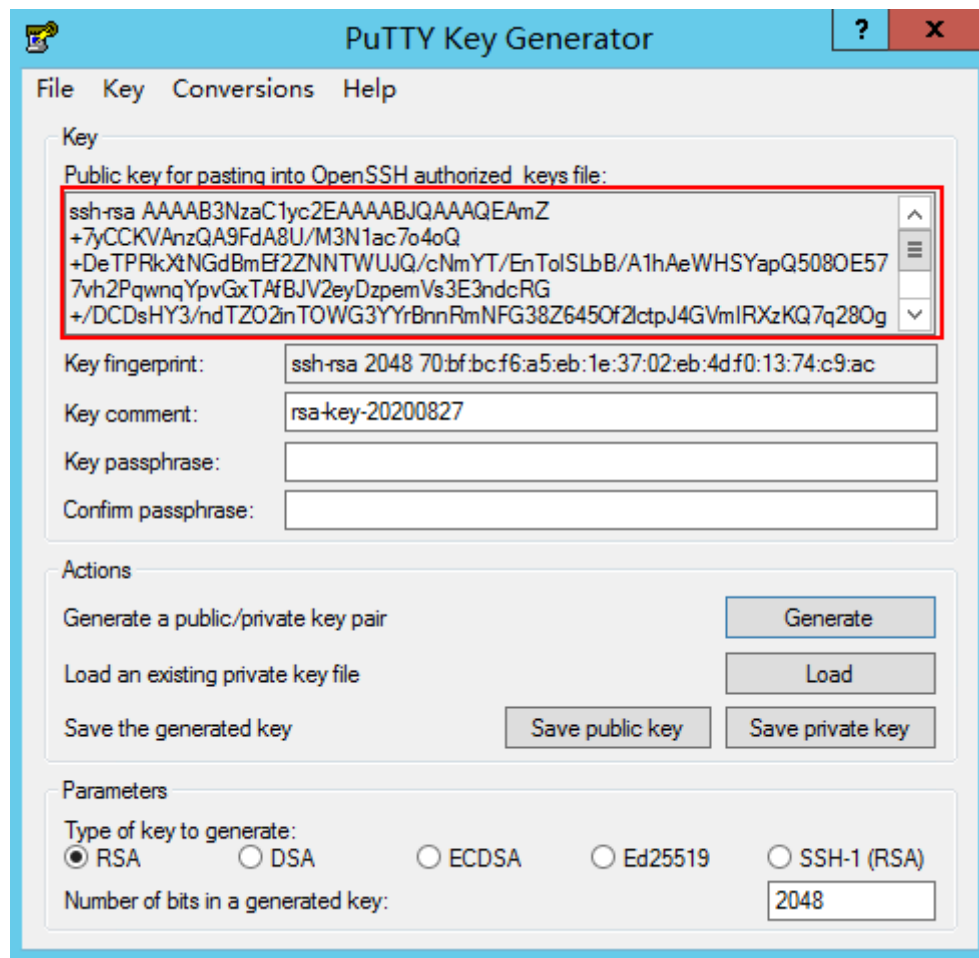
Figure 6-1 PuTTY Key Generator



2. Click **Generate**.

The key generator automatically generates a key pair that consists of a public key and a private key. The public key is shown in the red box in **Figure 6-2**.

Figure 6-2 Obtaining the public and private keys



Step 3 Copy the public key content to a .txt file and save the file in a local directory.

NOTE

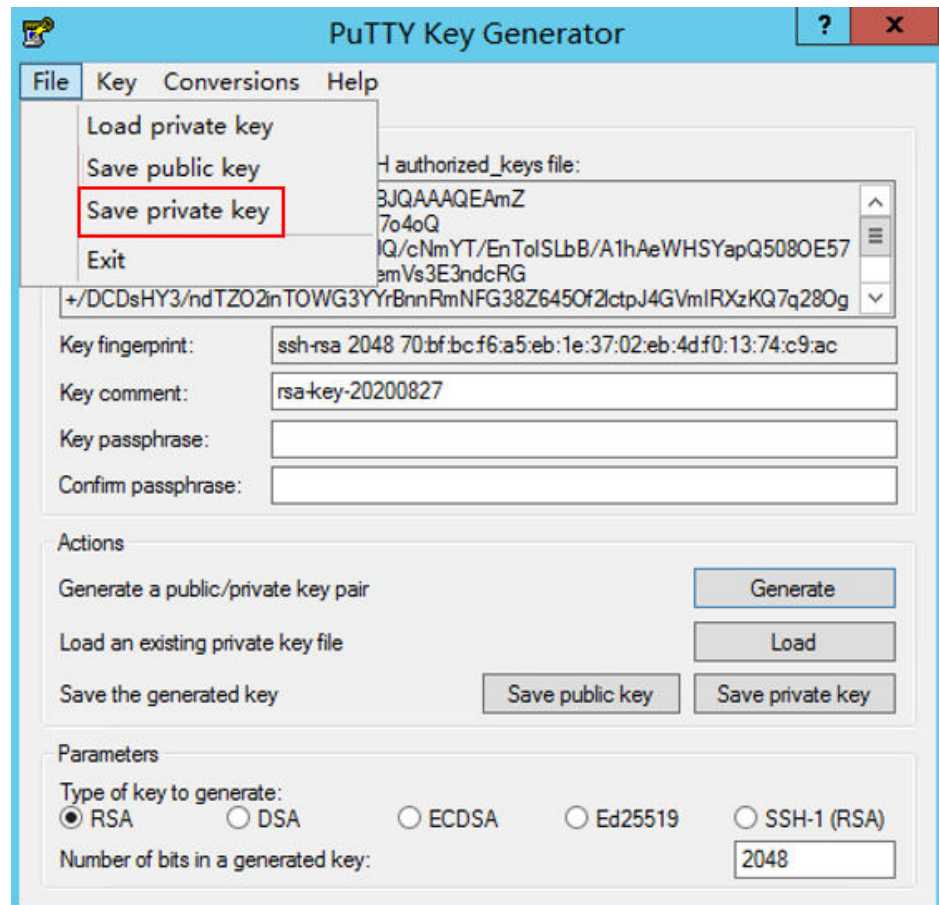
Do not save the public key by clicking **Save public key**. Storing a public key by clicking **Save public key** of **puttygen.exe** will change the format of the public key content. Such a key cannot be imported to the management console.

Step 4 Save the private key.

The format in which to save your private key varies depending on application scenarios:

- Saving the private key in .ppk format
When you are required to log in to a Linux ECS using PuTTY, you must use the .ppk private key. To save the private key in .ppk format, perform the following operations:
 - a. On the **PuTTY Key Generator** page, choose **File > Save private key**.

Figure 6-3 Save private key

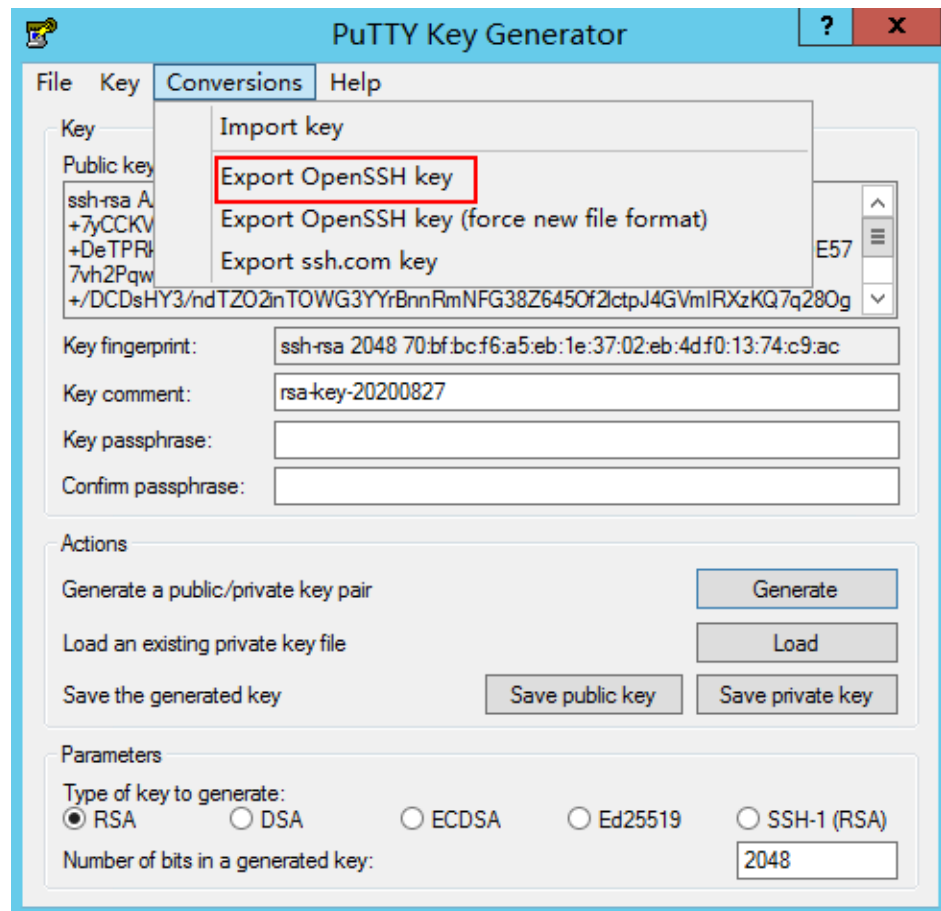


- b. Save the converted private key, for example, **kp-123.ppk**, in a local directory.
- Saving the private key in .pem format
When you are required to log in to a Linux ECS using Xshell or attempt to obtain the password for logging in to a Windows ECS, you must use the .pem private key for authentication. To save the private key in .pem format, perform the following operations:
 - a. Choose **Conversions > Export OpenSSH key**.

NOTICE

If you use this private file to obtain the password for logging in to a Windows ECS, when you choose **Export OpenSSH key**, do not configure **Key passphrase**. Otherwise, obtaining the password will fail.

Figure 6-4 Export OpenSSH key




- b. Save the private key, for example, **kp-123.pem**, in a local directory.

Step 5 Import the public key to the system. For details, see "Copying the public key content" in [Importing a Key Pair](#).

----End

Importing a Key Pair

If you store a public key by clicking **Save public key** of **puttygen.exe**, the format of the public key content will change. Such a key cannot be imported to the management console.

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. In the navigation pane on the left, choose **Key Pair**.
5. On the right side of the page, click **Import Key Pair**.
6. Use either of the following methods to import the key pair:
 - Selecting a file
 - i. On the **Import Key Pair** page of the management console, click **Select File** and select the local public key file, for example, the .txt file saved in [Step 3](#).

 **NOTE**

When importing a key pair, ensure that the public key is imported. Otherwise, the importing will fail.

- ii. Click **OK**.
After the public key is imported, you can change its name.
- Copying the public key content
 - i. Copy the content of the public key in .txt file into the **Public Key Content** text box.
 - ii. Click **OK**.


6.4 Obtaining the Password for Logging In to a Windows ECS

Scenarios

Password authentication is required to log in to a Windows ECS. Therefore, you must use the key file used when you created the ECS to obtain the administrator password generated during ECS creation. The administrator user is **Administrator** or the user configured using Cloudbase-Init. This password is randomly generated, offering high security.

You can obtain the initial password for logging in to a Windows ECS through the management console or APIs. For details, see this section.

Obtaining the Password Through the Management Console

1. Obtain the private key file (.pem file) used when you created the ECS.
2. Log in to the management console.
3. Click  in the upper left corner and select the desired region and project.
4. Under **Computing**, click **Elastic Cloud Server**.
5. On the **Elastic Cloud Server** page, select the target ECS.
6. In the **Operation** column, click **More** and select **Get Password**.
7. Use either of the following methods to obtain the password through the key file:
 - Click **Select File** and upload the key file from a local directory.
 - Copy the key file content to the text field.
8. Click **Get Password** to obtain a random password.

Obtaining the Password Through APIs

1. Obtain the private key file (.pem file) used when you created the ECS.
2. Set up the API calling environment.
3. Call APIs. For details, see "Before You Start" in *Elastic Cloud Server API Reference*.

4. Obtain the ciphertext password.

Call the password obtaining APIs to obtain the ciphertext password of the public key encrypted using RSA. The API URI is in the format "GET /v2/{tenant_id}/servers/{server_id}/os-server-password".

 **NOTE**

For instructions about how to call the APIs, see "Retrieving the Password of a Windows ECS (Native OpenStack API)" in *Elastic Cloud Server API Reference*.

5. Decrypt the ciphertext password.

Use the private key file used when you created the ECS to decrypt the ciphertext password obtained in step 4.

- a. Run the following command to convert the ciphertext password format to ".key -nocrypt" using OpenSSL:
openssl pkcs8 -topk8 -inform PEM -outform DER -in rsa_pem.key -out pkcs8_der.key -nocrypt
- b. Invoke the Java class library **org.bouncycastle.jce.provider.BouncyCastleProvider** and use the key file to edit the code decryption ciphertext.


6.5 Deleting the Initial Password for Logging In to a Windows ECS

Scenarios

After obtaining the initial password, you are advised to delete it to ensure system security.

Deleting the initial password does not affect ECS operation or login. Once deleted, the password cannot be retrieved. Before deleting a password, you are advised to record it.

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. In the **Operation** column, click **More** and select **Delete Password**.
The system displays a message, asking you whether you want to delete the password.
6. Click **OK** to delete the password.


7 NICs

7.1 Adding a NIC

Scenarios

If multiple NICs are required by your ECS, you can add them to your ECS. To add a NIC to the ECS, perform the following operations:

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. Click the name of the target ECS.
The page providing details about the ECS is displayed.
5. Click the **Network Interfaces** tab. Then, click **Add NIC**.
6. Select the subnet and security group to be added.
 - **Security Group:** You can select multiple security groups. In such a case, the access rules of all the selected security groups apply on the ECS.
 - **Private IP Address:** If you want to add a NIC with a specified IP address, enter an IP address into the **Private IP Address** field.
7. Click **OK**.

Follow-up Procedure

Some OSs cannot identify newly added NICs. In this case, you must manually activate the NICs. Ubuntu is used as an example in the following NIC activation procedure. Required operations may vary among systems. For additional information, see the documentation for your OS.

1. Locate the row containing the target ECS and click **Remote Login** in the **Operation** column.
Log in to the ECS.

2. Run the following command to view the NIC name:
ifconfig -a
In this example, the NIC name is **eth2**.
3. Run the following command to switch to the target directory:
cd /etc/network
4. Run the following command to open the **interfaces** file:
vi interfaces
5. Add the following information to the **interfaces** file:
auto eth2
iface eth2 inet dhcp
6. Run the following command to save and exit the **interfaces** file:
:wq
7. Run either the **ifup eth2** command or the **/etc/init.d/networking restart** command to make the newly added NIC take effect.
X in the preceding command indicates the NIC name and SN, for example, **ifup eth2**.
8. Run the following command to check whether the NIC name obtained in step 2 is displayed in the command output:
ifconfig
For example, check whether **eth2** is displayed in the command output.
 - If yes, the newly added NIC has been activated, and no further action is required.
 - If no, the newly added NIC failed to be activated. Go to step 9.
9. Log in to the management console. Locate the row containing the target ECS, click **More** in the **Operation** column, and select **Restart**.
10. Run the following command to check whether the NIC name obtained in step 2 is displayed in the command output:
 - If yes, no further action is required.
 - If no, contact customer service.

7.2 Deleting a NIC

Scenarios

An ECS can have up to 12 NICs, including one primary NIC that cannot be deleted and extension NICs. This section describes how to delete an extension NIC.

Procedure

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 **Network Interfaces** tab. Then, click **Delete** in the row of the target NIC.

 **NOTE**

You are not allowed to delete the primary ECS NIC. By default, the primary ECS NIC is the first NIC displayed in the NIC list.

5. Click **OK** in the displayed dialog box.

 **NOTE**

Certain ECSs do not support NIC deletion when they are running. For details about these ECSs, see the GUI display. To delete a NIC from such an ECS, stop the ECS.

7.3 Changing a VPC

Scenarios

This section describes how to change a VPC.

Constraints

- A VPC can be changed on a single NIC only.
A VPC can be changed only on a running ECS. However, ECS network connections will be interrupted during the change process.
- During the change process, do not perform operations on the ECS, including its EIP.
- After the VPC is changed, the subnet, private IP address, and MAC address of the ECS will change.
- After the VPC is changed, the source/destination check and virtual IP address must be configured again.
- After the VPC is changed, you are required to reconfigure network-related application software and services, such as ELB, VPN, NAT, and DNS.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Change VPC**.

The **Change VPC** page is displayed.

4. Select an available VPC and subnet from the drop-down lists, and set the private IP address and security group as prompted.

You can select multiple security groups. In such a case, the access rules of all the selected security groups apply on the ECS.

 **NOTE**

Using multiple security groups may deteriorate ECS network performance. You are suggested to select no more than five security groups.

5. Click **OK**.

7.4 Modifying a Private IP Address

Scenarios

The cloud platform allows you to modify the private IP address of the primary NIC. For details, see this section. To modify the private IP address of an extension NIC, delete the NIC and attach a new NIC.

Constraints

- The ECS must be stopped.
- If a virtual IP address or DNAT rule has been configured for the NIC, cancel the configuration before modifying the private IP address.
- If the NIC has an IPv6 address, its private IP address (IPv4 or IPv6 address) cannot be modified.
- Before changing the private IP address of an ELB backend server, delete the backend server group.

Procedure

1. Log in to the 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 **Network Interfaces** tab. Locate the row containing the primary NIC and click **Modify Private IP**.
The **Modify Private IP** dialog box is displayed.
5. Change the subnet and private IP address of the primary NIC as required.

NOTE

Subnets can be changed only within the same VPC.

If the target private IP address is not specified, the system will automatically assign one to the primary NIC.

7.5 Managing Virtual IP Addresses

Scenarios

A virtual IP address provides the second IP address for one or more ECS NICs, improving high availability between the ECSs.

Procedure

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 **Network Interfaces** tab. Then, click **Manage Virtual IP Address**.
5. On the **IP Addresses** tab of the page that is displayed, locate the row containing the target virtual IP address and select **Bind to EIP** or **Bind to Instance** in the **Operation** column.

Multiple ECSs deployed to work in active/standby mode can be bound with a virtual IP address to improve DR performance.

6. Click **OK**.

7.6 Enabling NIC Multi-Queue

Scenarios

Single-core CPU performance cannot meet the requirement of processing NIC interruptions incurred with the increase of network I/O bandwidth. NIC multi-queue enables multiple CPUs to process ECS NIC interruptions, thereby improving network PPS and I/O performance.

The ECS described in this section is assumed to comply with the requirements on specifications and virtualization type.

- If the ECS was created using a public image listed in [Support of NIC Multi-Queue](#), NIC multi-queue has been enabled on the ECS by default. Therefore, you do not need to perform the operations described in this section.
- In the ECS was created using a private image and the external image file is listed in [Support of NIC Multi-Queue](#), perform the following operations to enable NIC multi-queue:
 - a. [Importing the External Image File to the IMS Console](#)
 - b. [Setting NIC Multi-Queue for the Image](#)
 - c. [Creating an ECS Using a Private Image](#)
 - d. [Running the Script for Configuring NIC Multi-Queue](#)

NOTE

After NIC multi-queue is enabled on an ECS, you need to enable this function on the ECS again after you add or delete a NIC or change the VPC for the ECS. For details, see [Running the Script for Configuring NIC Multi-Queue](#).

Support of NIC Multi-Queue

NIC multi-queue can be enabled on an ECS only when the ECS specifications, virtualization type, and image OS meet the requirements described in this section.

- For details about the ECS specifications that support NIC multi-queue, see [1.6 x86 ECS Specifications and Types](#).

NOTE

If the number of NIC queues is greater than 1, NIC multi-queue is supported.

- Only KVM ECSs support NIC multi-queue.
- The Linux public images listed in [Table 7-2](#) support NIC multi-queue.

 **NOTE**

- Windows OSs have not commercially supported NIC multi-queue. If you enable NIC multi-queue in a Windows image, starting an ECS created using such an image may be slow.
- You are advised to upgrade the kernel version of the Linux ECS to 2.6.35 or later. Otherwise, NIC multi-queue is not supported.
Run the **uname -r** command to obtain the kernel version. If the kernel version is earlier than 2.6.35, contact customer service to upgrade the kernel.

Table 7-1 Support of NIC multi-queue for Windows ECSs

Image	Status
Windows Server 2008 WEB R2 64bit	Supported using private images
Windows Server 2008 Enterprise SP2 64bit	Supported using private images
Windows Server 2008 R2 Standard/DataCenter/Enterprise 64bit	Supported using private images
Windows Server 2008 R2 Enterprise 64bit_WithGPUdriver	Supported using private images
Windows Server 2012 R2 Standard 64bit_WithGPUdriver	Supported using private images
Windows Server 2012 R2 Standard/DataCenter 64bit	Supported using private images

Table 7-2 Support of NIC multi-queue for Linux ECSs

Image	Support of NIC Multi-Queue	NIC Multi-Queue Enabled by Default
Ubuntu 14.04/16.04 server 64bit	Yes	Yes
OpenSUSE 42.2 64bit	Yes	Yes
SUSE Enterprise 12 SP1/SP2 64bit	Yes	Yes
CentOS 6.8/6.9/7.0/7.1/7.2/7.3/7.4/7.5/7.6 64bit	Yes	Yes
Debian 8.0.0/8.8.0/8.9.0/9.0.0 64bit	Yes	Yes
Fedora 24/25 64bit	Yes	Yes
EulerOS 2.2 64bit	Yes	Yes

Importing the External Image File to the IMS Console

For details, see "Registering an Image File as a Private Image" in *Image Management Service User Guide*.

Setting NIC Multi-Queue for the Image

Windows OSs have not commercially supported NIC multi-queue. If you enable NIC multi-queue in a Windows image, starting an ECS created using such an image may be slow.

Use one of the following methods to set the NIC multi-queue attribute:

Method 1:

1. Log in to the management console.
2. Under **Computing**, click **Image Management Service**.
3. Click the **Private Images** tab, locate the row containing the target image, click **Modify** in the **Operation** column.
4. Set the NIC multi-queue attribute of the image.

Method 2:

1. Log in to the management console.
2. Under **Computing**, click **Image Management Service**.
3. Click the **Private Images** tab. In the image list, click the name of the target image to switch to the page providing details about the image.
4. Click **Modify** in the upper right corner. In the displayed **Modify Image** dialog box, set the NIC multi-queue attribute.

Method 3: Add `hw_vif_multiqueue_enabled` to an image through the API.

1. For instructions about how to obtain the token, see **Calling APIs > Authentication** in *Image Management Service API Reference*.
2. For instructions about how to call an API to update image information, see "Updating Image Information (Native OpenStack API)" in *Image Management Service API Reference*.
3. Add **X-Auth-Token** to the request header.
The value of **X-Auth-Token** is the token obtained in step 1.
4. Add **Content-Type** to the request header.

The value of **Content-Type** is **application/openstack-images-v2.1-json-patch**.

The request URI is in the following format:

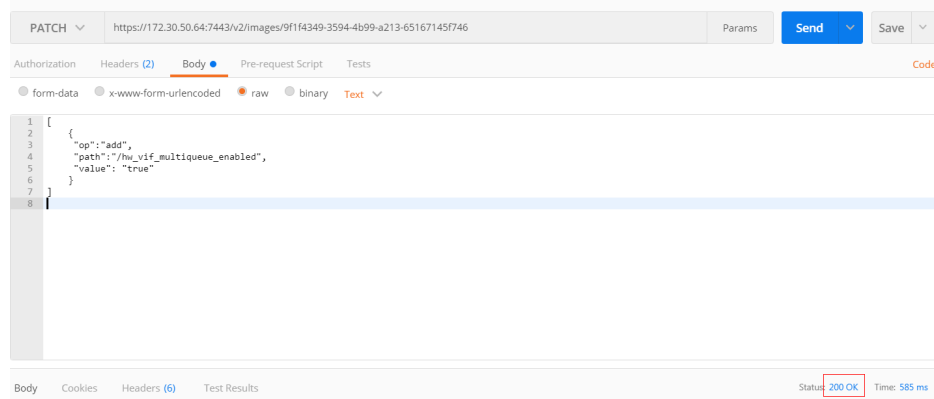
```
PATCH /v2/images/{image_id}
```

The request body is as follows:

```
[
  {
    "op": "add",
    "path": "/hw_vif_multiqueue_enabled",
    "value": "true"
  }
]
```

Figure 7-1 shows an example request body for modifying the NIC multi-queue attribute.

Figure 7-1 Example request body



Creating an ECS Using a Private Image

Create an ECS using a registered private image. For details, see [2.1 Creating an ECS](#). Note the following when setting the parameters:

- **Region:** Select the region where the private image is located.
- **Image:** Select **Private image** and then the desired image from the drop-down list.

Running the Script for Configuring NIC Multi-Queue

Windows OSs have not commercially supported NIC multi-queue. If you enable NIC multi-queue in a Windows image, starting an ECS created using such an image may be slow.

A script for automatically enabling NIC multi-queue on a Linux ECS is available. After the script is configured, the ECS supports NIC multi-queue.

1. Download the configuration script.
2. Run the following command to assign execution permissions to the script:
chmod +x multi-queue-hw
3. Run the following command to move the **multi-queue-hw** script to the **/etc/init.d** directory:
mv multi-queue-hw /etc/init.d
4. Run the following command to run the script:
/etc/init.d/multi-queue-hw start
The script takes effect immediately after being executed. However, after the ECS is stopped, NIC multi-queue automatically becomes invalid.
5. Add startup configuration for each OS so that NIC multi-queue automatically enables upon the ECS startup.
 - For CentOS, Red Hat, Fedora, EulerOS, SUSE, and OpenSUSE, run the following command:
chkconfig multi-queue-hw on
 - For Ubuntu, run the following command:
update-rc.d multi-queue-hw defaults 90 10

- For Debian, run the following command:
systemctl enable multi-queue-hw

8 Security

8.1 Security Groups

8.1.1 Overview

Security Group

A security group is a collection of access control rules for ECSs that have the same security protection requirements and that are mutually trusted. After a security group is created, you can create various access rules for the security group, these rules will apply to all ECSs added to this security group.

You can also customize a security group or use the default one. The system provides a default security group for you, which permits all outbound traffic and denies inbound traffic. ECSs in a security group are accessible to each other. For details about the default security group, see [8.1.2 Default Security Group and Rules](#).

Security Group Rules

After a security group is created, you can add rules to the security group. A rule applies either to inbound traffic (ingress) or outbound traffic (egress). After ECSs are added to the security group, they are protected by the rules of that group.

Each security group has default rules. For details, see [8.1.2 Default Security Group and Rules](#). You can also customize security group rules. For details, see [8.1.4 Configuring Security Group Rules](#).

Security Group Constraints

- By default, you can create up to 100 security groups in your cloud account.
- By default, each security group can have up to 50 security group rules.
- By default, an ECS or an ECS extension NIC can be added to a maximum of five security groups.
- A maximum of 20 instances can be added to a security group at a time.

- A security group can be associated with a maximum of 1000 instances.

8.1.2 Default Security Group and Rules

Your account automatically comes with a default security group. The default security group allows all outbound traffic, denies all inbound traffic, and allows all traffic between ECSs in the group. Your ECSs in this security group can communicate with each other already without adding additional rules.

Figure 8-1 shows the default security group.

Figure 8-1 Default security group

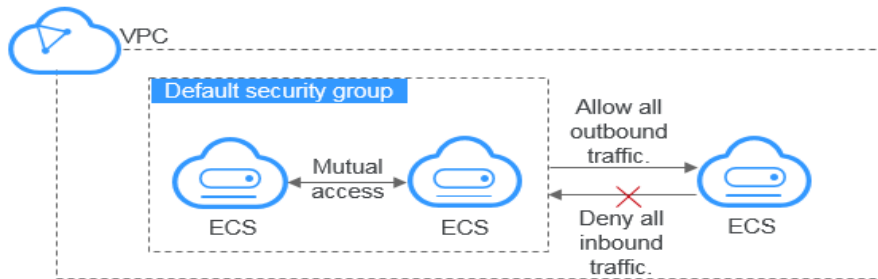


Table 8-1 describes default security group rules.

Table 8-1 Rules in the default security group

Direction	Protocol	Port/Range	Source/Destination	Description
Outbound	All	All	Destination: 0.0.0.0/0	Allows all outbound traffic.
Inbound	All	All	Source: the current security group (for example, sg-xxxxx)	Allows communication among ECSs within the security group and denies all inbound traffic (incoming data packets).
Inbound	TCP	22	Source: 0.0.0.0/0	Allows all IP addresses to access Linux ECSs over SSH.
Inbound	TCP	3389	Source: 0.0.0.0/0	Allows all IP addresses to access Windows ECSs over RDP.

8.1.3 Security Group Configuration Examples

Common security group configuration examples are as follows: The following examples allow all outgoing data packets by default and only describe how to configure the inbound rules of a security group.

- [Enabling ECSs in Different Security Groups to Communicate with Each Other Through an Internal Network](#)
- [Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group](#)
- [Remotely Connecting to Linux ECSs Using SSH](#)
- [Remotely Connecting to Windows ECSs Using RDP](#)
- [Enabling Communication Between ECSs](#)
- [Hosting a Website on ECSs](#)
- [Enabling an ECS to Function as a DNS Server](#)
- [Uploading or Downloading Files Using FTP](#)

Enabling ECSs in Different Security Groups to Communicate with Each Other Through an Internal Network

- Example scenario:
Resources on an ECS in a security group need to be copied to an ECS associated with another security group. The two ECSs are in the same VPC. We recommend that you enable private network communication between the ECSs and then copy the resources.
- Security group configuration:
Within a given VPC, ECSs in the same security group can communicate with one another by default. However, ECSs in different security groups cannot communicate with each other by default. To enable these ECSs to communicate with each other, you need to add certain security group rules. You can add an inbound rule to the security groups containing the ECSs to allow access from ECSs in the other security group. The required rule is as follows.

Direction	Protocol/Application	Port	Source
Inbound	Used for communication through an internal network	Port or port range	ID of another security group

Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group

- Example scenario:
To prevent ECSs from being attacked, you can change the port number for remote login and configure security group rules that allow only specified IP addresses to remotely access the ECSs.

- Security group configuration:
To allow IP address **192.168.20.2** to remotely access Linux ECSs in a security group over the SSH protocol (port 22), you can configure the following security group rule.

Direction	Protocol/ Application	Port	Source
Inbound	SSH (22)	22	IPv4 CIDR block or ID of another security group For example, 192.168.20.2/32

Remotely Connecting to Linux ECSs Using SSH

- Example scenario:
After creating Linux ECSs, you can add a security group rule to enable remote SSH access to the ECSs.

NOTE

The default security group comes with the following rule. If you use the default security group, you do not need to add this rule again.

- Security group rule:

Direction	Protocol/ Application	Port	Source
Inbound	SSH (22)	22	0.0.0.0/0

Remotely Connecting to Windows ECSs Using RDP

- Example scenario:
After creating Windows ECSs, you can add a security group rule to enable remote RDP access to the ECSs.

NOTE

The default security group comes with the following rule. If you use the default security group, you do not need to add this rule again.

- Security group rule:

Direction	Protocol/ Application	Port	Source
Inbound	RDP (3389)	3389	0.0.0.0/0

Enabling Communication Between ECSs

- Example scenario:
After creating ECSs, you need to add a security group rule so that you can run the **ping** command to test communication between the ECSs.

- Security group rule:

Direction	Protocol/ Application	Port	Source
Inbound	ICMP	All	0.0.0.0/0

Hosting a Website on ECSs

- Example scenario:

If you deploy a website on your ECSs and require that your website be accessed over HTTP or HTTPS, you can add rules to the security group used by the ECSs that function as the web servers.

- Security group rule:

Direction	Protocol/ Application	Port	Source
Inbound	HTTP (80)	80	0.0.0.0/0
Inbound	HTTPS (443)	443	0.0.0.0/0

Enabling an ECS to Function as a DNS Server

- Example scenario:

If you need to use an ECS as a DNS server, you must allow TCP and UDP access from port 53 to the DNS server. You can add the following rules to the security group associated with the ECS.

- Security group rules:

Direction	Protocol/ Application	Port	Source
Inbound	TCP	53	0.0.0.0/0
Inbound	UDP	53	0.0.0.0/0

Uploading or Downloading Files Using FTP

- Example scenario:

If you want to use File Transfer Protocol (FTP) to upload files to or download files from ECSs, you need to add a security group rule.

NOTE

You must first install the FTP server program on the ECSs and check whether ports 20 and 21 are working properly.

- Security group rule:

Direction	Protocol/ Application	Port	Source
Inbound	TCP	20-21	0.0.0.0/0

8.1.4 Configuring Security Group Rules

Scenarios

Similar to firewall, a security group is a logical group used to control network access. You can define access rules for a security group to protect the ECSs that are added to this security group.

- Inbound: Inbound rules allow external network traffic to be sent to the ECSs in the security group.
- Outbound: Outbound rules allow network traffic from the ECSs in the security group to be sent out of the security group.

For details about the default security group rules, see *Virtual Private Cloud User Guide*. For details about configuration examples for security group rules, see [8.1.3 Security Group Configuration Examples](#).

Procedure

1. Under **Computing**, click **Elastic Cloud Server**.
2. On the **Elastic Cloud Server** page, click the name of the target ECS.
The page providing details about the ECS is displayed.
3. Click the **Security Groups** tab, expand the information of the security group, and view security group rules.
4. Click the security group ID.
The system automatically switches to the **Security Group** page.
5. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.
You can click + to add more inbound rules.

Table 8-2 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	Protocol: specifies the network protocol. Currently, the value can be All , TCP , UDP , ICMP , GRE , or others.	TCP
	Port: specifies the port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.	22, or 22-30

Parameter	Description	Example Value
Type	Specifies the IP address type. <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
Source	Specifies the source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example: <ul style="list-style-type: none"> • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (IP address range) • 0.0.0.0/0 (all IP addresses) • sg-abc (security group) 	0.0.0.0/0
Description	Provides supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

6. On the **Outbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.
You can click + to add more outbound rules.

Table 8-3 Outbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	Protocol: specifies the network protocol. Currently, the value can be All , TCP , UDP , ICMP , GRE , or others.	TCP
	Port: specifies the port or port range over which the traffic can leave your ECS. The value ranges from 1 to 65535.	22, or 22-30
Type	Specifies the IP address type. <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4

Parameter	Description	Example Value
Destination	Specifies the destination of the security group rule. The value can be a single IP address or a security group to allow access to the IP address or instances in the security group. For example: <ul style="list-style-type: none">• xxx.xxx.xxx.xxx/32 (IPv4 address)• xxx.xxx.xxx.0/24 (IP address range)• 0.0.0.0/0 (all IP addresses)• sg-abc (security group)	0.0.0.0/0
Description	Provides supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

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

8.1.5 Changing a Security Group

Scenarios

To change the security group of an ECS NIC, perform the operations described in this section.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Manage Network > Change Security Group**.

The **Change Security Group** dialog box is displayed.

4. Select the target NIC and security group as prompted.

You can select multiple security groups. In such a case, the access rules of all the selected security groups apply on the ECS. To create a security group, click **Create Security Group**.

NOTE

Using multiple security groups may deteriorate ECS network performance. You are suggested to select no more than five security groups.

5. Click **OK**.


9 EIPs

9.1 Binding an EIP

Scenarios

You can assign an EIP and bind it to an ECS to enable the ECS to access the Internet.

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. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Manage Network > Bind EIP**.
5. Select an EIP and click **OK**.

NOTE

If no EIP is available in the current region, the EIP list is empty. In such a case, allocate an EIP and then bind it.


6. After the EIP is bound, view it on the **Elastic Cloud Server** page.

9.2 Unbinding an EIP

Scenarios

This section describes how to unbind an EIP from an ECS.

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. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Manage Network > Unbind EIP**.
5. Verify the EIP and click **Yes**.

 **NOTE**

Unreleased EIPs will continue to be billed. To stop the EIPs from being billed, release them.


9.3 Changing an EIP

Scenarios


If your ECS has an EIP bound, perform the operations described in this section to change the EIP.

The management console does not allow you to directly change the EIP bound to an ECS. Therefore, to change an EIP, unbind it from the ECS and bind the desired one to the ECS.

Unbinding an EIP

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Manage Network > Unbind EIP**.
4. Confirm the displayed information and click **Yes**.

Binding a New EIP

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Manage Network > Bind EIP**.
4. Select the desired EIP and click **OK**.

 **NOTE**


If no EIP is available in the current region, the EIP list is empty. In such a case, allocate an EIP and then bind it.

9.4 Changing an EIP Bandwidth

Scenarios

If an EIP has been bound to the ECS, the ECS can access the Internet in a specified bandwidth. This section describes how to adjust the bandwidth of an ECS.

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. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Modify Bandwidth**.
5. Change the bandwidth name, billing mode, or bandwidth size as prompted.

9.5 Having an ECS Without a Public IP Address Access the Internet

Scenarios

To ensure platform security and conserve public IP address resources, public IP addresses are assigned only to specified ECSs. ECSs without public IP addresses cannot access the Internet directly. If these ECSs need to access the Internet (for example, to perform a software upgrade or install a patch), you can select an ECS with a public IP address bound to function as a proxy ECS, providing an access channel for these ECS.



NOTE

NAT Gateway is recommended, which provides both the SNAT and DNAT functions for your ECSs in a VPC and allows the ECSs to access or provide services accessible from the Internet.

Prerequisites

- A proxy ECS with a public IP address bound is available.
In this example, the proxy ECS runs CentOS 6.5.
- The IP address of the proxy ECS is in the same network segment and same security group as the ECSs that need to access the Internet.

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. In the search box above the upper right corner of the ECS list, enter the proxy ECS name for search.
5. Click the name of the proxy ECS. The page providing details about the ECS is displayed.
6. Click the **Network Interfaces** tab and then . Then, disable **Source/Destination Check**.
By default, the source/destination check function is enabled. When this function is enabled, the system checks whether source IP addresses contained in the packets sent by ECSs are correct. If the IP addresses are incorrect, the

system does not allow the ECSs to send the packets. This mechanism prevents packet spoofing, thereby improving system security. However, this mechanism prevents the packet sender from receiving returned packets. Therefore, disable the source/destination check.

7. Log in to the proxy ECS.

For more details, see [3.4.1 Login Overview](#).

8. Run the following command to check whether the proxy ECS can access the Internet:

```
ping www.baidu.com
```

The proxy ECS can access the Internet if information similar to the following is displayed:

Figure 9-1 Checking whether the Internet is accessible

```
[root@ecs-f4f0 ~]# ping www.baidu.com
PING www.a.shifen.com (61.135.169.121) 56(84) bytes of data:
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=1 ttl=47 time=2.77 ms
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=2 ttl=47 time=2.65 ms
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=3 ttl=47 time=2.61 ms
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=4 ttl=47 time=2.83 ms
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=5 ttl=47 time=2.69 ms
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=6 ttl=47 time=2.63 ms
```

9. Run the following command to check whether IP forwarding is enabled on the proxy ECS:

```
cat /proc/sys/net/ipv4/ip_forward
```

- If **0** (disabled) is displayed, go to [10](#).
- If **1** (enabled), go to [16](#).

10. Run the following command to open the IP forwarding configuration file in the vi editor:

```
vi /etc/sysctl.conf
```

11. Press **i** to enter editing mode.

12. Set the **net.ipv4.ip_forward** value to **1**.

Set the **net.ipv4.ip_forward** value to **1**.

NOTE

If the **sysctl.conf** file does not contain the **net.ipv4.ip_forward** parameter, run the following command to add it:

```
echo net.ipv4.ip_forward=1 >> /etc/sysctl.conf
```

13. Press **Esc**, type **:wq**, and press **Enter**.

The system saves the configurations and exits the vi editor.

14. Run the following command to effect the modification:

```
sysctl -p /etc/sysctl.conf
```

15. Run the following command to delete the original iptables rule:

```
iptables -F
```

16. Run the following command to configure source network address translation (SNAT) to enable ECSs in the same network segment to access the Internet through the proxy ECS:

```
iptables -t nat -A POSTROUTING -o eth0 -s subnet/netmask-bits -j SNAT --to nat-instance-ip
```

For example, if the proxy ECS is in network segment 192.168.125.0, the subnet mask has 24 bits, and the private IP address is 192.168.125.4, run the following command:

```
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.125.0/24 -j SNAT --to 192.168.125.4
```

NOTE

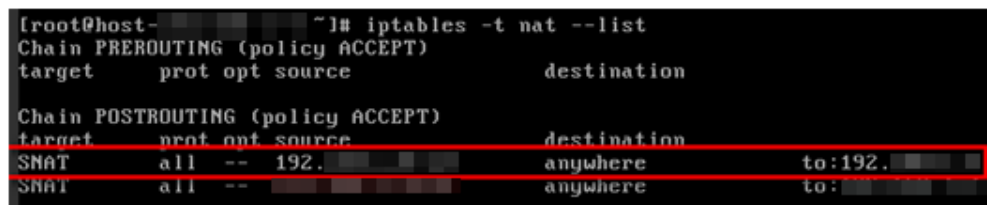
To retain the preceding configuration even after the ECS is restarted, run the `vi /etc/rc.local` command to edit the `rc.local` file. Specifically, copy the rule described in step 16 into `rc.local`, press `Esc` to exit the editing mode, and enter `:wq` to save and exit the file.

17. Run the following command to check whether SNAT has been configured:

```
iptables -t nat --list
```


SNAT has been configured if information similar to [Figure 9-2](#) is displayed.

Figure 9-2 Successful SNAT configuration



```
[root@host- ~]# iptables -t nat --list
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
SNAT      all  --  192.168.125.0/24      anywhere             to:192.168.125.4
SNAT      all  --  192.168.125.0/24      anywhere             to:
```

18. Add a route.
 - a. Log in to the management console.
 - b. Click  in the upper left corner and select the desired region and project.
 - c. Under **Network**, click **Virtual Private Cloud**.
 - d. Select a VPC to which a route is to be added and click **Route Tables**. On the **Route Tables** page, click **Add Route**.
 - e. Set route information on the displayed page.
 - **Destination:** indicates the destination network segment. The default value is `0.0.0.0/0`.
 - **Next Hop:** indicates the private IP address of the SNAT ECS.
You can obtain the private IP address of the ECS on the **Elastic Cloud Server** page.

Follow-up Procedure

To delete the added iptables rules, run the following command:

```
iptables -t nat -D POSTROUTING -o eth0 -s subnet/netmask-bits -j SNAT --to nat-instance-ip
```

For example, if the proxy ECS is in network segment 192.168.125.0, the subnet mask has 24 bits, and the private IP address is 192.168.125.4, run the following command:

```
iptables -t nat -D POSTROUTING -o eth0 -s 192.168.125.0/24 -j SNAT --to  
192.168.125.4
```

10 Resources



10.1 Quota Adjustment

What Is Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click  .
The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.

If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

The system does not support online quota adjustment. If you need to adjust a quota, call the hotline or send an email to the customer service mailbox. Customer service personnel will timely process your request for quota adjustment and inform you of the real-time progress by making a call or sending an email.

Before dialing the hotline number or sending an email, make sure that the following information has been obtained:

- Account name, project name, and project ID, which can be obtained by performing the following operations:

Log in to the management console using the cloud account, click the username in the upper right corner, select **My Credentials** from the drop-down list, and obtain the account name, project name, and project ID on the **My Credentials** page.

- Quota information, which includes:
 - Service name
 - Quota type
 - Required quota

If you need to adjust a quota, contact the administrator.

11 Monitoring

11.1 Monitoring ECSs

Monitoring is the key for ensuring ECS performance, reliability, and availability. Using monitored data, you can determine ECS resource usage. The public cloud provides Cloud Eye to help you obtain the running statuses of your ECSs. You can use Cloud Eye to automatically monitor ECSs in real time and manage alarms and notifications to keep track of ECS performance metrics.

Server Monitoring includes **Basic Monitoring** and **OS Monitoring**.

- **Basic Monitoring** automatically reports ECS metrics to Cloud Eye.
- Using the agent installed on the target ECS, **OS Monitoring** provides system-wide, active, and fine-grained ECS monitoring.

For instructions about how to install and configure the agent, see **Server Monitoring** in *Cloud Eye User Guide*.

This section covers the following content:

- Viewing basic ECS metrics
- Customizing ECS alarm rules
- Viewing ECS running statuses for routine monitoring

11.2 Basic ECS Metrics

Description

This section describes monitoring metrics reported by ECS to Cloud Eye and their namespaces. You can use Cloud Eye to view these metrics and alarms generated for ECSs.

Namespace

SYS.ECS

ECS Metrics

ECS metrics vary depending on ECS OSs and types. For details, see [Table 11-1](#). ✓ indicates that the metric is supported, and x indicates that the metric is not supported.

Table 11-1 ECS metrics

Metric	Windows		Linux	
	Xen	KVM	Xen	KVM
None	Xen	KVM	Xen	KVM
CPU Usage	✓	✓	✓	✓
Memory Usage	✓	✓	✓ (VMTools must be installed on the image. Otherwise, this metric is unavailable.)	x (Agent must be installed on the ECS. Otherwise, this metric is unavailable.)
Disk Usage	✓	✓	✓ (VMTools must be installed on the image. Otherwise, this metric is unavailable.)	x (Agent must be installed on the ECS. Otherwise, this metric is unavailable.)
Disk Read Bandwidth	✓	✓	✓	✓
Disk Write Bandwidth	✓	✓	✓	✓
Disk Read IOPS	✓	✓	✓	✓
Disk Write IOPS	✓	✓	✓	✓
Inband Incoming Rate	✓ (VMTools must be installed on the image. Otherwise, this metric is unavailable.)	✓	✓ (VMTools must be installed on the image. Otherwise, this metric is unavailable.)	x (Agent must be installed on the ECS. Otherwise, this metric is unavailable.)

Metric	Windows		Linux	
Inband Outgoing Rate	√ (VMTools must be installed on the image. Otherwise, this metric is unavailable.)	√	√ (VMTools must be installed on the image. Otherwise, this metric is unavailable.)	x (Agent must be installed on the ECS. Otherwise, this metric is unavailable.)
Outband Incoming Rate	√ (If VMTools is installed on the image, this metric is unavailable. In such a case, use the inband incoming rate.)	√	√ (If VMTools is installed on the image, this metric is unavailable. In such a case, use the inband incoming rate.)	√
Outband Outgoing Rate	√ (If VMTools is installed on the image, this metric is unavailable. In such a case, use the inband outgoing rate.)	√	√ (If VMTools is installed on the image, this metric is unavailable. In such a case, use the inband outgoing rate.)	√

 **NOTE**

- Certain ECS metrics require the installation of VMTools on the image, based on which the ECS is created. For instructions about how to install VMTools, see <https://github.com/UEP-Tools/UEP-Tools/>.
- Certain ECS metrics require the installation of the agent on the ECS. After the agent is installed, log in to the management console and choose **Cloud Eye** under **Management & Deployment**. Then, view ECS metrics, such as **AGT. User Space CPU Usage**, by choosing **ECS Monitoring** > Target ECS > **OS Monitoring**. For details, see **ECS Metrics Under OS Monitoring**.
 - For instructions about how to install the agent on a Windows ECS, see "Installing and Configuring the Agent (Windows)" in *Cloud Eye User Guide*.
 - For instructions about how to install the agent on a Linux ECS, see "Installing and Configuring the Agent (Linux)" in *Cloud Eye User Guide*.

Table 11-2 describes these ECS metrics.

The monitoring intervals for the following ECSs with raw monitoring metrics are as follows:

- Xen ECS: 4 minutes

- KVM ECS: 5 minutes

Table 11-2 Metric description

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
cpu_util	CPU Usage	CPU usage of an ECS Unit: Percent Formula: CPU usage of an ECS/Number of vCPUs in the ECS	≥ 0	ECS	5 minutes
mem_util	Memory Usage	Memory usage of an ECS This metric is unavailable if the image has no VMTools installed. Unit: Percent Formula: Used memory of an ECS/ Total memory of the ECS	≥ 0	ECS	5 minutes
disk_util_inband	Disk Usage	Disk usage of an ECS This metric is unavailable if the image has no VMTools installed. Unit: Percent Formula: Used capacity of an ECS disk/Total capacity of the ECS disk	≥ 0	ECS	5 minutes

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
disk_read_bytes_rate	Disk Read Bandwidth	Number of bytes read from an ECS disk per second Unit: byte/s Formula: Total number of bytes read from an ECS disk/Monitoring interval $byte_out = (rd_bytes - last_rd_bytes)/Time\ difference$	≥ 0	ECS	5 minutes
disk_write_bytes_rate	Disk Write Bandwidth	Number of bytes written to an ECS disk per second Unit: byte/s Formula: Total number of bytes written to an ECS disk/Monitoring interval	≥ 0	ECS	5 minutes
disk_read_requests_rate	Disk Read IOPS	Number of read requests sent to an ECS disk per second Unit: request/s Formula: Total number of read requests sent to an ECS disk/Monitoring interval $req_out = (rd_req - last_rd_req)/Time\ difference$	≥ 0	ECS	5 minutes

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
disk_write_requests_rate	Disk Write IOPS	Number of write requests sent to an ECS disk per second Unit: request/s Formula: Total number of write requests sent to an ECS disk/Monitoring interval $req_in = (wr_req - last_wr_req) / \text{Time difference}$	≥ 0	ECS	5 minutes
network_incoming_bytes_rate_inband	Inband Incoming Rate	Number of incoming bytes on an ECS per second Unit: byte/s Formula: Total number of inband incoming bytes on an ECS/Monitoring interval	≥ 0	ECS	5 minutes
network_outgoing_bytes_rate_inband	Inband Outgoing Rate	Number of outgoing bytes on an ECS per second Unit: byte/s Formula: Total number of inband outgoing bytes on an ECS/Monitoring interval	≥ 0	ECS	5 minutes

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
network_incoming_bytes_aggregate_rate	Outband Incoming Rate	Number of incoming bytes on an ECS per second on the hypervisor Unit: byte/s Formula: Total number of outband incoming bytes on an ECS/Monitoring interval This metric is unavailable if SR-IOV is enabled.	≥ 0	ECS	5 minutes
network_outgoing_bytes_aggregate_rate	Outband Outgoing Rate	Number of outgoing bytes on an ECS per second on the hypervisor Unit: byte/s Formula: Total number of outband outgoing bytes on an ECS/Monitoring interval This metric is unavailable if SR-IOV is enabled.	≥ 0	ECS	5 minutes

Dimensions

Key	Value
instance_id	Specifies the ECS ID.

11.3 OS Monitoring Metrics Supported by ECSs with the Agent Installed

This section describes monitoring metrics reported by ECSs to Cloud Eye as well as their namespaces and dimensions. You can use the Cloud Eye management console or APIs to obtain the monitoring metrics and alarms generated for ECSs.

After installing the agent on an ECS, you can view its OS monitoring metrics. Monitoring data is collected every 1 minute.

Table 11-3 OS monitoring metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
cpu_usage	(Agent) CPU Usage	<p>CPU usage of the monitored object</p> <p>Unit: percent</p> <ul style="list-style-type: none"> Linux: Check metric value changes in file /proc/stat in a collection period. Run the top command to check the %Cpu(s) value. Windows: Obtain the metric value using the Windows API GetSystemTimes. 	0-100	ECS	1 minute
load_average5	(Agent) 5-Minute Load Average	<p>CPU load averaged from the last 5 minutes</p> <ul style="list-style-type: none"> Linux: Obtain the metric value from the number of logic CPUs in load5/ in file /proc/loadavg. Run the top command to check the load5 value. Windows does not support this metric. 	≥ 0	ECS	1 minute
memory_usage	(Agent) Memory Usage	<p>Memory usage of the monitored object</p> <p>Unit: percent</p> <ul style="list-style-type: none"> Linux: Obtain the metric value from the /proc/meminfo file (MemTotal - MemAvailable)/MemTotal. Windows: Obtain the value using the following formula: Used memory size/Total memory size x 100% 	0-100	ECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_free	(Agent) Available Disk Space	<p>Free disk space Unit: GB</p> <ul style="list-style-type: none"> Linux: Run the df -h command to check the value in the Avail column. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). Windows: Obtain the metric value using the WMI API GetDiskFreeSpaceExW. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). 	≥ 0	ECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_usedPercent	(Agent) Disk Usage	<p>Percentage of total disk space that is used</p> <p>Unit: percent</p> <ul style="list-style-type: none"> Linux: Obtain the metric value using following formula: Disk Usage = Used Disk Space/Disk Storage Capacity. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). Windows: Obtain the metric value using the WMI API GetDiskFreeSpaceExW. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). 	0-100	ECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_io Utils	(Agent) Disk I/O Usage	<p>Percentage of the time that the disk has had I/O requests queued to the total disk operation time</p> <p>Unit: percent</p> <ul style="list-style-type: none"> Linux: Obtain the metric value by calculating the data changes in the thirteenth column of the monitored object in file /proc/diskstats in a collection period. <p>The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).</p> <ul style="list-style-type: none"> Windows does not support this metric. 	0-100	ECS	1 minute
disk_in odesUsed Percent	(Agent) Percent age of Total inode Used	<p>Number of used index nodes on the disk</p> <p>Unit: percent</p> <ul style="list-style-type: none"> Linux: Run the df -i command to check the value in the IUse% column. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). Windows does not support this metric. 	0-100	ECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
net_bit Sent	(Agent) Inbound Bandwidth	Number of bits sent by the target NIC per second Unit: bit/s <ul style="list-style-type: none"> Linux: Check metric value changes in file / proc/net/dev in a collection period. Windows: Obtain the metric value using the WMI MibIfRow object. 	≥ 0	ECS	1 minute
net_bit Recv	(Agent) Outbound Bandwidth	Number of bits received by the monitored object per second Unit: bit/s <ul style="list-style-type: none"> Linux: Check metric value changes in file / proc/net/dev in a collection period. Windows: Obtain the metric value using the WMI MibIfRow object. 	≥ 0	ECS	1 minute
net_packetRecv	(Agent) NIC Packet Receive Rate	Number of packets received by this NIC per second Unit: count/s <ul style="list-style-type: none"> Linux: Check metric value changes in file / proc/net/dev in a collection period. Windows: Obtain the metric value using the WMI MibIfRow object. 	≥ 0	ECS	1 minute
net_packetSent	(Agent) NIC Packet Send Rate	Number of packets sent by this NIC per second Unit: count/s <ul style="list-style-type: none"> Linux: Check metric value changes in file / proc/net/dev in a collection period. Windows: Obtain the metric value using the WMI MibIfRow object. 	≥ 0	ECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
net_tcp_total	(Agent) Total number of TCP connections	Total number of TCP connections of this NIC	≥ 0	ECS	1 minute
net_tcp_established	(Agent) Number of ESTABLISHED TCP connections	Number of ESTABLISHED TCP connections of this NIC	≥ 0	ECS	1 minute

11.4 Setting Alarm Rules

Scenarios

Setting ECS alarm rules allows you to customize the monitored objects and notification policies and determine the running statuses of your ECSs at any time.

This section describes how to set ECS alarm rules, including alarm rule names, monitoring objects, monitoring metrics, alarm thresholds, monitoring intervals, and notifications.

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, click **Cloud Eye**.
3. In the navigation pane on the left, choose **Alarm Management > Alarm Rules**.
4. On the **Alarm Rules** page, click **Create Alarm Rule** to create an alarm rule, or modify an existing alarm rule.

The following operations use modifying an existing alarm rule as an example.

- a. Click the target alarm rule.
- b. Click **Modify** in the upper right corner of the page.
- c. On the **Modify Alarm Rule** page, set parameters as prompted.
- d. Click **OK**.

After an alarm rule is modified, the system automatically notifies you of an alarm when the alarm complying with the alarm rule is generated.

 NOTE

For more information about ECS alarm rules, see *Cloud Eye User Guide*.

11.5 Viewing ECS Metrics

Scenarios

The public cloud platform provides Cloud Eye, which monitors the running statuses of your ECSs. You can obtain the monitoring metrics of each ECS on the management console.

Prerequisites

- The ECS is running properly.
Cloud Eye does not display the monitoring data for a stopped, faulty, or deleted ECS. After such an ECS restarts or recovers, the monitoring data is available in Cloud Eye.

 NOTE

Cloud Eye discontinues monitoring ECSs that remain in **Stopped** or **Faulty** state for 24 hours and removes them from the monitoring list. However, the alarm rules for such ECSs are not automatically deleted.

- Alarm rules have been configured in Cloud Eye for the target ECS.
The monitoring data is unavailable for the ECSs without alarm rules configured in Cloud Eye. For details, see [11.4 Setting Alarm Rules](#).
- The target ECS has been properly running for at least 10 minutes.
The monitoring data and graphics are available for a new ECS after the ECS runs for at least 10 minutes.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. In the search box above the upper right corner of the ECS list, enter the ECS name, IP address, or ID for search.
4. Click the name of the target ECS. The page providing details about the ECS is displayed.
5. Click the **Monitoring** tab to view the monitoring data.
6. In the ECS monitoring area, select a duration to view the monitoring data.
You can view the monitoring data of the ECS in the last 1, 3, or 12 hours.

12_{CTS}

12.1 Supported CTS Operations

Scenarios

Cloud Trace Service (CTS) is available on the platform. It records ECS-related operations for later query, audit, and backtrack operations.

Prerequisites

CTS is available.

Key ECS Operations Recorded by CTS

Table 12-1 ECS operations recorded by CTS

Operation	Resource Type	Event Name
Creating an ECS	ECS	createServer
Deleting an ECS	ECS	deleteServer
Starting an ECS	ECS	startServer
Restarting an ECS	ECS	rebootServer
Stopping an ECS	ECS	stopServer
Adding an ECS NIC	ECS	addNic
Deleting an ECS NIC	ECS	deleteNic
Attaching a disk (on the EVS console)	ECS	attachVolume2
Reinstalling an OS	ECS	reinstallOs
Changing an OS	ECS	changeOs

Operation	Resource Type	Event Name
Modifying specifications	ECS	resizeServer
Enabling automatic recovery on an ECS	ECS	addAutoRecovery
Disabling automatic recovery on an ECS	ECS	deleteAutoRecovery
Creating a security group	ECS	createSecurityGroup

12.2 Viewing Tracing Logs

Scenarios

CTS records ECS operations immediately after it is provisioned. You can view the operation records of the last seven days on the management console.

This section describes how to view the operation records.

Procedure

1. Log in to the management console.
2. Click **Service List**. Under **Management & Deployment**, click **Cloud Trace Service**.
3. In the navigation pane on the left, choose **Trace List**.
4. Click **Filter** and specify filter criteria as needed. The following four filter criteria are available:
 - **Trace Source, Resource Type, and Search By**
Select a filter criterion from the drop-down list.
If you select **Trace name** for **Search By**, you need to select a specific trace name.
If you select **Resource ID** for **Search By**, you need to select or enter a specific resource ID.
When you select **Resource name** for **Search By**, you need to select or enter a specific resource name.
 - **Operator**: Select a specific operator (which is a user rather than the tenant).
 - **Trace Status**: Available options include **All trace statuses, normal, warning, and incident**. You can only select one of them.
 - **Time Range**: You can view traces generated during any time range of the last seven days.
5. Expand the trace for details.
6. Click **View Trace**. A dialog box is displayed, in which the trace structure details are displayed.
For more information about CTS, see *Cloud Trace Service User Guide*.

13 FAQs

13.1 Product Consultation

13.1.1 What Restrictions Apply to ECSs?

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

13.1.2 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.

13.1.3 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

13.2 Creation and Deletion

13.2.1 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.

13.2.2 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.
- This issue does not occur if a full-ECS image is created using a CBR backup.

Solution Using CBR

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.
In such a case, use the ECS to create a CBR backup and use this 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 Backup and Recovery 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. Use an ECS to create a CBR backup.
For details, see *Cloud Backup and Recovery User Guide*.
 - c. Use the CBR backup to create a full-ECS image.
For details, see *Image Management Service User Guide*.
The created full-ECS image can be used to rapidly create ECSs.

Solution Using CSBS

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.

13.2.3 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.

13.2.4 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.
2. Under **Computing**, click **Elastic Cloud Server**.
3. Select the ECS to be deleted.
4. In the upper part of the ECS list, click **Delete**.

13.2.5 Can a Deleted ECS Be Provisioned Again?

Deleted is an intermediate state of the ECS. ECSs in this state can no longer provide services and are soon removed from the system.


A deleted ECS is retained in the ECS list on the management console only for a short period of time before it is permanently removed from the system. You can create new ECSs of the same specifications again.

13.2.6 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.

13.2.7 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, 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.
3. Under **Computing**, click **Elastic Cloud Server**.
4. Select the target ECS and click **Restart** or **Stop**.
A dialog box is displayed to confirm whether you want to restart or stop the ECS.
5. Select **Forcibly restart the preceding ECSs** or **Forcibly stop the preceding ECSs**.
6. Click **OK**.

13.3 Login and Connection

13.3.1 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.

```

Connected (encrypted) to: QEMU (i-000FA82E) Before you exit, ensure that computer is locked.
ec2: #####
ec2: ----BEGIN SSH HOST KEY FINGERPRINTS----
ec2: 256 a4:9c:e9:d9:35:68:26:27:c1:0c:43:77:ce:db:17:35 (ECDSA)
ec2: 2048 67:e0:3d:0e:1a:0b:7a:ee:46:5a:1c:4e:44:c3:6f:b7 (RSA)
ec2: ----END SSH HOST KEY FINGERPRINTS----
ec2: #####
----BEGIN SSH HOST KEY KEYS----
ecdsa-sha2-nistp256 AAAAE2UjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGgDDEcd
5y0ugl32daqN011YL3U8R1ZFx91ywQT8mBGUxh7X72y1opMbhQxP2E7t0o5JXt5i831P1+YPLRi9X0w=

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACBx42XP8+4pqD810A7fUz_jhhwR487z8uHa+eEvG
H1dWAU0tY4XrSZE73y_jhSvXyaGY/1GLpeczo6MgdQfW7p8/rnu+TnJ+CHUZ/x0cCDSpInZpYe2cWTrsg
PBGpVZK6ZgqxFcWmkJMMZEYR_j51BtUARU8HCeh7A8bbGJaOUzCuLuUwH0edpdMUiu1BD4bGP/5zsPDGo
y_jexLlavWvsRReaWZAWQ6nTxJ55qx2fs54Gb53SUItleiE2u3aH4DtwCeSox1+/7jc3tSmcc/PHvWnb5
562U0sI1c6p+9xmcI8Rm8KncKr8NMUv3xR/BbGIXcY4dniZZC81Q5IB7yAs7
----END SSH HOST KEY KEYS----
cloud-init[37321]: Cloud-init v. 0.7.5 finished at Wed, 17 Jan 2018 06:39:54 +0000.
0. Datasource DataSourceEc2. Up 36.21 seconds

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

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

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

```
SyslogFacility AUTH
PermitRootLogin yes
# Do not enable sshd passwd auth without ensuring really strong passwords
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication no
GSSAPICleanupCredentials yes
UsePAM yes
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MEASUREMENT
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
X11Forwarding yes
Subsystem sftp /usr/libexec/openssh/sftp-server
#UseDNS no
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
KexAlgorithms diffie-hellman-group-exchange-sha256
AllowTcpForwarding no
GatewayPorts no
X11UseLocalhost yes
AllowAgentForwarding yes
PermitTunnel no
LogLevel VERBOSE
RSAAuthentication yes
PubkeyAuthentication yes
PermitEmptyPasswords no
RhostsRSAAuthentication no
HostbasedAuthentication no
IgnoreRhosts yes
AllowUsers root
~
~
~
~
"sshd_config" 31L, 938C written
hash-4 1#
```

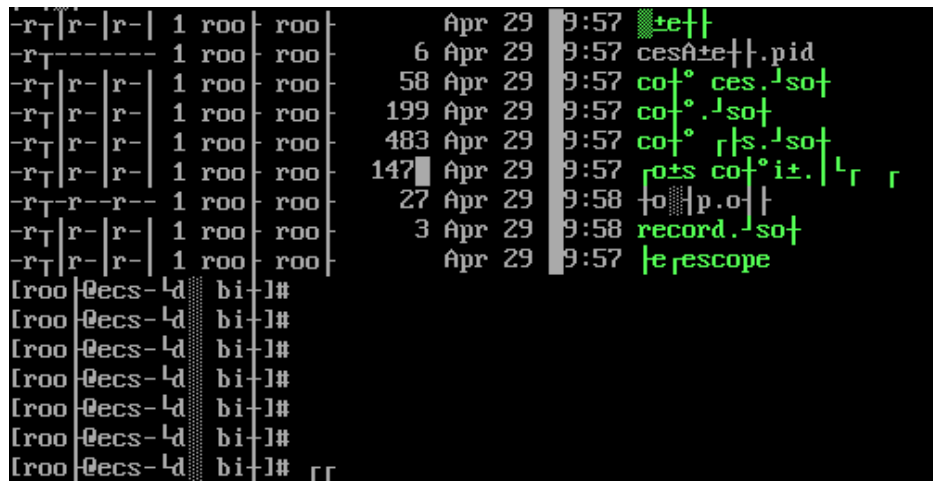
4. Save the modification and exit. Then, run the following command to restart SSH:
service sshd restart
5. Log in to the ECS through SSH.
6. If the fault persists, contact customer service.

13.3.2 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 13-1](#).

Figure 13-1 Garbled characters on the VNC-based login page



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.

13.3.3 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.

13.3.4 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.

13.3.5 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.

13.3.6 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.

Figure 13-2 Error message displayed in a VNC-based remote login



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.

13.3.7 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.

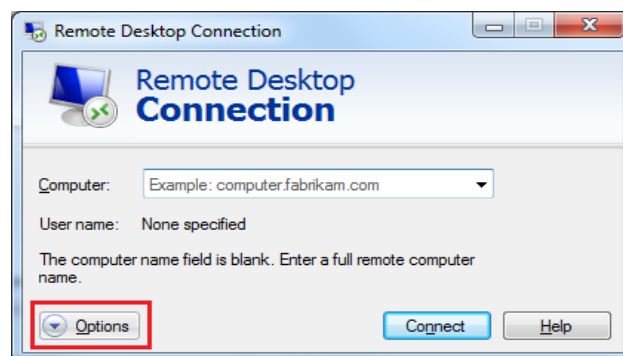
NOTE

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

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

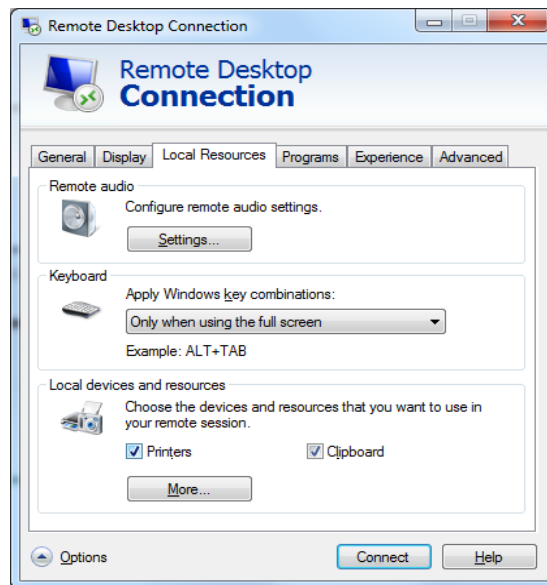
The **Remote Desktop Connection** window is displayed.

Figure 13-3 Remote Desktop Connection



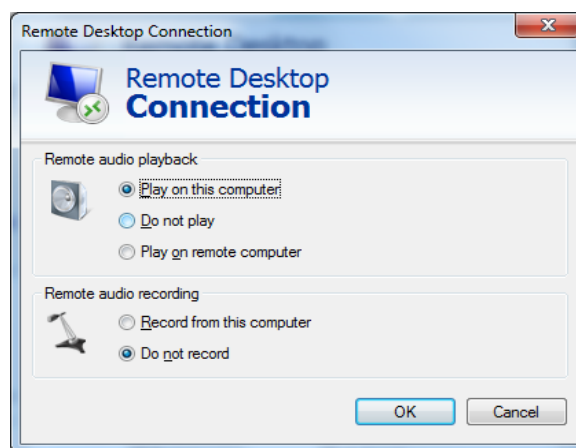
4. Click **Options** in the lower left corner and click the **Local Resources** tab.

Figure 13-4 Local Resources



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

Figure 13-5 Setting remote audio playback



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

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

Scenarios

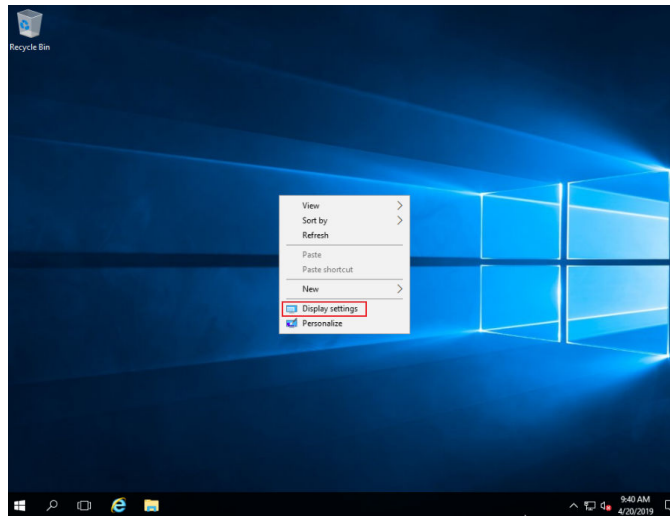
The resolution of a Windows ECS that is remotely logged in must be changed.

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.

Figure 13-6 Display settings

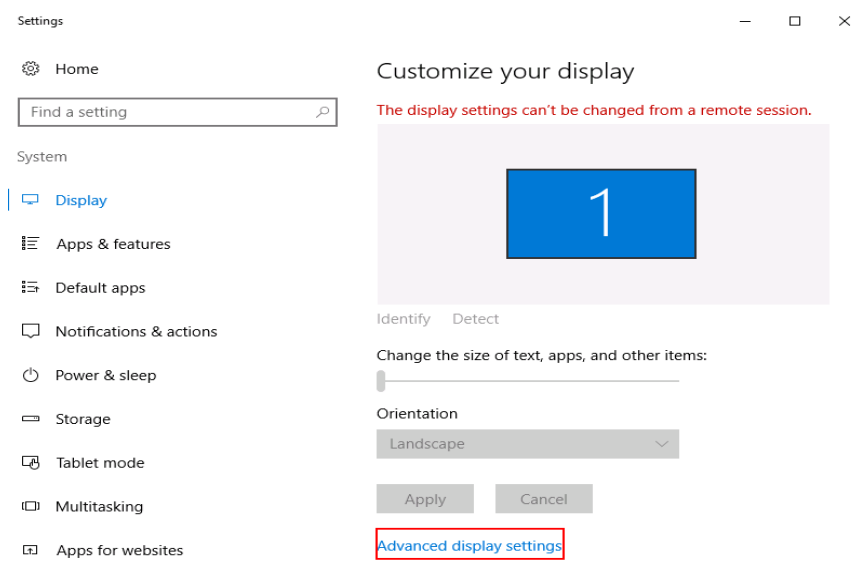


3. On the **Settings** page, click the **Display** tab and then **Advanced display settings**.

 **NOTE**

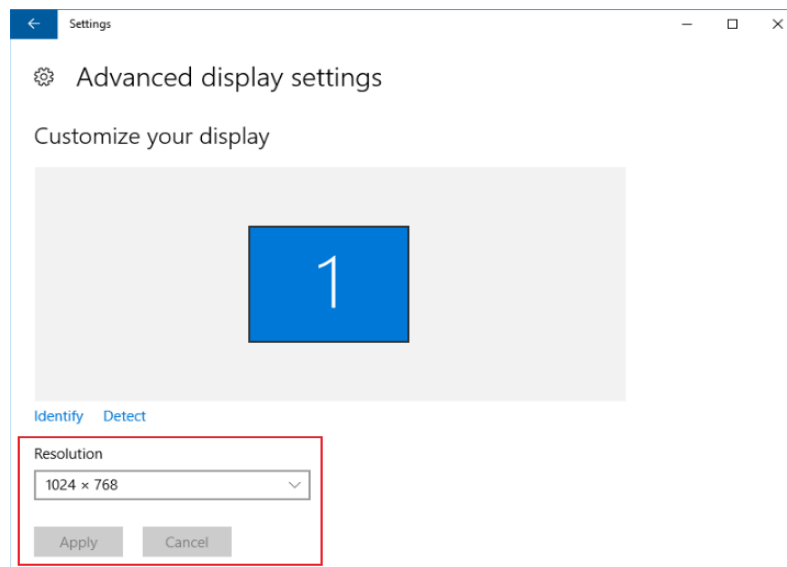
If the remote desktop is not fully displayed, set **Change the size of text, apps, and other items** to **100%**.

Figure 13-7 Settings



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

Figure 13-8 Setting a resolution



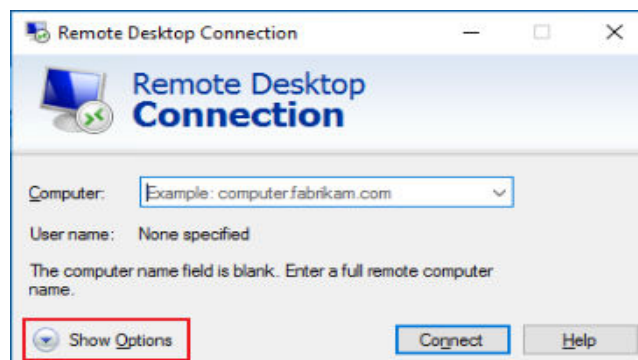
5. Click **Apply**.

Solution 2: Using MSTSC

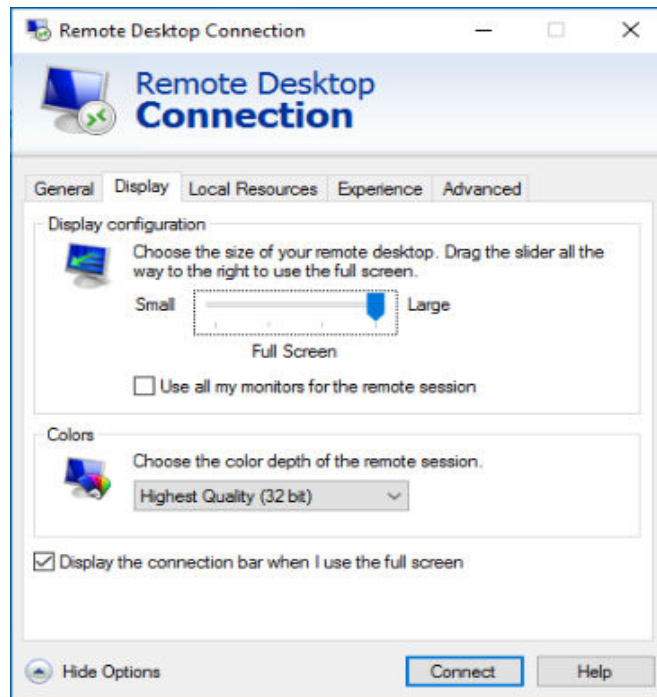
Before remotely logging in to your ECS using MSTSC, change the resolution of the Windows ECS.

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

Figure 13-9 Remote Desktop Connection



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

Figure 13-10 Display

5. Use MSTSC to log in to the ECS.

13.3.9 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.
enablecredsspsupport:i:0
 - g. Double-click the edited .rdp file to set up the remote desktop connection.
 - h. Click **Connect** to connect to the ECS running the Windows Server 2012 OS again.

13.3.10 How Can I Change a Remote Login Port?

Scenarios

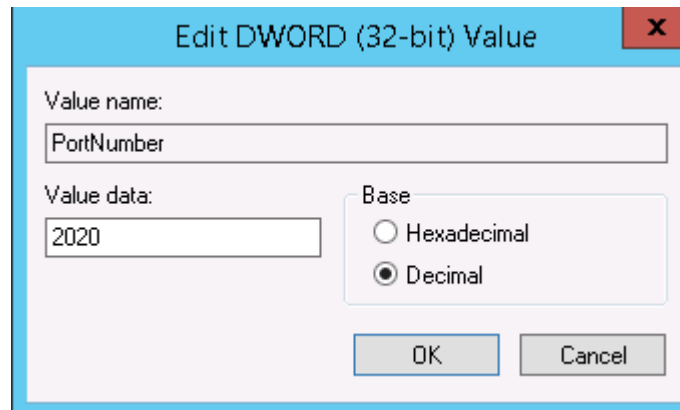
This section describes how to change a port for remote logins.

Windows

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

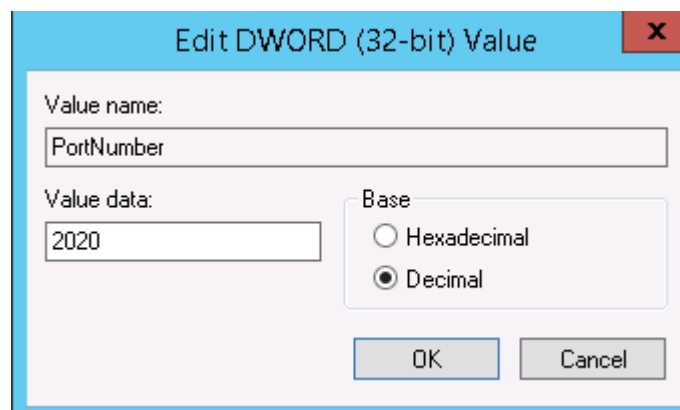
1. In the **Run** dialog box, enter **regedit** to access the registry editor.
2. In **Registry Editor**, choose **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Terminal Server > Wds > rdpwd > Tds > tcp** and double-click **PortNumber**.
 - a. In the dialog box that is displayed, set **Base** to **Decimal**.
 - b. Change the value in **Value data** to the new port number, which is **2020** in this example.

Figure 13-11 Changing the port number to 2020



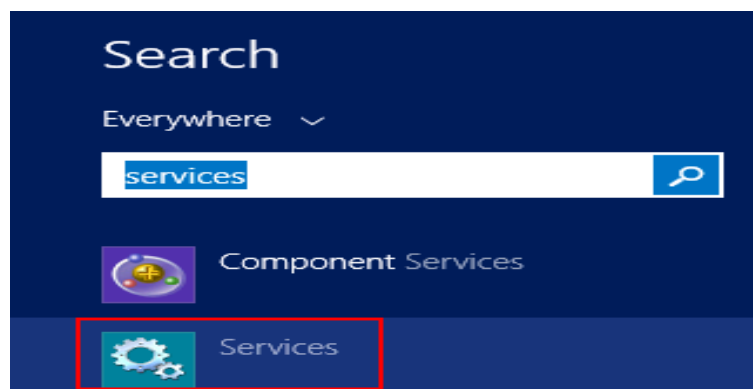
3. In **Registry Editor**, choose **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Terminal Server > WinStations > RDP-Tcp** and double-click **PortNumber**.
 - a. In the dialog box that is displayed, set **Base** to **Decimal**.
 - b. Change the value in **Value data** to the new port number, which is **2020** in this example.

Figure 13-12 Changing the port number to 2020



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

Figure 13-13 Services



5. In the **Services** window, restart **Remote Desktop Services** or the ECS.

6. Modify the inbound rules of the firewall. Perform this operation only if the firewall is enabled.

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

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

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

7. Modify the security group rule.

Add an inbound rule in which **Protocol** is set to **TCP** and **Port Range** is set to **2020**.

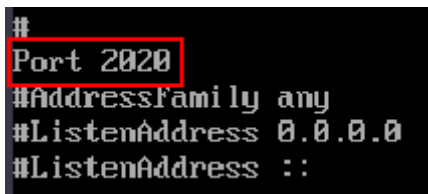
Use port 2020 to remotely log in to the ECS.

Linux

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

1. Run the following command to edit the sshd configuration file:
vi /etc/ssh/sshd_config
2. Delete the comment tag (#) from the **#port 22** line and change **22** to **2020**.

Figure 13-14 Changing the port number to 2020



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

3. Press **Esc** to exit editing mode. Enter **:wq!** to save and exit the configuration.
4. Run either of the following commands to restart sshd:
service sshd restart
Or
systemctl restart sshd
5. (Optional) Configure the firewall. Perform this step if the firewall is enabled. The firewall varies depending on the CentOS version. CentOS 7 uses firewalld, and CentOS 6 uses iptables. The following operations use CentOS 7 as an example.

Run the **firewall-cmd --state** command to check the firewall status.

- Method 1: Disable the firewall and the function of automatically enabling the firewall upon ECS startup.

```
systemctl stop firewalld  
systemctl disable firewalld
```

- Method 2: Add information about a new port to firewalld.
 - i. Run the following commands to add a rule for port 2020:
firewall-cmd --zone=public --add-port=2020/tcp --permanent
firewall-cmd --reload
 - ii. View the added port. The TCP connection of port 2020 has been added.
firewall-cmd --list-all
 - iii. Restart firewalld.
systemctl restart firewalld.service
- 6. Modify the security group rule.
Add an inbound rule in which **Protocol** is set to **TCP** and **Port Range** is set to **2020**.
Use port 2020 to remotely log in to the ECS.

13.3.11 What Should I Do If I Cannot Obtain the Password for Logging In to My Windows ECS Authenticated Using a Key Pair?

Symptom

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

Possible Causes

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

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

Solution

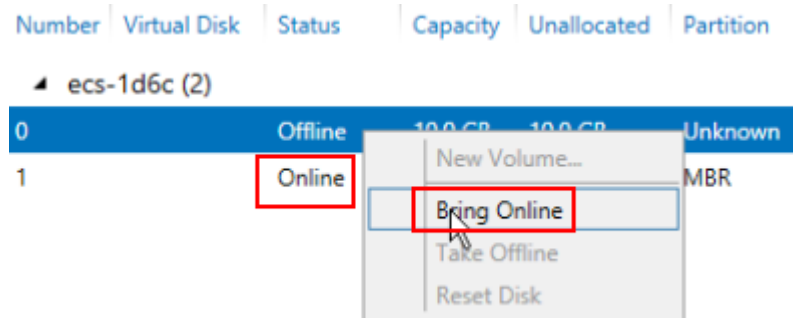
If logging in to an ECS with Cloudbase-Init enabled failed, perform the following operations to locate the fault:

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

For details, see "Installing and Configuring Cloudbase-Init" in *Image Management Service User Guide*.

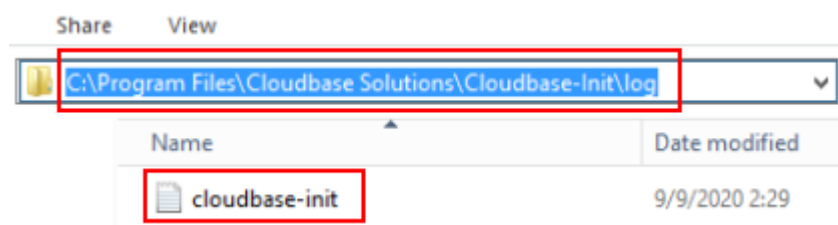
2. Ensure that the key pair for logging in to the ECS is correct.
The key used for obtaining the password must be the key used during the ECS creation.
3. Ensure that DHCP is enabled in the VPC to which the ECS belongs.
On the management console, check whether DHCP has been enabled in the target subnet.
4. Ensure that the ECS has an EIP bound.
5. Ensure that traffic to and from port 80 is allowed in security group rules.
6. Check Cloudbase-Init logs to identify the cause.
 - a. Stop the affected ECS and detach the system disk from it.
 - b. Use a public image to create a temporary Windows ECS and attach the system disk detached in 6.a to the ECS.
 - c. Log in to the temporary ECS, open the **Server Manager** page, choose **File and Storage Services > Volumes > Disks**, right-click the offline disk, and choose **Online** from the shortcut menu.

Figure 13-15 Setting disk online



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

Figure 13-16 cloudbase-init



13.3.12 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 13-1](#).

Table 13-1 Browser version requirements

Browser	Version
Google Chrome	31.0-75.0
Mozilla Firefox	27.0-62.0
Internet Explorer	10.0-11.0

13.3.13 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 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 the password cannot be obtained, contact customer service for technical support.

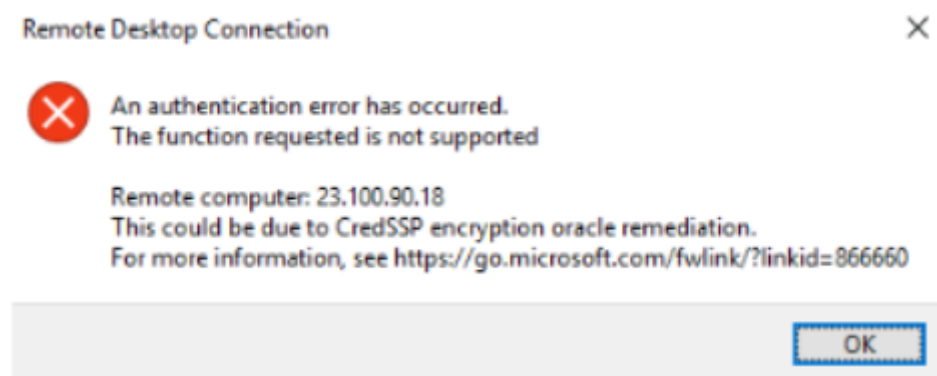
13.3.14 What Should I Do If an Authentication Failure Occurs After I Attempt to Remotely Log In to a Windows ECS?

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 13-17](#), 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 13-17 Failed to set up a remote desktop connection

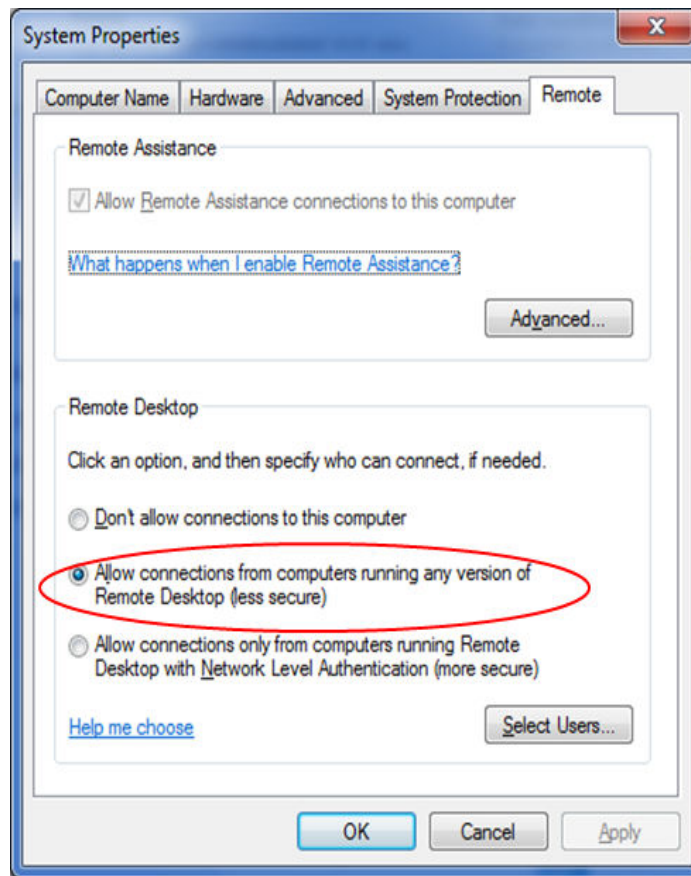


Solution

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

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

Figure 13-18 Remote settings



5. Click **OK**.

13.3.15 What Should I Do If the Local Computer Cannot Connect to My Windows ECS?

Symptom

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

Figure 13-19 Cannot connect to the remote computer



Possible Causes

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

Checking Port Configuration on the ECS

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

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

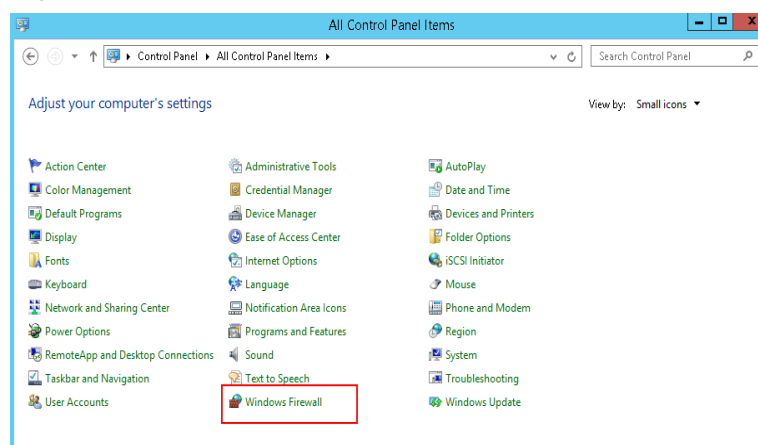
On the page providing details about the ECS, click the **Security Groups** tab and view port 3389 in the inbound rule of the security group.

Checking Whether the Firewall Is Correctly Configured

Check whether the firewall is enabled on the ECS.

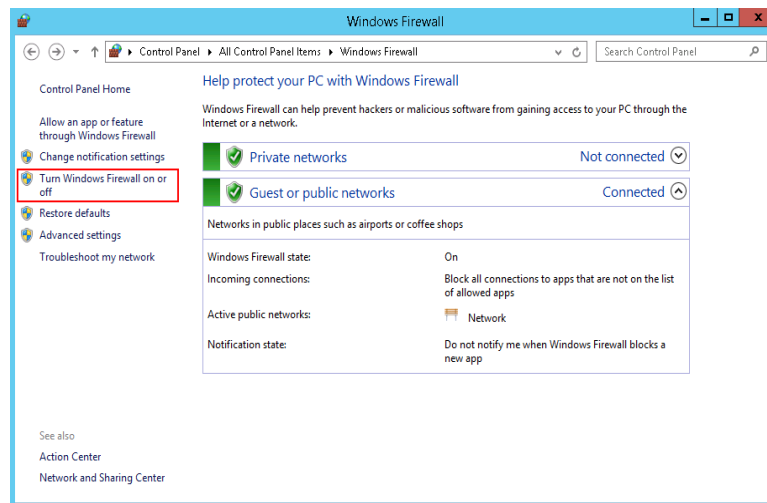
1. Log in to the ECS using VNC available on the management console.
2. Click the Windows icon in the lower left corner of the desktop and choose **Control Panel > Windows Firewall**.

Figure 13-20 Windows Firewall



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

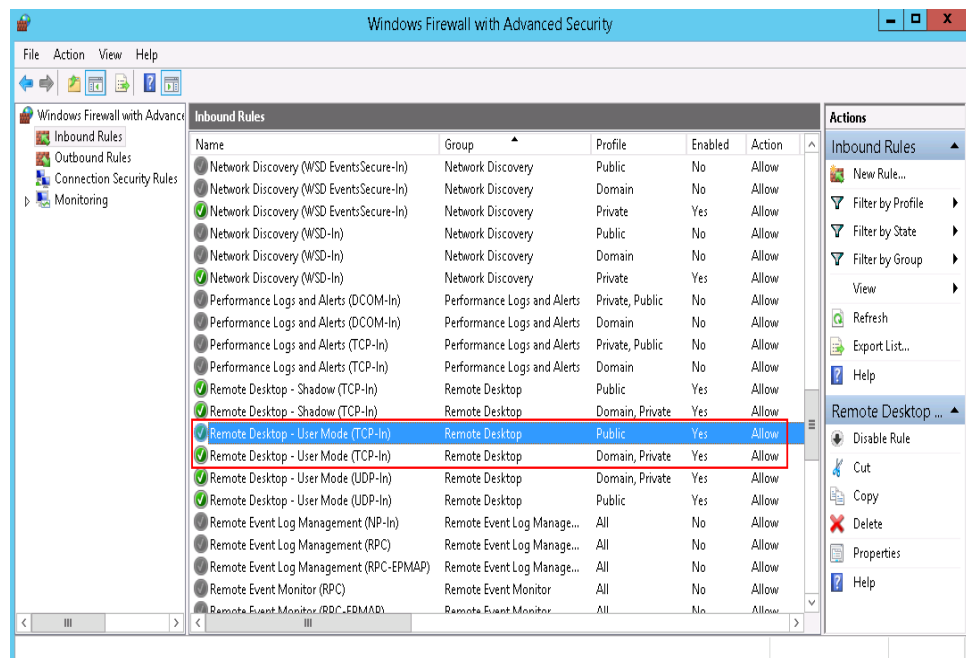
Figure 13-21 Checking firewall status



To enable Windows firewall, perform the following steps:

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

Figure 13-22 Inbound Rules



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

 **NOTE**

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

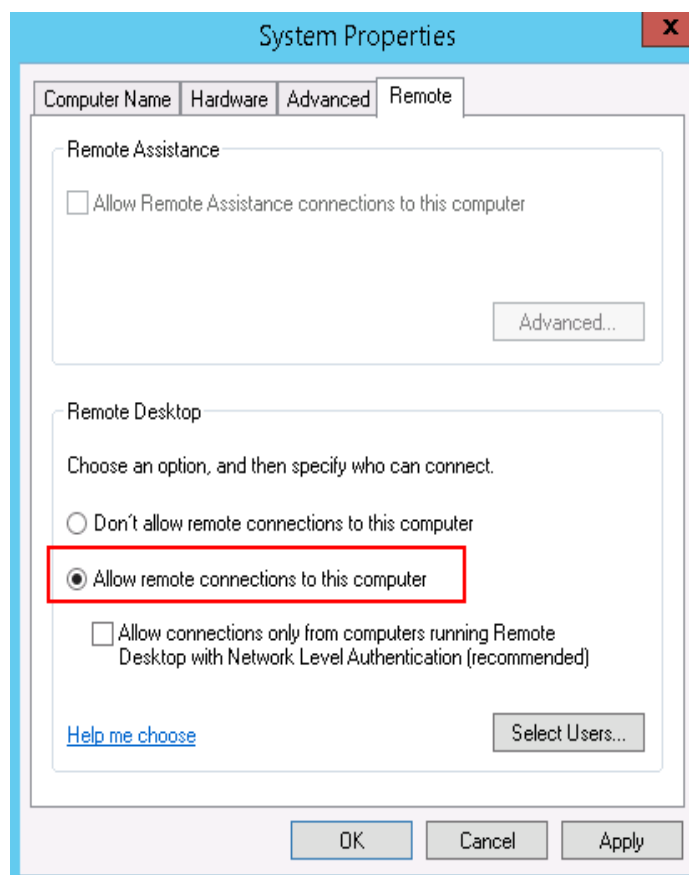
After performing the preceding operations, try to remotely log in to the ECS again.

Checking Remote Desktop Connection Settings

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

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

Figure 13-23 Remote settings

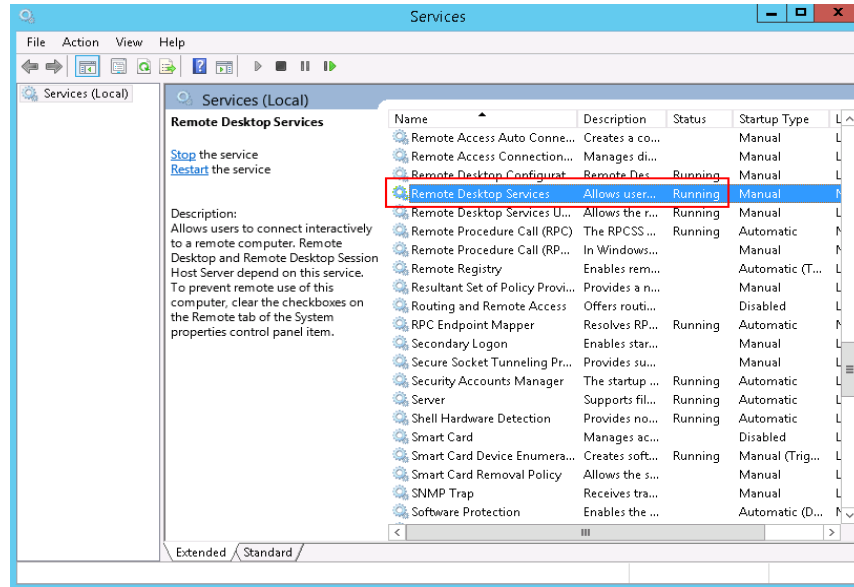


5. Click **OK**.

Checking Remote Desktop Services

1. Open the Windows search box, enter **services**, and select **Services**.
2. In the **Services** window, restart **Remote Desktop Services**. Ensure that **Remote Desktop Services** is in the **Running** status.

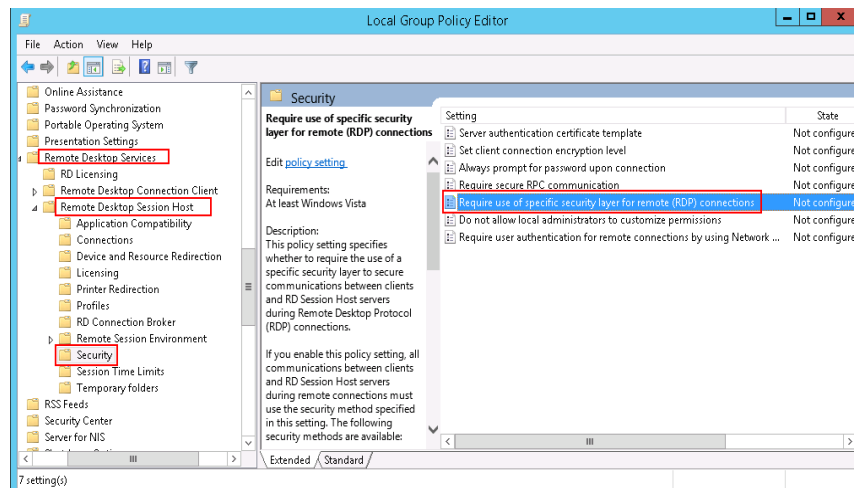
Figure 13-24 Remote Desktop Services



Checking Remote Desktop Session Host Configuration

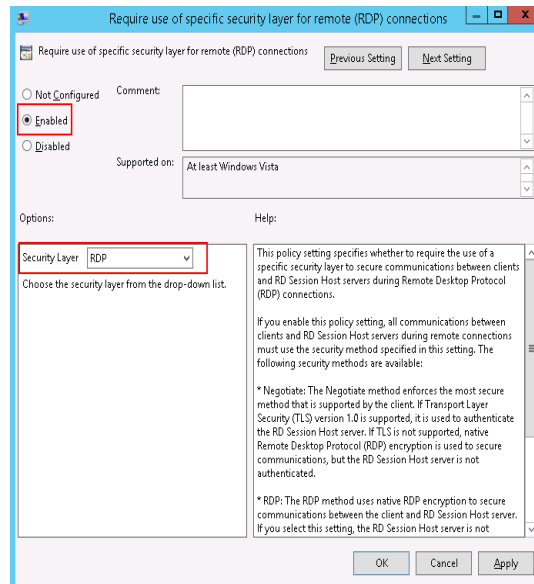
1. Open the **cmd** window and enter **gpedit.msc**.
2. Click **OK** to start Local Group Policy Editor.
3. Choose **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services**.
4. Choose **Remote Desktop Session Host > Security > Require use of specific security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

Figure 13-25 Require use of specific security layer for remote (RDP) connections



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

Figure 13-26 Setting security layer to RDP

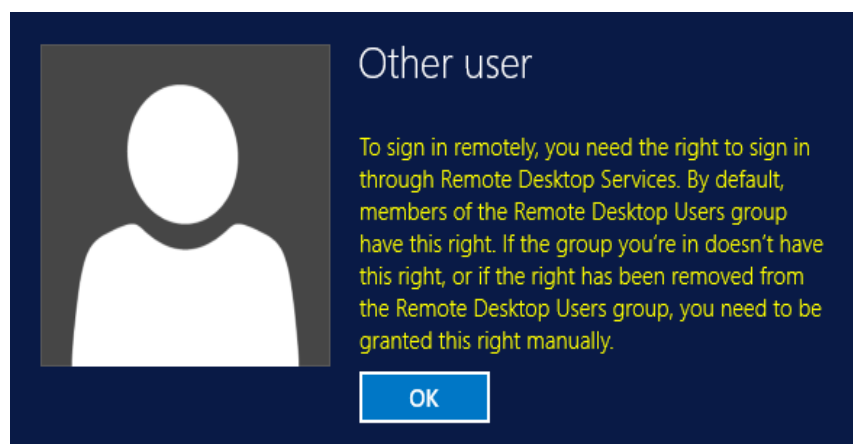


13.3.16 What Should I Do If I Do Not Have the Permission to Remotely Log In to a Windows ECS?

Symptom

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

Figure 13-27 Remote login right missing.

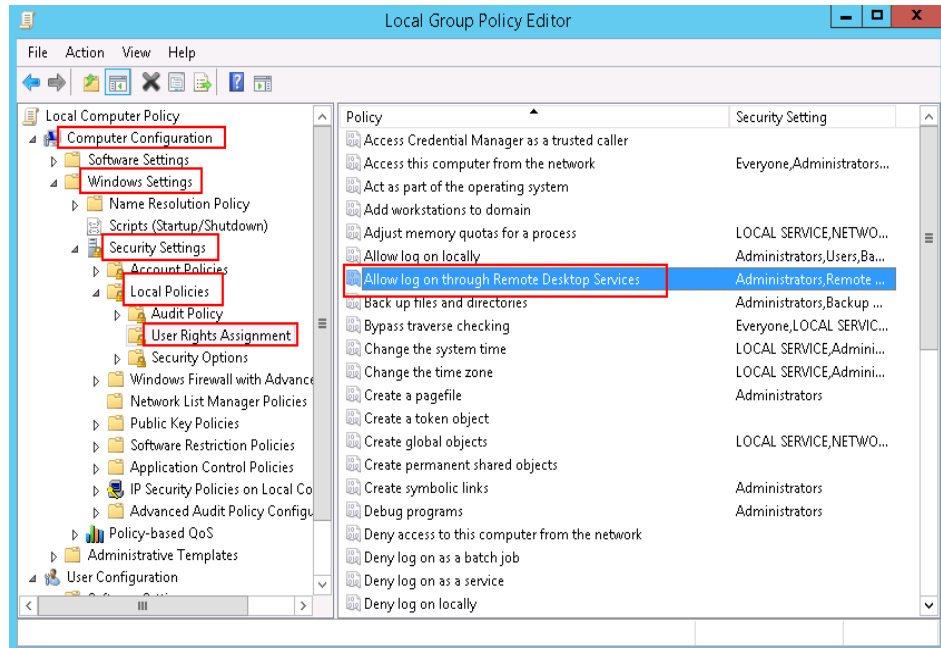


Solution

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

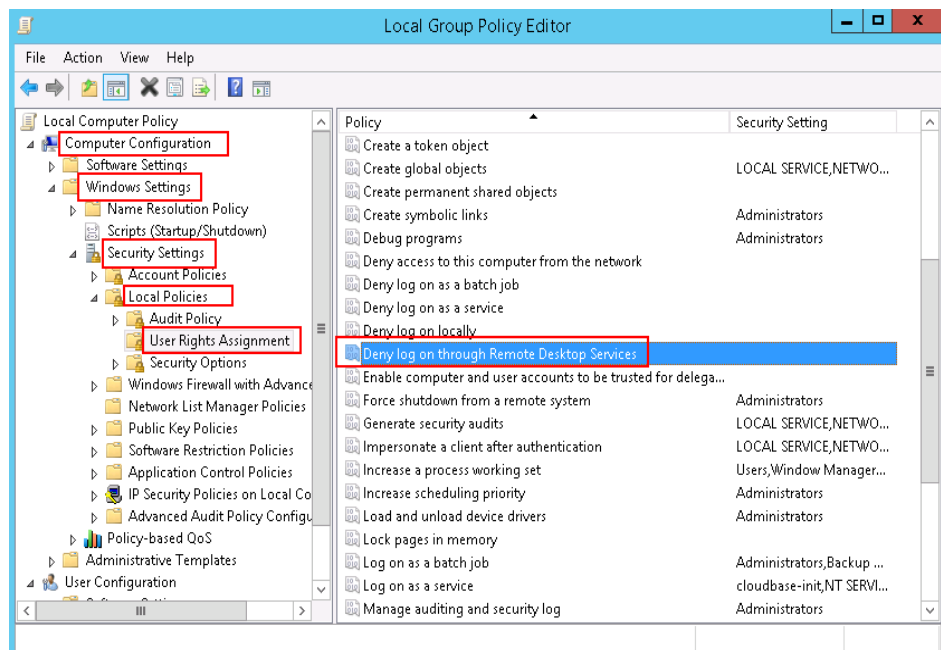
3. Choose **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.
 - a. Locate and double-click **Allow log on through Remote Desktop Services**. Ensure that **Administrators** and **Remote Desktop Users** have been added.

Figure 13-28 Allow log on through Remote Desktop Services properties



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

Figure 13-29 Deny log on through Remote Desktop Services properties

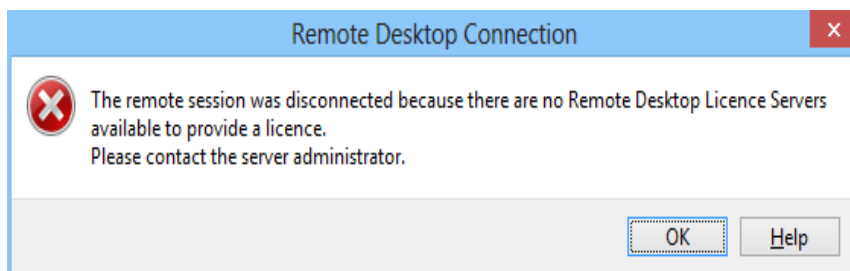


13.3.17 What Should I Do If the System Displays No Remote Desktop License Servers Available to Provide a License When I Log In to a Windows ECS?

Symptom

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

Figure 13-30 No Remote Desktop License Servers available to provide a license



Possible Causes

You have installed the Remote Desktop Session Host.

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

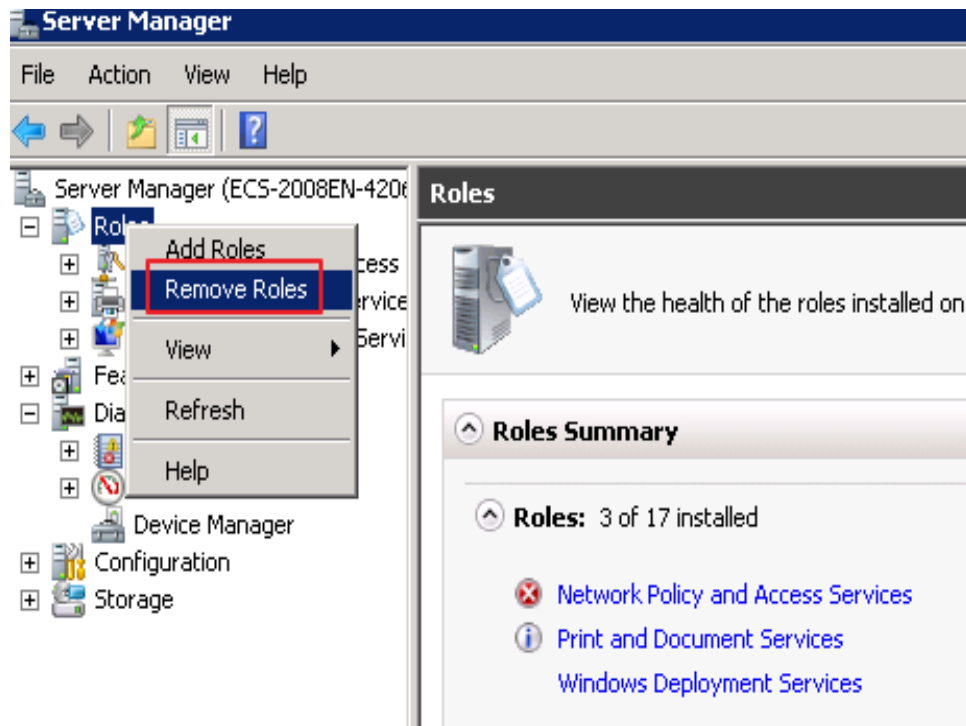
Precautions

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

Windows Server 2008

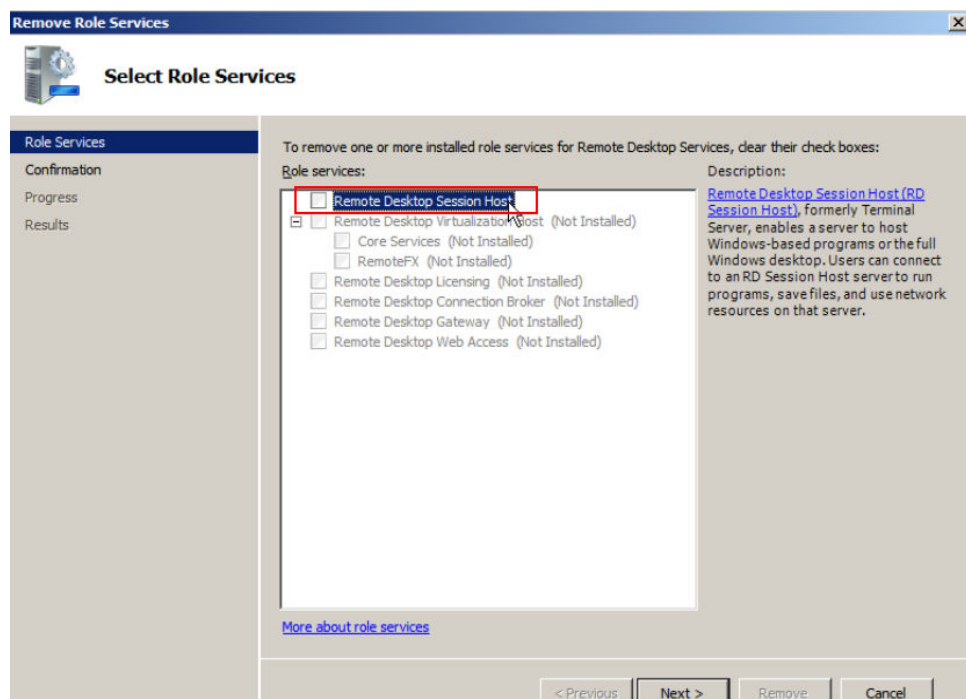
1. Log in to the Windows ECS using VNC available on the management console.
2. Open **Server Manager**, right-click **Remote Desktop Services** under **Roles**, and choose **Remove Roles** from the shortcut menu.

Figure 13-31 Deleting roles



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

Figure 13-32 Deselecting Remote Desktop Session Host

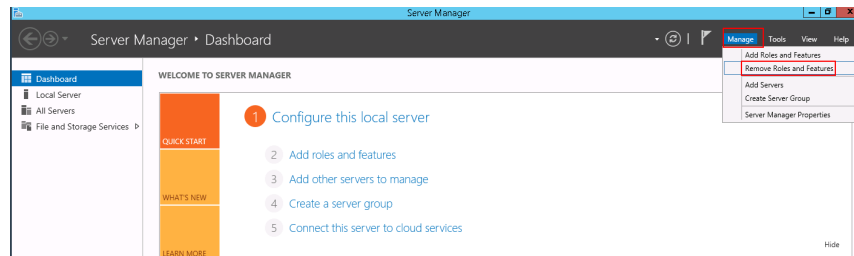


4. Click **Delete**.
5. Restart the ECS.

Windows Server 2012

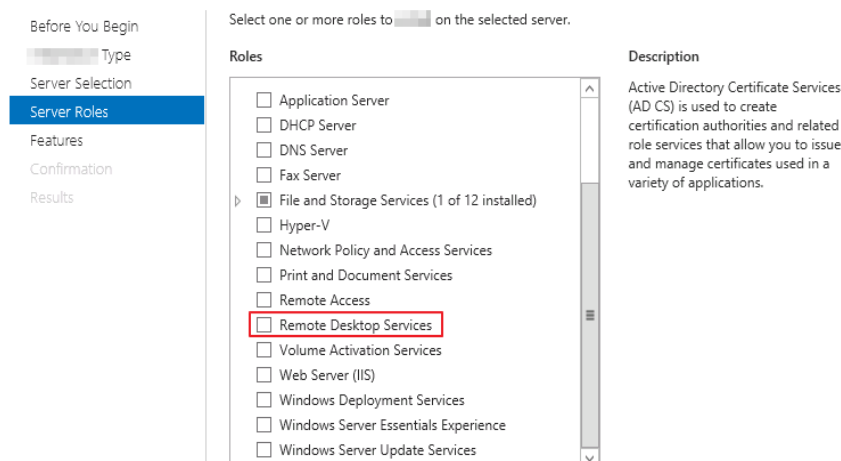
1. Log in to the Windows ECS using VNC available on the management console.
2. Open **Server Manager**, choose **Manage > Remove Roles and Features**, and click **Next**.

Figure 13-33 Deleting roles and features



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

Figure 13-34 Deselecting Remote Desktop Services



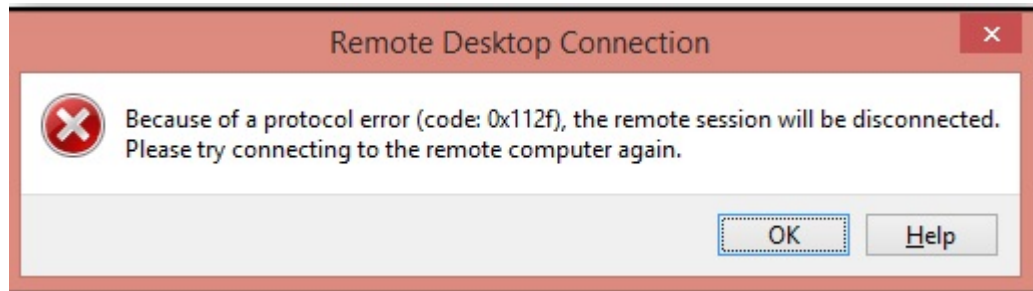
5. Click **Delete**.
6. Restart the ECS.

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

Symptom

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

Figure 13-35 Error message (code: 0x112f)



Possible Causes

The ECS memory is insufficient.

Solution

- Method 1 (recommended)
Modify the ECS specifications to increase the vCPUs and memory size. For instructions about how to modify ECS specifications, see [3.6.1 General Operations for Modifying Specifications](#).
- Method 2
Enable virtual memory on the ECS to obtain its idle memory.
For instructions about how to enable virtual memory, see [13.8.5 How Can I Enable Virtual Memory on a Windows ECS?](#)

NOTE

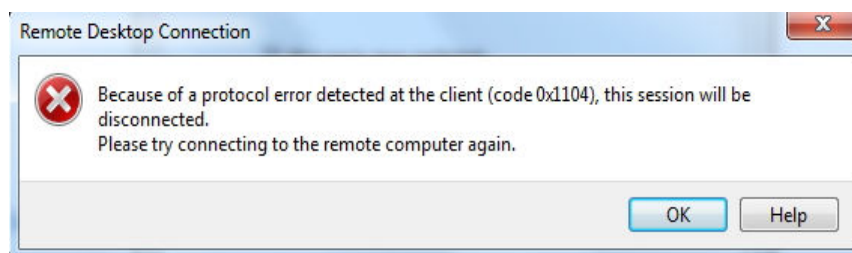
This method will deteriorate the disk I/O performance. Therefore, use this method only when necessary.

13.3.19 What Should I Do If the System Displays Error Code 0x1104 When I Log In to a Windows ECS?

Symptom

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

Figure 13-36 Protocol error (code: 0x1104)



Possible Causes

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

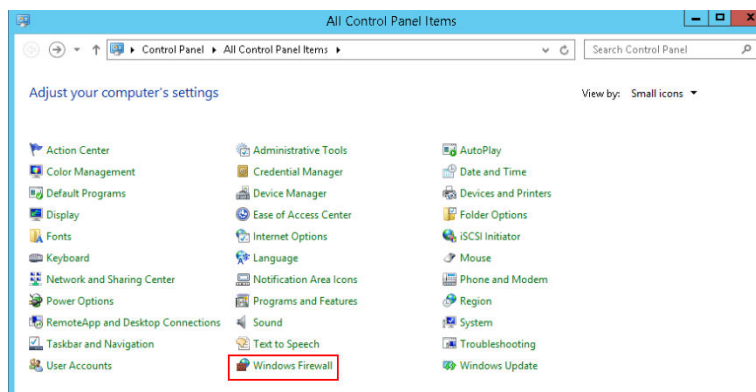
Solution

Step 1 Check security group settings.

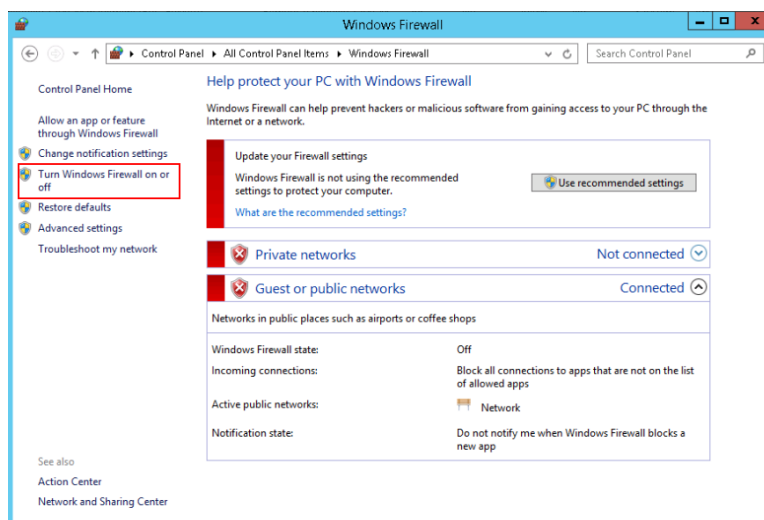
Check whether port 3389 is allowed in inbound direction. If it is, go to [Step 2](#).

Step 2 Check whether the firewall is disabled:

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



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



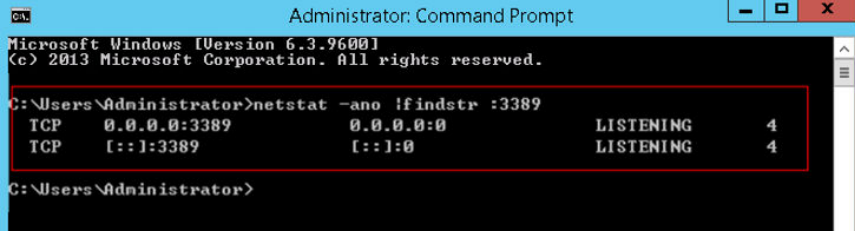
If the firewall is enabled, go to [Step 3](#).

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

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

```
netstat -ano |findstr: 3389
```

Figure 13-37 Checking port 3389



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

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

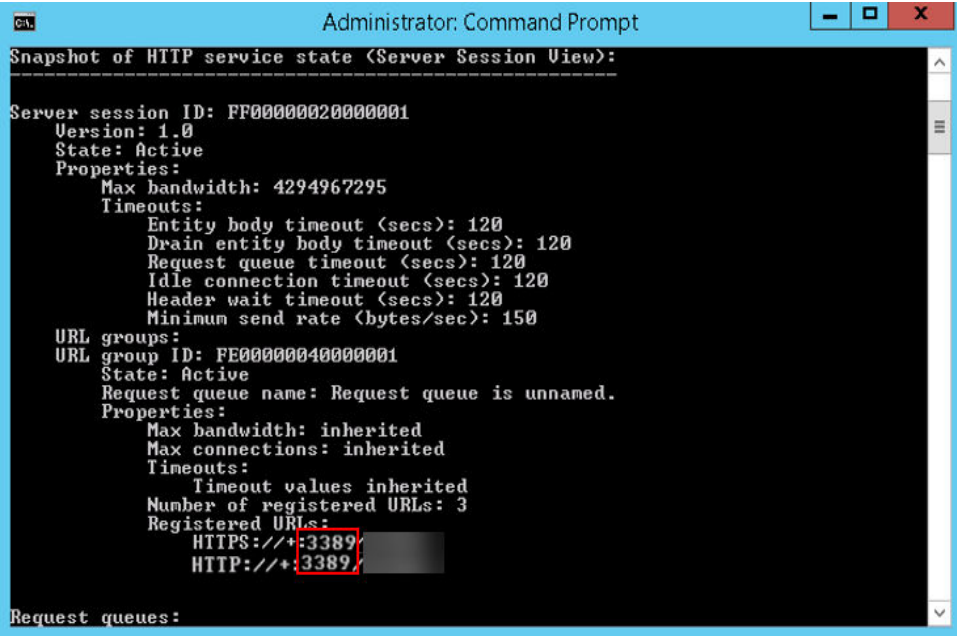
C:\Users\Administrator>
```

As shown in [Figure 13-37](#), port 3389 is used by the process with ID of 4.

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

```
netsh http show servicestate
```

Figure 13-38 Checking System process



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

Request queues:
```

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

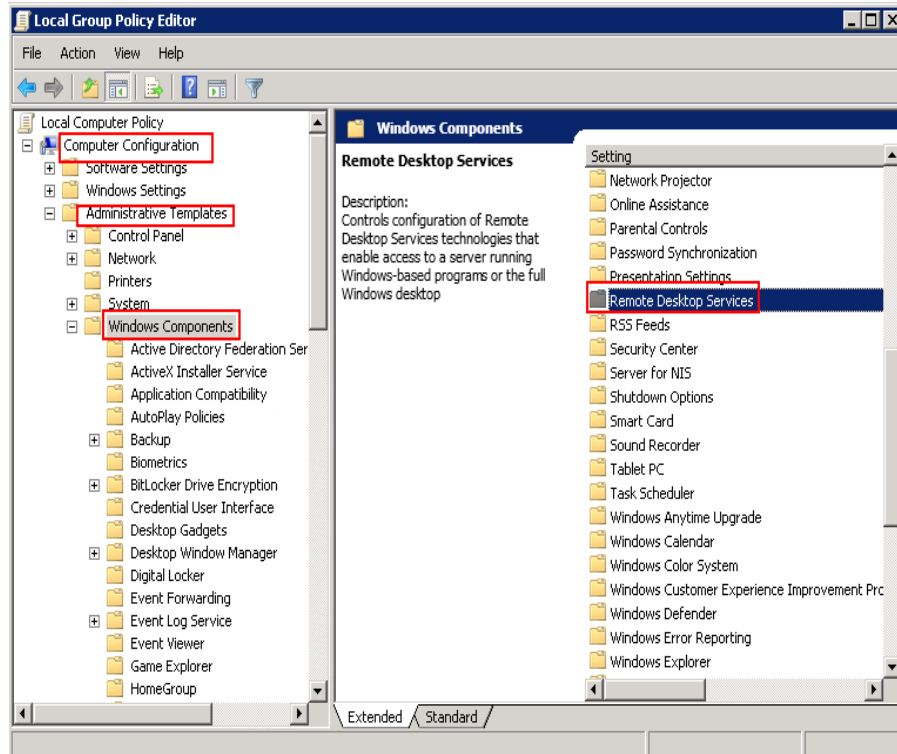
Step 4 If no error occurs during the preceding steps, go to step [Step 5](#) to check whether error 0x1104 is caused by the configuration of Remote Desktop Session Host.

Step 5 Check the remote desktop session host configuration.

1. Log in to the ECS using VNC.
2. Open the `cmd` window and enter `gpedit.msc`.
3. Click **OK** to start Local Group Policy Editor.

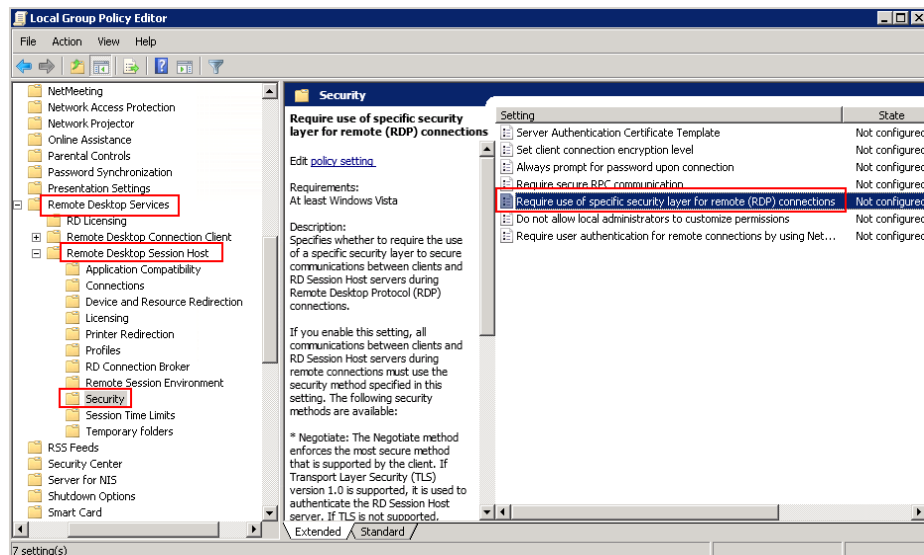
- 4. Choose **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services >**

Figure 13-39 Remote Desktop Services



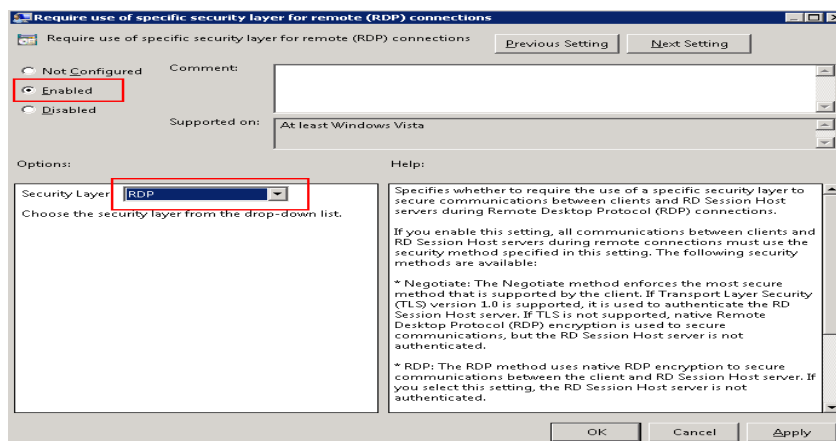
- 5. **Remote Desktop Session Host > Security.**

Figure 13-40 Remote (RDP) Connection requires the use of the specified security layer



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

Figure 13-41 Setting security layer



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

Figure 13-42 Updating the group policy

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

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

C:\Users\Administrator>_
```

----End

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

Symptom

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

Possible Causes

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

Solution

- Step 1** Check system logs.


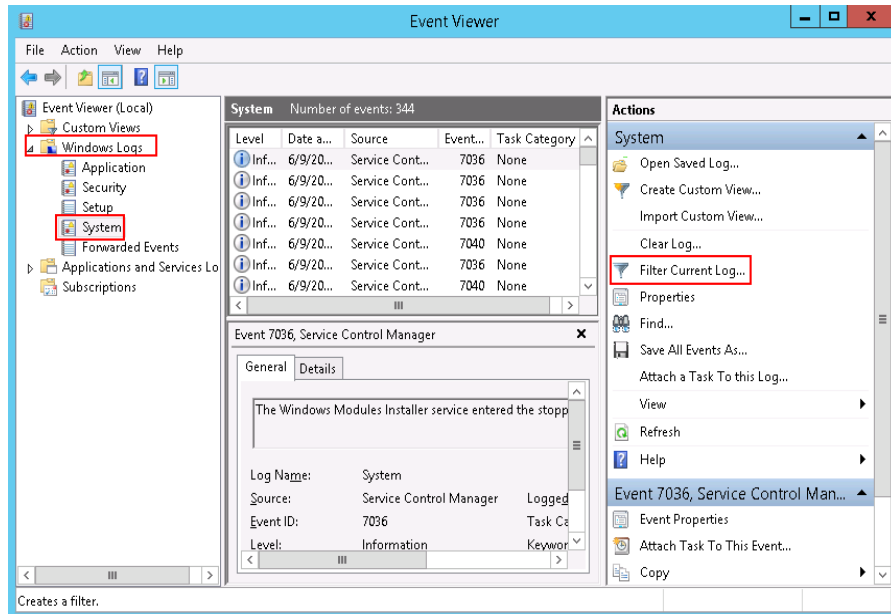
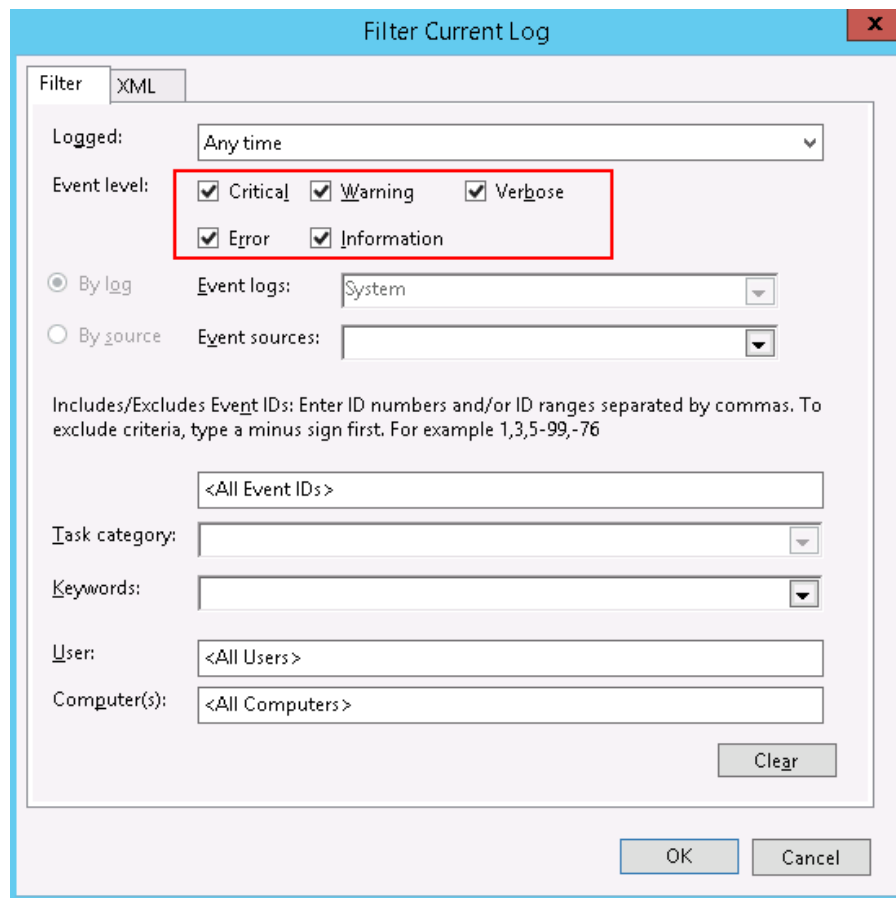
1. Log in to the ECS using VNC.
2. Click  to start the service manager and choose **Administrative Tools > Event Viewer > Windows Logs > System > Filter Current Logs**.

Figure 13-43 Event viewer



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

Figure 13-44 Filtering logs



4. Search for login logs.

Step 2 Check the usage of host resources.

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

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

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

----End

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

Symptom

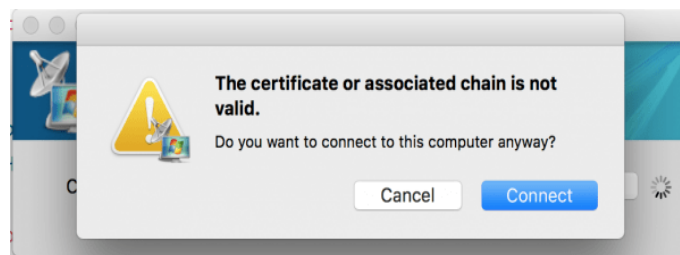
When I use Microsoft Remote Desktop for Mac to remotely access a Windows ECS, the system displays invalid certificate or associated chain.

Figure 13-45 Microsoft Remote Desktop for Mac



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

Figure 13-46 Invalid certificate or associated chain



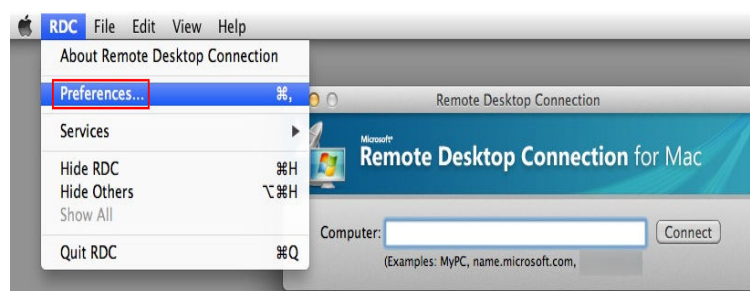
Possible Causes

The group policy setting is incorrect on the ECS.

Procedure

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

Figure 13-47 Preferences setting



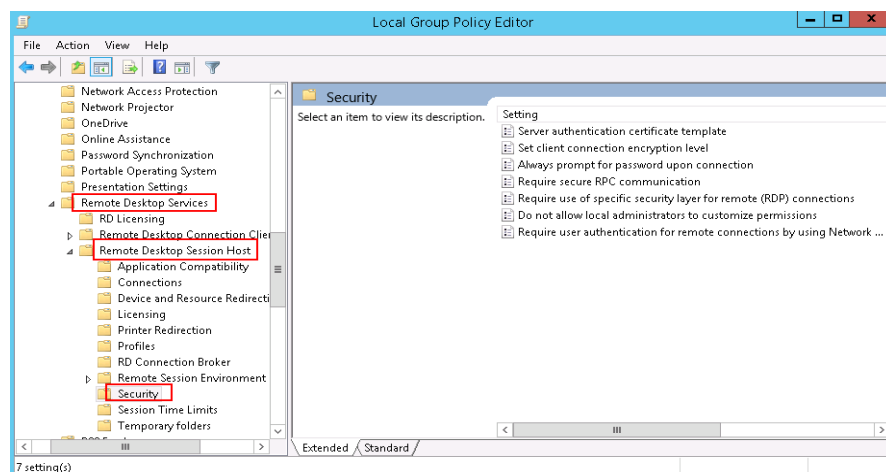
2. Select **Security** and modify the parameter settings according the following figure.

Figure 13-48 Security setting



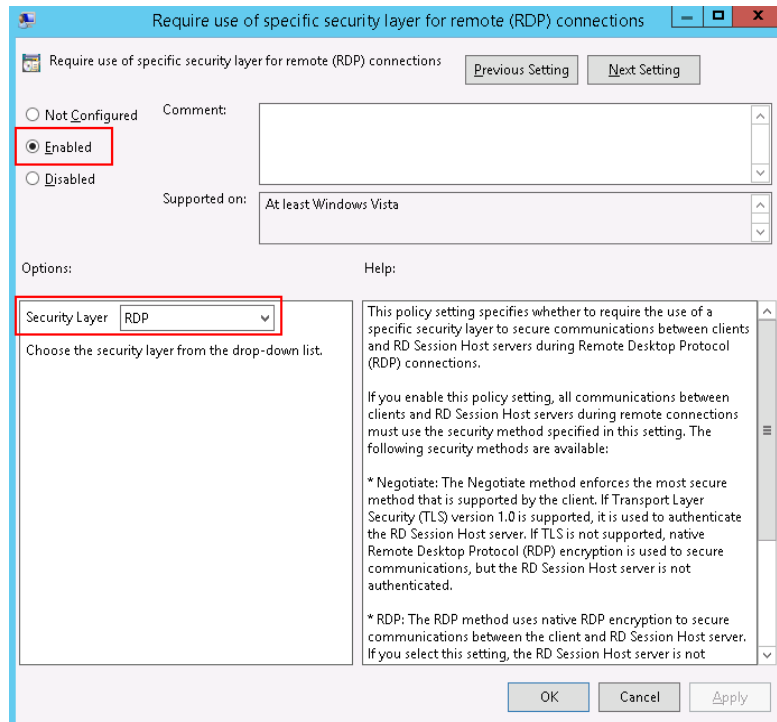
3. Remotely connect to the Windows ECS again. If the error message **Invalid certificate or associated chain** is still displayed, go to 4.
4. Log in to the Windows ECS using VNC.
5. Press **Win+R** to start the **Open** text box.
6. Enter **gpedit.msc** to access the Local Group Policy Editor.
7. In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

Figure 13-49 Remote Desktop Session Host



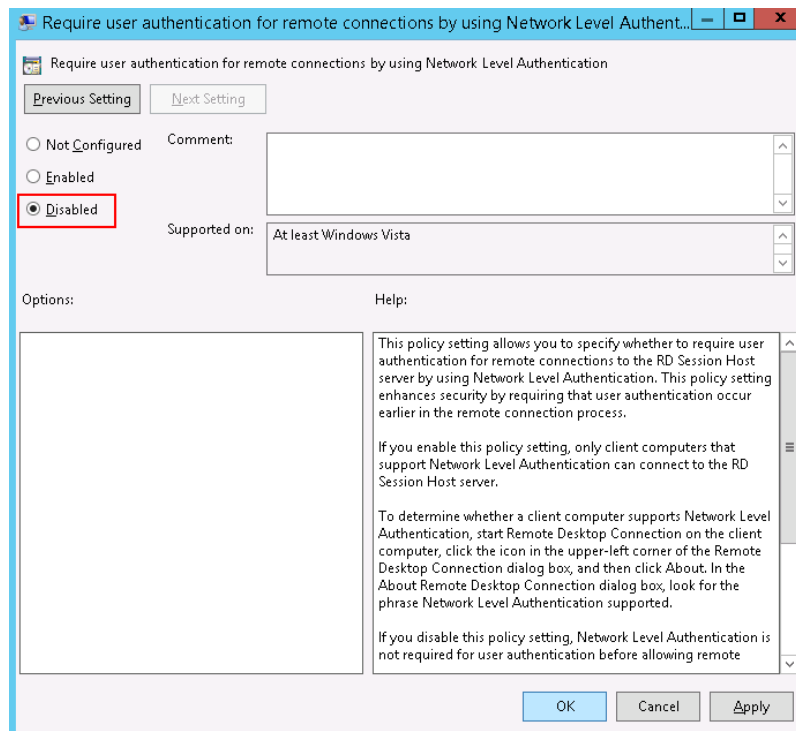
8. Modify the following parameters as prompted:
 - Enable **Require use of specific security layer for remote (RDP) connections**.

Figure 13-50 Require use of specific security layer for remote (RDP) connections



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

Figure 13-51 Remote connection authentication



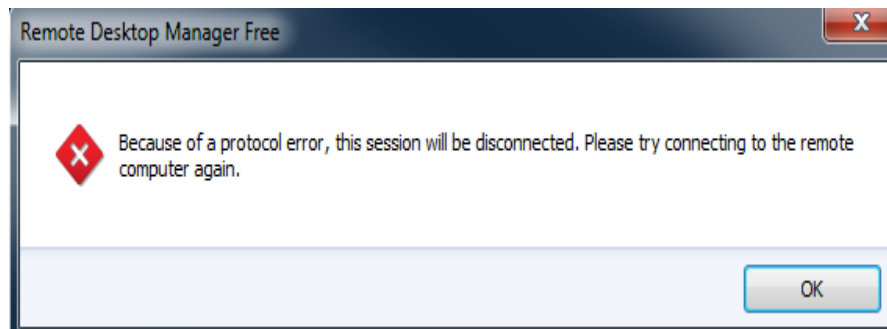
9. Close the group policy editor and restart the ECS.

13.3.22 Troubleshooting Disconnected Session Because of a Protocol Error

Symptom

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

Figure 13-52 Protocol error



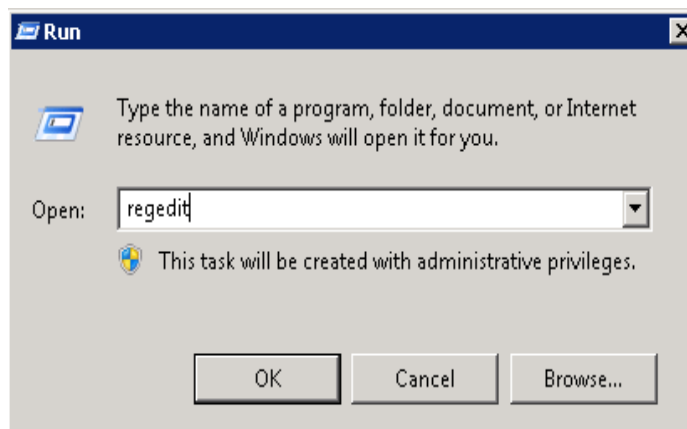
Possible Causes

The registry subkey Certificate is damaged.

Solution

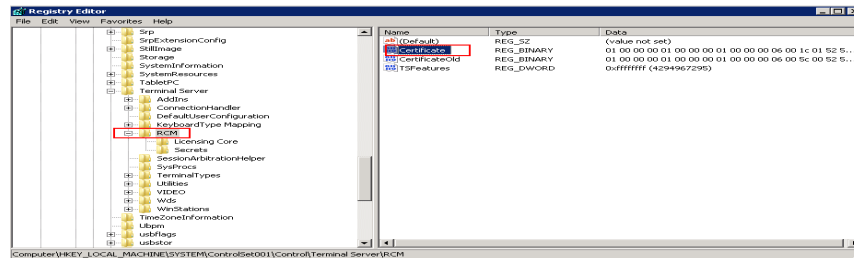
1. In the **Run** dialog box, enter **regedit** and click **OK** to open the registry editor.

Figure 13-53 Opening the registry editor



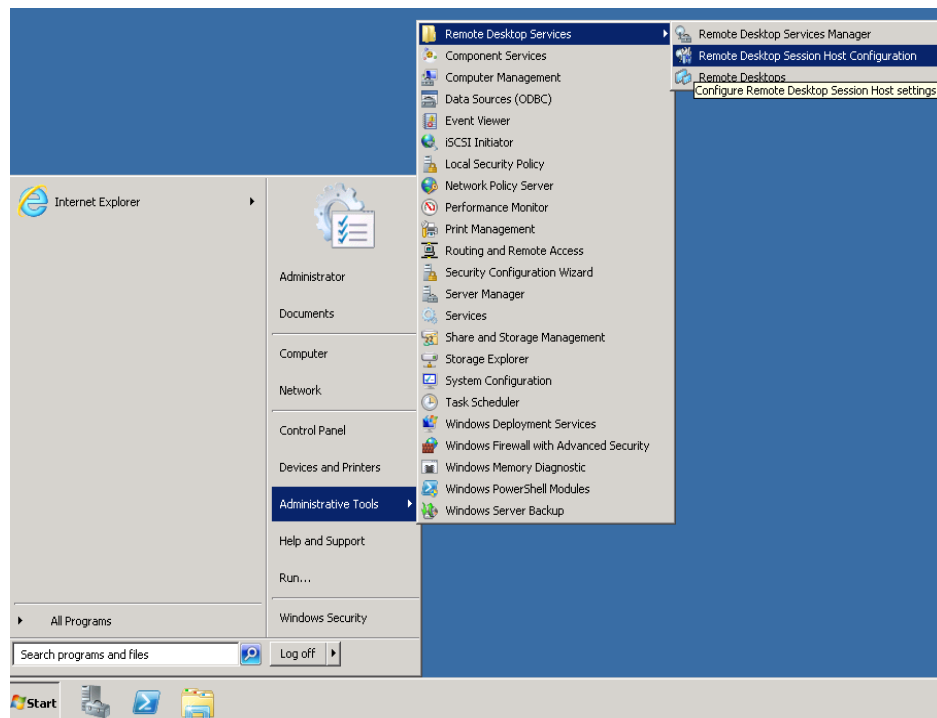
2. Choose **HKEY_LOCAL_MACHINE > SYSTEM > ControlSet001 > Control > Terminal Server > RCM**.
3. Delete **Certificate**.

Figure 13-54 Deleting Certificate



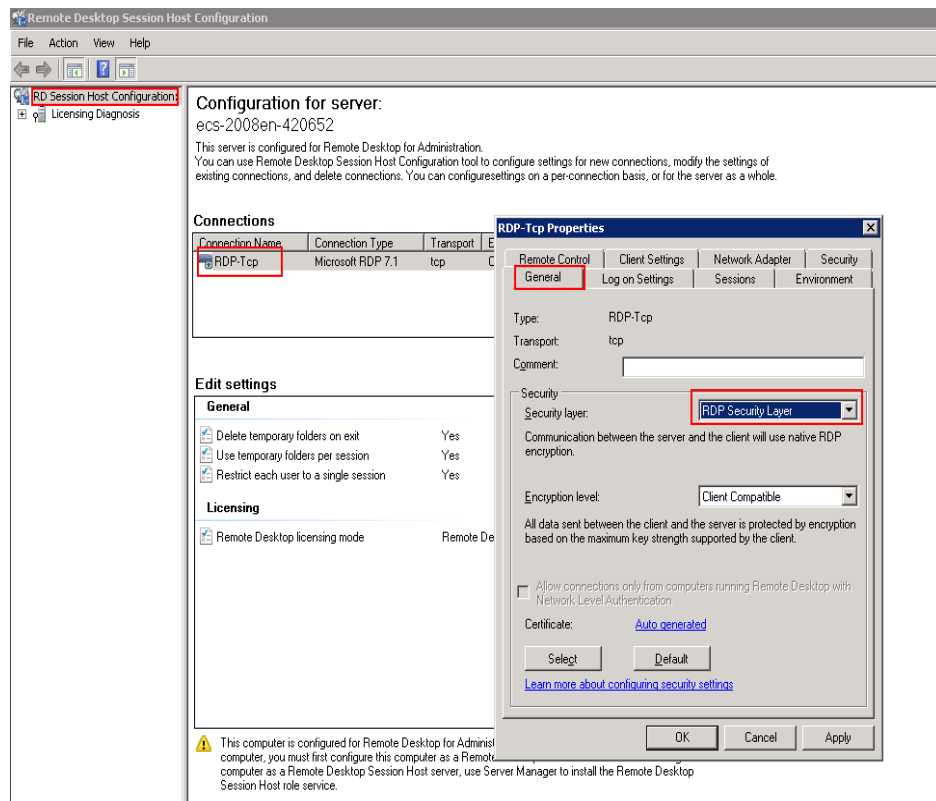
4. Restart the ECS.
5. Choose **Start > Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration**.

Figure 13-55 Opening Remote Desktop Session Host Configuration



6. Right-click **RDP-Tcp** and choose **Properties**. In the displayed dialog box, click **General** and set **Security layer** to **RDP Security Layer**.

Figure 13-56 RDP-Tcp properties

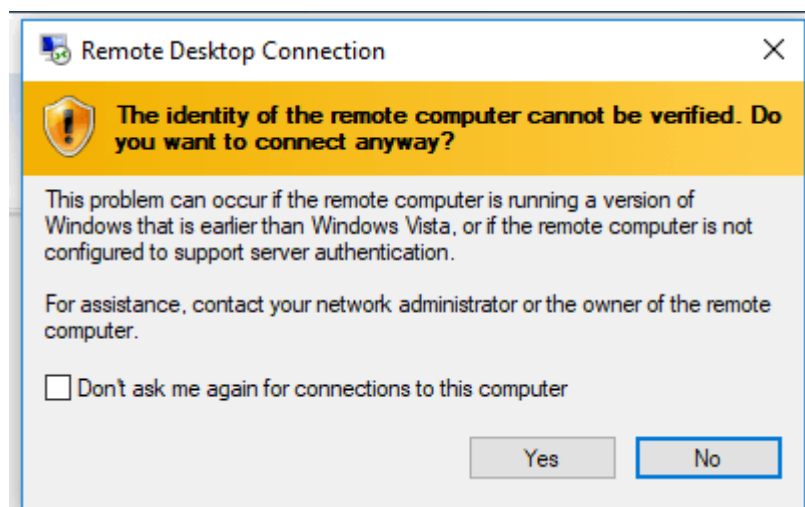


13.3.23 Troubleshooting an Identity Error of the Remote Computer

Symptom

An error message is displayed indicating that the identity of the remote computer cannot be verified. You are required to enter the password and log in again.

Figure 13-57 Protocol error



Possible Causes

Security software installed on the ECS prevents logins from unknown IP addresses.

Solution

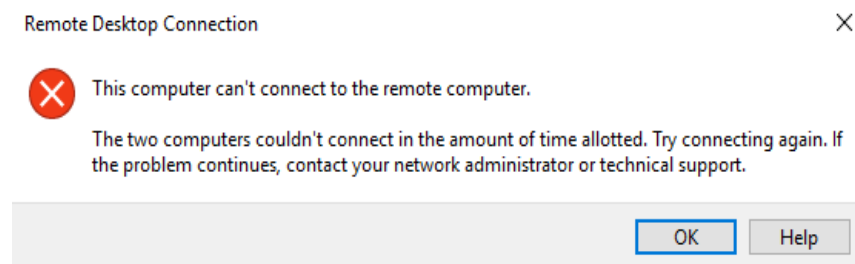
- Uninstall the security software.
- Open the security software and enable the default login mode.

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

Symptom

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

Figure 13-58 Error message



Solution

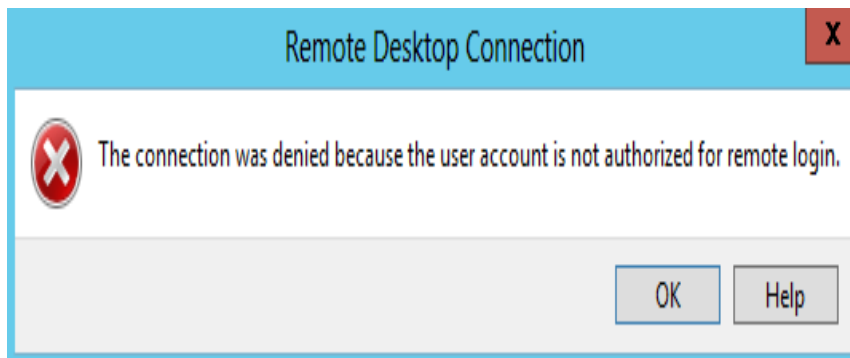
Run `cmd` and then `netsh winsock reset`, restart the ECS as prompted, and try connecting again.

13.3.25 Troubleshooting a Denied Connection Because of Unauthorized User Account

Symptom

An error message is displayed indicating that the connection is denied because the user account is not authorized for remote login.

Figure 13-59 Error message



Possible Causes

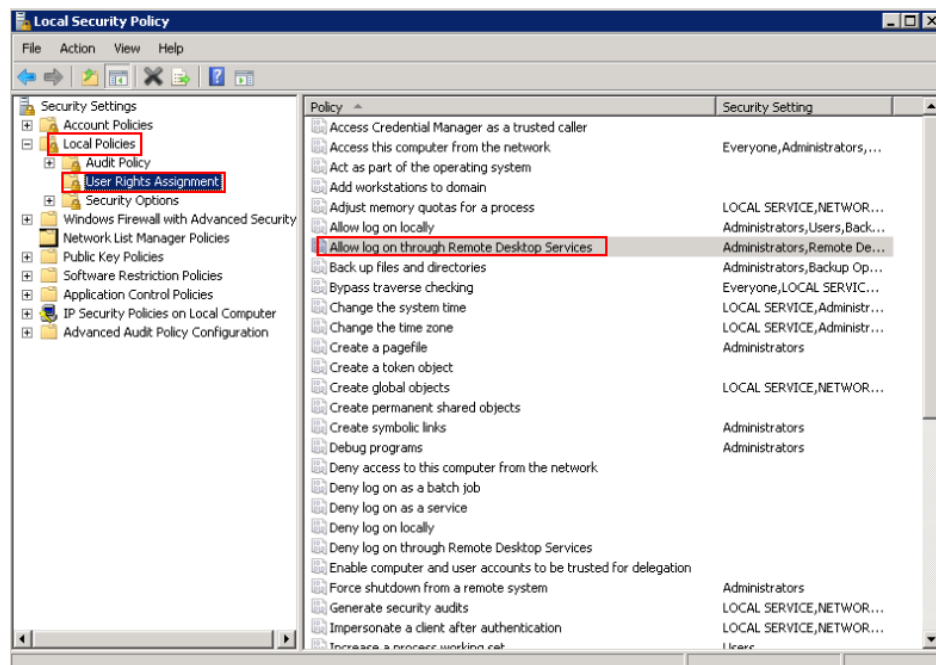
The remote desktop connection permissions have been incorrectly configured.

Solution

Step 1 Check remote desktop permissions on the ECS.

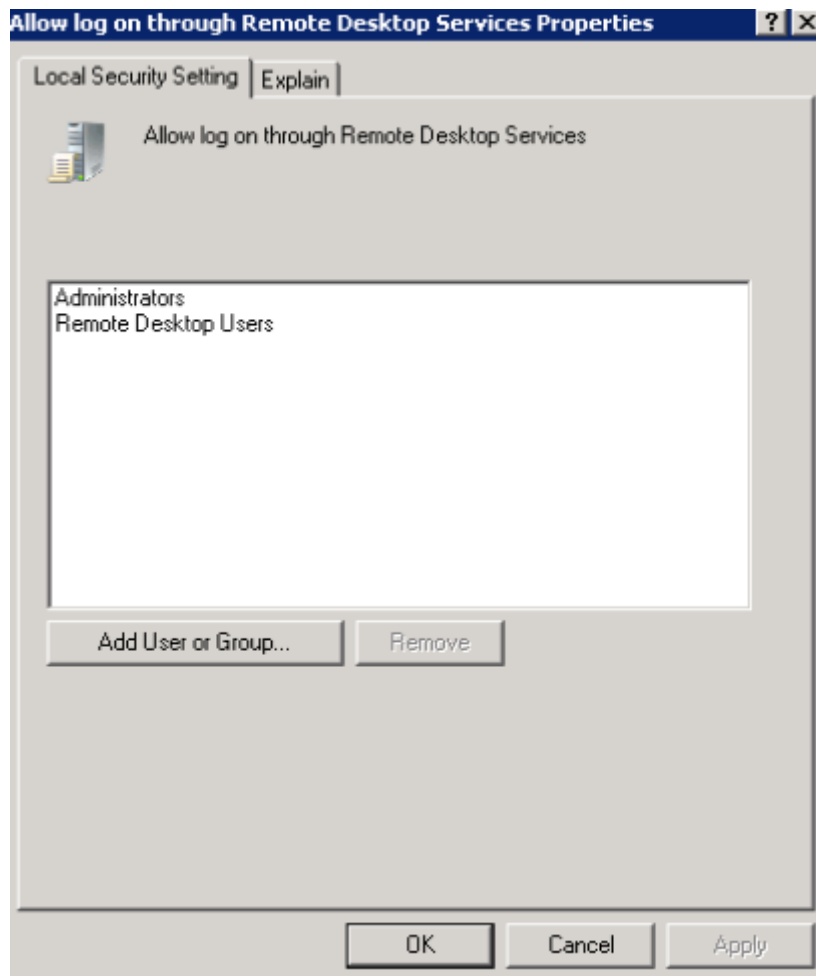
1. In the **Run** dialog box, enter **secpol.msc** and click **OK** to open **Local Security Policy**.
2. Choose **Local Policies > User Rights Assignment > Allow log on through Remote Desktop Services**.

Figure 13-60 Local security policy



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

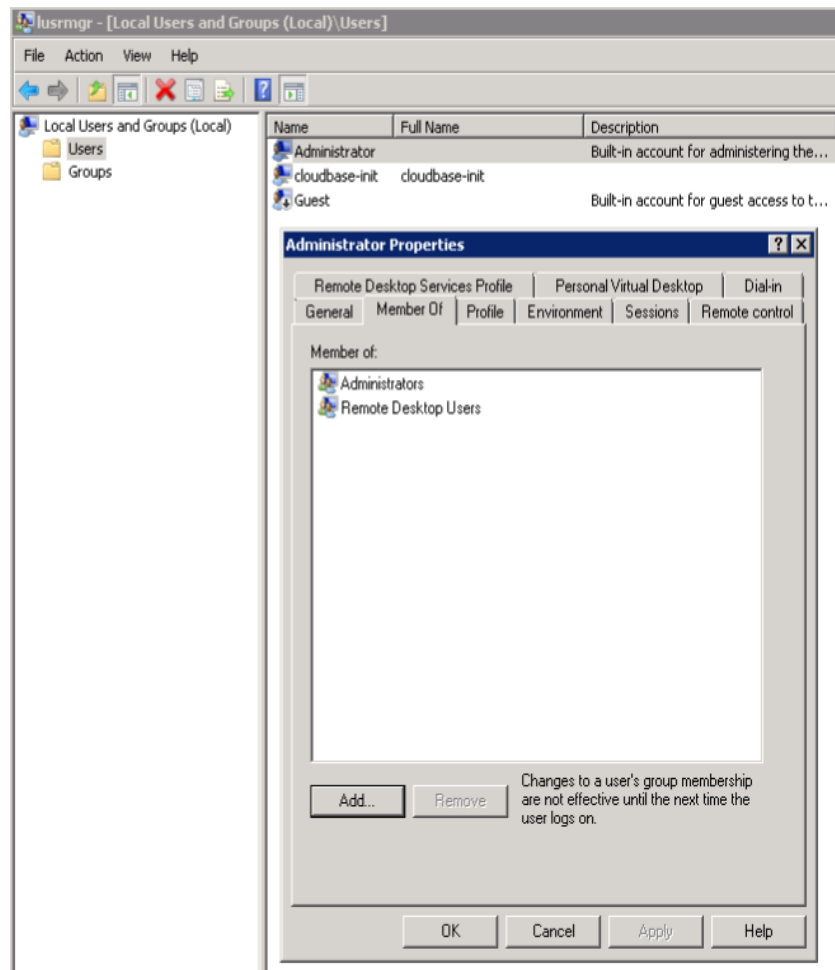
Figure 13-61 Allow log on through Remote Desktop Services properties



Step 2 Check the target user group.

1. Open the **Run** dialog box, enter **lusrmgr.msc**, and click **OK** to open **Local Users and Groups**.
2. Double-click **Users** on the left.
3. Double-click the name of the user that encounters a login error.
4. In the displayed dialog box, click the **Member Of** tab. Ensure that the user belongs to the user group that is assigned with the remote login permission in [Step 2.2](#).

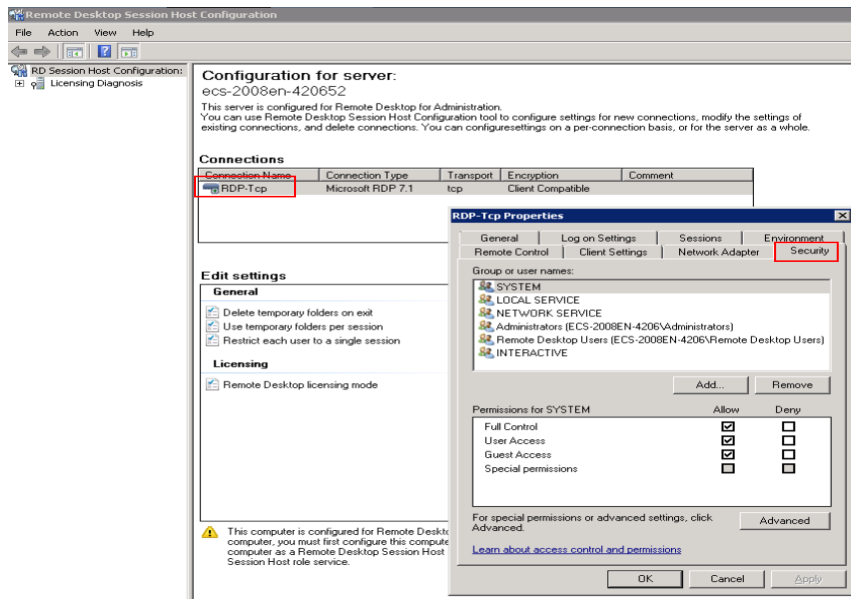
Figure 13-62 Checking the target user group



Step 3 Check the remote desktop session host configuration.

1. In the **Run** dialog box, enter **tsconfig.msc** and click **OK** to open **Remote Desktop Session Host Configuration**.
2. Double-click **RDP-Tcp** or other connections added by a user under **Connections** and click the **Security** tab.

Figure 13-63 Security



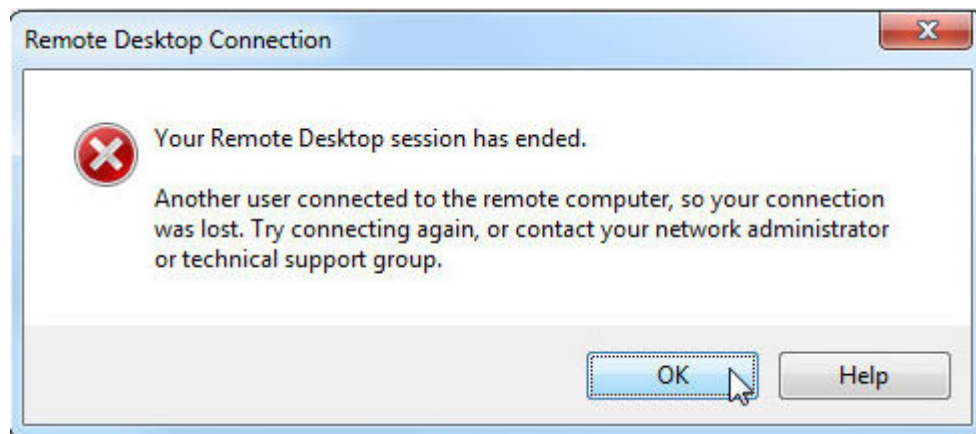
3. Check whether there are user groups or users that have been granted the remote login permission under **Group or user names**.
If not, add required users or groups.
4. Restart the ECS or run the following commands in the CLI to restart the Remote Desktop Services:
`net stop TermService`
`net start TermService`
----End

13.3.26 Troubleshooting a Lost Connection Because of Another User's Login

Symptom

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

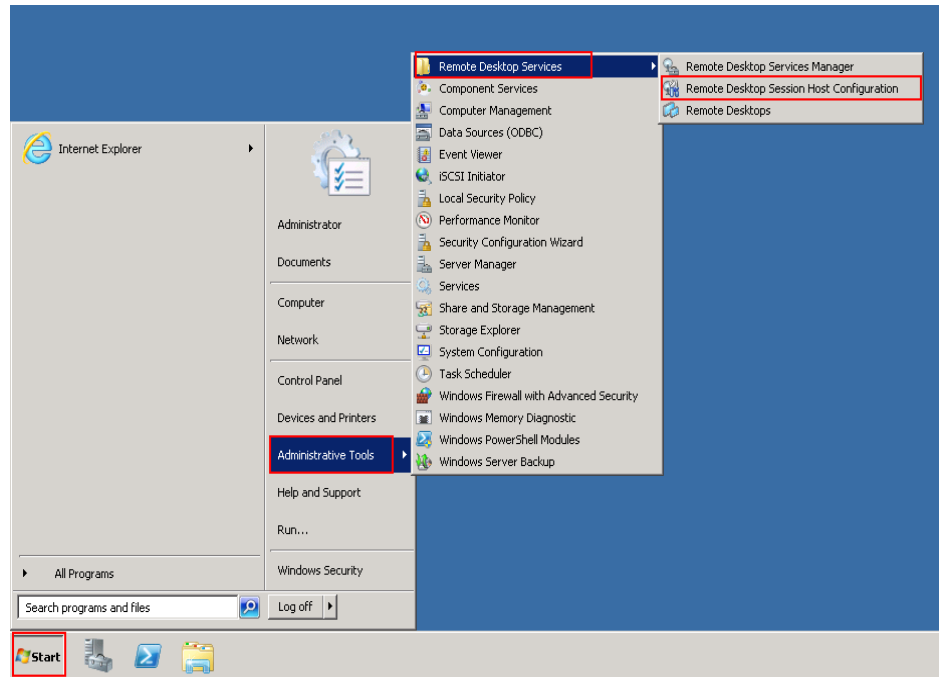
Figure 13-64 Ended remote desktop session



Windows Server 2008

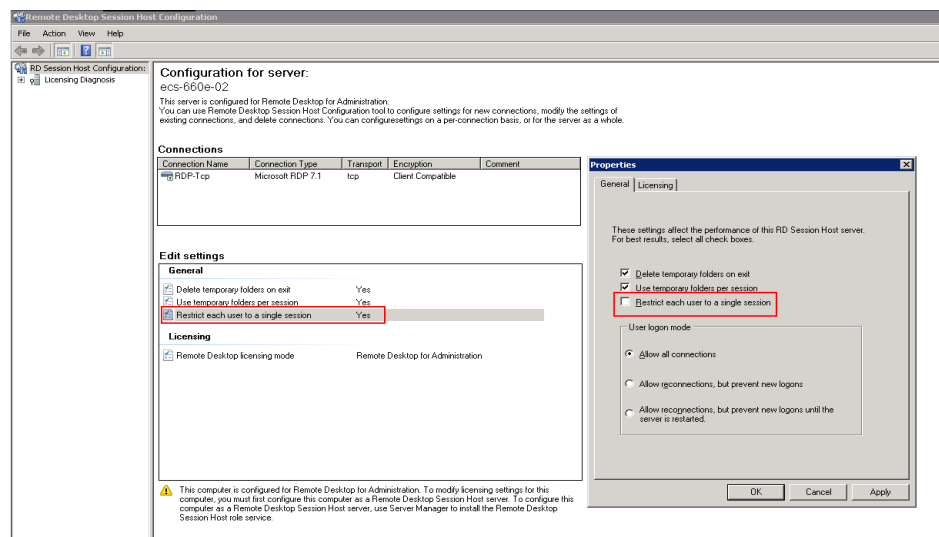
1. Choose **Start > Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration**.

Figure 13-65 Remote Desktop Session Host Configuration



2. Double-click **Restrict each user to a single session** and deselect **Restrict each user to a single session**, and click **OK**.

Figure 13-66 Modifying the configuration

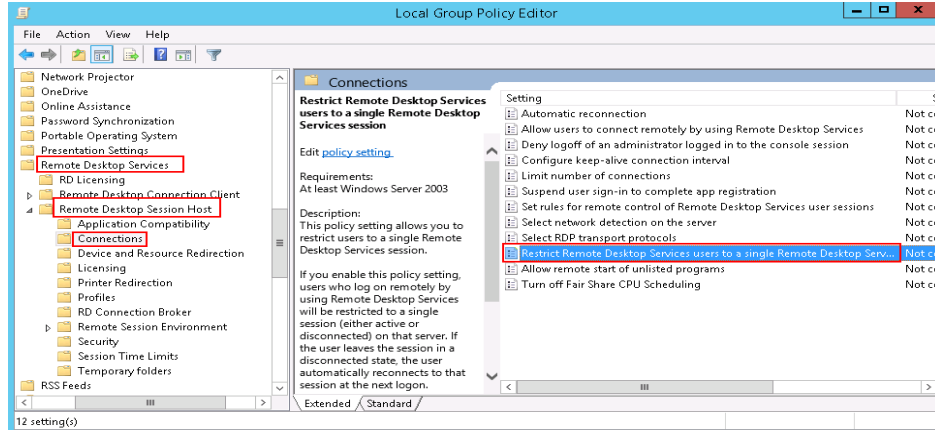


Windows Server 2012

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

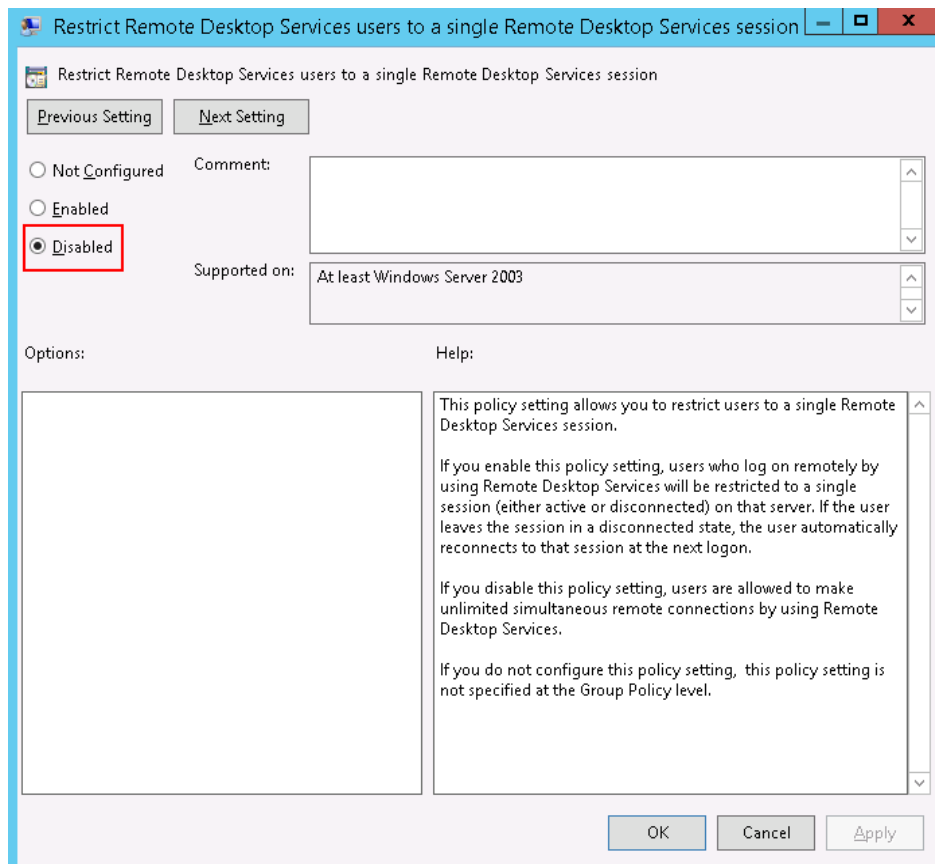
2. Choose **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections**.

Figure 13-67 Connections



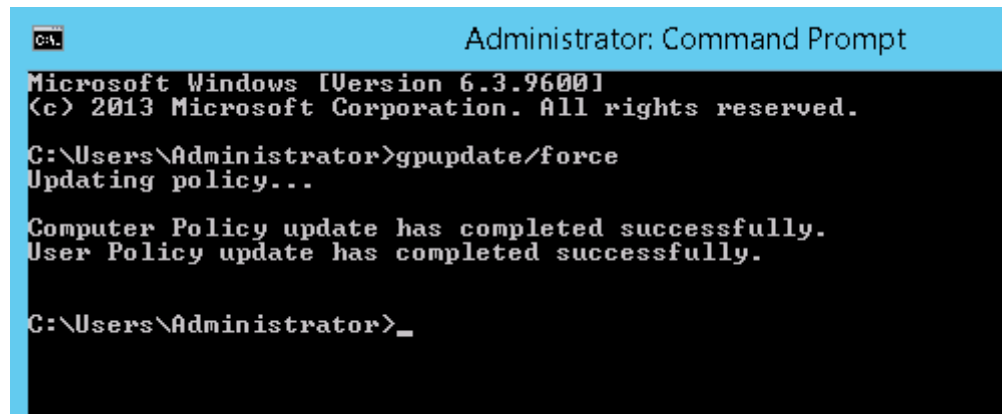
3. Double-click **Restrict Remote Desktop Services users to a single Remote Desktop Services session**, change the value to **Disabled**, and click **OK**.

Figure 13-68 Modifying the configuration



4. Run **gpupdate/force** to update the group policy.

Figure 13-69 Updating the group policy

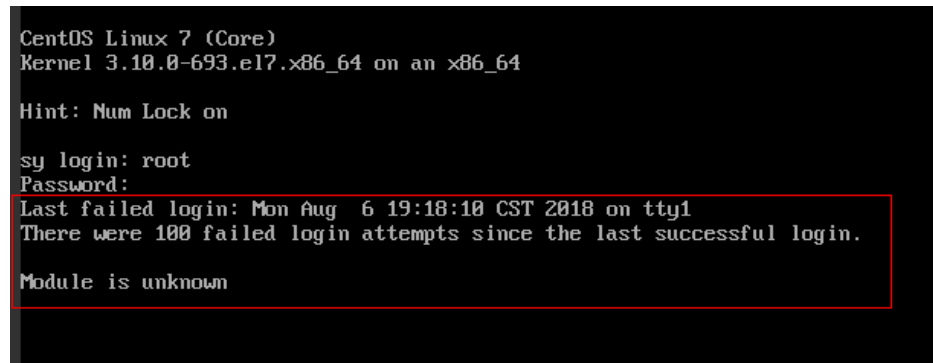


13.3.27 What Should I Do If Error Message "Module is unknown" Is Displayed When I Remotely Log In to a Linux ECS?

Symptom

When I attempted to remotely log in to a Linux ECS, the system displayed error Message "Module is unknown".

Figure 13-70 Module is unknown



NOTE

- To resolve this issue, you are required to restart the ECS and enter the rescue mode.
- Restarting the ECS may interrupt services. Exercise caution when performing this operation.

Root Cause

The file in the `/etc/pam.d/` directory was modified by mistake.

Solution

1. Enter the single-user mode.
The following uses CentOS 7 as an example:

- a. Restart the ECS and click **Remote Login**.
- b. Press the up arrow key to prevent automatic system startup. When the kernels are displayed, press **e** to enter the editing mode.

Figure 13-71 Entering the kernel editing mode

```
CentOS Linux (3.10.0-693.11.1.el7.x86_64) ? (Core)
CentOS Linux (3.10.0-693.el7.x86_64) ? (Core)
CentOS Linux (0-rescue-fd73dfebf69a4e4183fd3f86ccc29526) ? (Core)
```

NOTE

The grub file is encrypted by Euler images by default. Before entering the edit mode, you need to contact customer service to obtain username and password.

- c. Locate the row containing **linux16** and delete undesired parameters.
- d. Change **ro** to **rw** for mounting the root partition with read-write permissions.
- e. Add **rd.break** and press **Ctrl+X**.

Figure 13-72 Before the modification

```
insmod ext2
set root='hd0,msdos1'
if [ x${feature_platform_search_hint} = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1' b13ee9c\
8-0ef0-4159-9b90-fc47bde0d464
else
  search --no-floppy --fs-uuid --set=root b13ee9c8-0ef0-4159-9b90-fc47\
bde0d464
fi
linux16 /boot/vmlinuz-3.10.0-327.62.59.83.h162.x86_64 root=UUID=b13ee9\
c8-0ef0-4159-9b90-fc47bde0d464 ro crash_kexec_post_notifiers softlockup_panic=\
1 panic=3 reserve_kbox_mem=16M nmi_watchdog=1 rd.shell=0 net.ifnames=0 spectre\
_v2=off nopti noibrs noibpb crashkernel=auto LANG=en_US.UTF-8
initrd16 /boot/initramfs-3.10.0-327.62.59.83.h162.x86_64.img
```

Figure 13-73 After the modification

```
insmod ext2
set root='hd0,msdos1'
if [ x${feature_platform_search_hint} = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1' b13ee9c\
8-0ef0-4159-9b90-fc47bde0d464
else
  search --no-floppy --fs-uuid --set=root b13ee9c8-0ef0-4159-9b90-fc47\
bde0d464
fi
linux16 /boot/vmlinuz-3.10.0-327.62.59.83.h162.x86_64 root=UUID=b13ee9\
c8-0ef0-4159-9b90-fc47bde0d464 rw rd.break
initrd16 /boot/initramfs-3.10.0-327.62.59.83.h162.x86_64.img
```

- f. Run the following command to go to the **/sysroot** directory:
chroot /sysroot
2. Run the following command to view the system log for error files:
grep Module /var/log/messages

Figure 13-74 System log

```
Aug 6 18:08:09 sy login: pam_succeed_if(login:auth): requirement "uid >= 1000" not met by user "root"
Aug 6 18:08:11 sy login: FAILED LOGIN 1 FROM tty1 FOR root, Authentication failure
Aug 6 18:08:15 sy login: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Aug 6 18:08:15 sy login: Module is unknown
Aug 6 18:18:41 sy login: PAM unable to dlopen(/lib/security/pam_limits.so): /lib/security/pam_limits.so: cannot open shared object file: No such file or directory
Aug 6 18:18:41 sy login: PAM adding faulty module: /lib/security/pam_limits.so
Aug 6 18:18:44 sy login: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Aug 6 18:18:44 sy login: Module is unknown
```

3. Comment out or modify the error line in the error files displayed in the system log.

`vi /etc/pam.d/login`

Figure 13-75 Modifying the error information

```
session required pam_selinux.so open
session required pam_namespace.so
session optional pam_keyinit.so force revoke
session include system-auth
session include postlogin
-session optional pam_ck_connector.so
# session required /lib/security/pam_limits.so
```

4. Restart the ECS and try to log in to it again.

 NOTE

- To view the modification records and check whether the modification is caused by misoperations, run the following command:

`vi /root/.bash_history`

Search for the keyword `vi` or `login`.

- Do not modify the files in the `/etc/pam.d/` directory. Run the following command for details about pam:

`man pam.d`

13.3.28 What Should I Do If Error Message "Permission denied" Is Displayed When I Remotely Log In to a Linux ECS?

Symptom

When I attempted to remotely log in to a Linux ECS, the system displayed error Message "Permission denied".

Figure 13-76 Permission denied

```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.11.1.el7.x86_64 on an x86_64

ecs-ams-03 login: :
Password:
Permission denied
_
```

NOTE

- To resolve this issue, you are required to restart the ECS and enter the rescue mode.
- Restarting the ECS may interrupt services. Exercise caution when performing this operation.

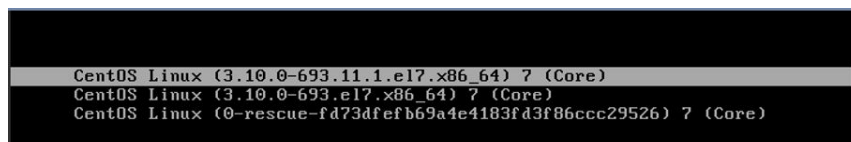
Root Cause

The **nofile** parameter in **/etc/security/limits.conf** is used to set the maximum number of files that can be opened in the system. If the value is greater than the **fs.nr_open** value (**1048576** by default) set in **PermissionDenied.png**, a login verification error will occur, leading to "Permission denied".

Solution

1. Enter the single-user mode.
The following uses CentOS 7 as an example:
 - a. Restart the ECS and click **Remote Login**.
 - b. Press the up arrow key to prevent automatic system startup. When the kernels are displayed, press **e** to enter the editing mode.

Figure 13-77 Entering the kernel editing mode



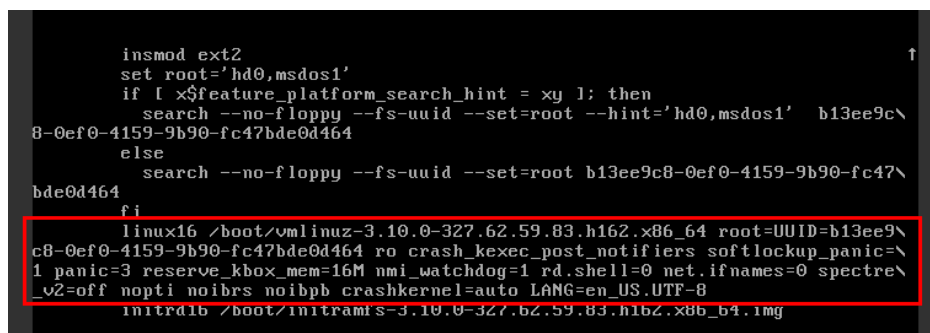
```
CentOS Linux (3.10.0-693.11.1.el7.x86_64) ? (Core)
CentOS Linux (3.10.0-693.el7.x86_64) ? (Core)
CentOS Linux (0-rescue-fd73dfefb69a4e4183fd3f86ccc29526) ? (Core)
```

NOTE

The grub file is encrypted by Euler images by default. Before entering the edit mode, you need to contact customer service to obtain username and password.

- c. Locate the row containing **linux16** and delete undesired parameters.
- d. Change **ro** to **rw** for mounting the root partition with read-write permissions.
- e. Add **rd.break** and press **Ctrl+X**.

Figure 13-78 Before the modification



```
insmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1' b13ee9c\
8-0ef0-4159-9b90-fc47bde0d464
else
  search --no-floppy --fs-uuid --set=root b13ee9c8-0ef0-4159-9b90-fc47\
bde0d464
fi
linux16 /boot/vmlinuz-3.10.0-327.62.59.83.h162.x86_64 root=UUID=b13ee9\
c8-0ef0-4159-9b90-fc47bde0d464 ro crash_kexec_post_notifiers softlockup_panic=\
1 panic=3 reserve_kbox_mem=16M nmi_watchdog=1 rd.shell=0 net.ifnames=0 spectre\
_v2=off nopti noibrs noibpb crashkernel=auto LANG=en_US.UTF-8
initrd16 /boot/initramfs-3.10.0-327.62.59.83.h162.x86_64.img
```

Figure 13-79 After the modification

```
insmod ext2
set root='hd0,msdos1'
if [ x${feature_platform_search_hint} = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1' b13ee9c\
8-0ef0-4159-9b90-fc47bde0d464
else
  search --no-floppy --fs-uuid --set=root b13ee9c8-0ef0-4159-9b90-fc47\
bde0d464
fi
linux16 /boot/vmlinuz-3.10.0-327.62.59.83.h162.x86_64 root=UUID=b13ee9\
c8-0ef0-4159-9b90-fc47bde0d464 rw rd.break
initrd16 /boot/initramfs-3.10.0-327.62.59.83.h162.x86_64.img
```

f. Run the following command to go to the `/sysroot` directory:

```
# chroot /sysroot
```

2. Run the following command to view the `fs.nr_open` value:

```
sysctl fs.nr_open
```

3. Change the `nofile` value in `/etc/security/limits.conf` so that the value is smaller than the `fs.nr_open` value obtained in 2.

```
vi /etc/security/limits.conf
```

NOTE

`limits.conf` is the `pam_limits.so` configuration file of Linux Pluggable Authentication Module (PAM). For more details, run the following command:

```
man limits.conf
```

4. Restart the ECS and try to log in to it again.

13.3.29 What Should I Do If Error Message "read: Connection reset by peer" Is Displayed When I Remotely Log In to a Linux ECS?

Symptom

When I attempted to remotely log in to a Linux ECS, the system displayed error message "read: Connection reset by peer".

Figure 13-80 read: Connection reset by peer

```
debug1: Local version string SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4
ssh_exchange_identification: read: Connection reset by peer
ubuntu@node2:~$ _
```

Possible Causes

- The remote login port is not permitted in the security group.
- The firewall is enabled on the ECS, but the remote login port is blocked by the firewall.

Solution

Perform the following operations for troubleshooting:

- **Check security group rules.**
 - Inbound: Add the remote login port. The default port 22 is used as an example.
 - Outbound: Outbound rules allow network traffic to be out of specified ports.
- **Add a port to the ECS firewall exception.**

The following uses Ubuntu as an example:

- a. Run the following command to view the firewall status:

```
sudo ufw status
```

The following information is displayed:

```
Status: active
```

- b. Add a port to the firewall exception, taking the default port 22 as an example.

```
ufw allow 22
```

```
Rule added
```

```
Rule added (v6)
```

- c. Run following command to check the firewall status again:

```
sudo ufw status
```

```
Status: active
```

```
To Action From
--
22 ALLOW Anywhere
22 (v6) ALLOW Anywhere (v6)
```

Try to remotely log in to the ECS again.

13.3.30 What Should I Do If Error Message "Access denied" Is Displayed When I Remotely Log In to a Linux ECS?

Symptom

When I attempted to remotely log in to a Linux ECS, the system displayed error message "Access denied".

Possible Causes

- Incorrect username or password.
- A policy that denies logins from user **root** is enabled on the SSH server.

Solution

- If the username or password is incorrect
Check the username and password.
- If a policy that denies logins from user **root** is enabled on the SSH server
 - a. Edit the `/etc/ssh/sshd_config` file and check the following settings to ensure that the SSH logins from user **root** are allowed:

```
PermitRootLogin yes
```
 - b. Restart SSH.

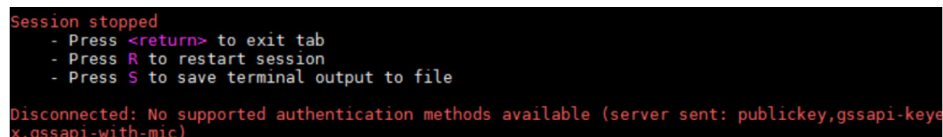
- CentOS 6
`service sshd restart`
- CentOS 7
`systemctl restart sshd`

13.3.31 What Should I Do If Error Message "Disconnected: No supported authentication methods available" Is Displayed When I Remotely Log In to a Linux ECS?

Symptom

When I attempted to remotely log in to a Linux ECS, the system displayed error message "Disconnected: No supported authentication methods available".

Figure 13-81 No supported authentication methods available



```
Session stopped
- Press <return> to exit tab
- Press R to restart session
- Press S to save terminal output to file
Disconnected: No supported authentication methods available (server sent: publickey,gssapi-keyex,gssapi-with-mic)
```

Possible Causes

A policy that denies password-authenticated logins is enabled on the SSH server.

Solution

1. Open the `/etc/ssh/sshd_config` file and check the following settings:
`vi /etc/ssh/sshd_config`
1. Modify the following settings:
Change **PasswordAuthentication no** to **PasswordAuthentication yes**.
Alternatively, delete the comment tag (#) before **PasswordAuthentication yes**.
2. Restart SSH.
 - CentOS 6
`service sshd restart`
 - CentOS 7
`systemctl restart sshd`

13.4 ECS Management

13.4.1 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:
sudo vim /etc/hostname
2. Change the hostname to the new one.
3. Run the following command to save and exit the configuration file:
:wq

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

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

NOTE

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

An example is provided as follows:

HOSTNAME=new_hostname

3. Run the following command to save and exit the configuration file:
:wq

Step 3 Modify the **/etc/cloud/cloud.cfg** configuration file.

1. Run the following command to edit the configuration file:
sudo vim /etc/cloud/cloud.cfg
2. 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:

```
sudo reboot
```

Step 5 Run the following command to check whether the hostname has been changed:

```
sudo hostname
```

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

----End

13.4.2 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 13-2](#) lists the hostnames (obtained by running the **hostname** command) of ECSs created using different images and those displayed after the ECSs are restarted.

Table 13-2 Hostnames of ECSs created from different images

Image	Hostname Before ECS Restart	Hostname After ECS Restart
CentOS 6.8	abc	abc.novalocal
CentOS 7.3	abc.novalocal	abc.novalocal
Ubuntu 16	abc	abc

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 [13.4.1 How Can a Changed Static Hostname Take Effect Permanently?](#)

13.4.3 What Should I Do If the 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.

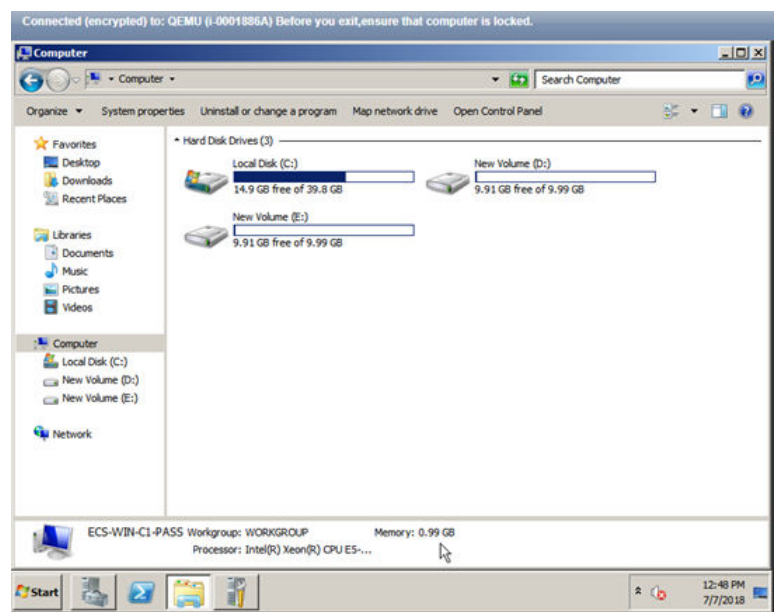
Procedure

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:

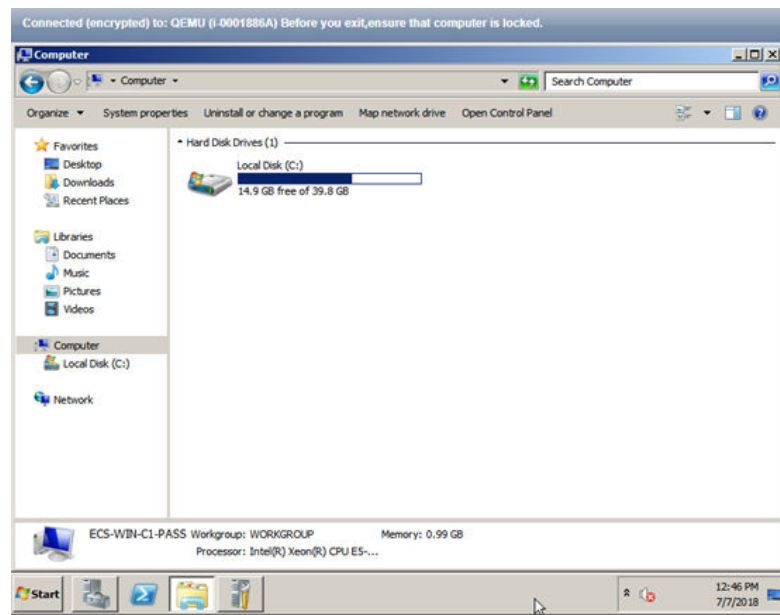
An ECS running Windows Server 2008 has one system disk and two data disks attached before specifications modification.

Figure 13-82 Disk attachment before specifications modification



After the specifications are modified, check disk attachment.

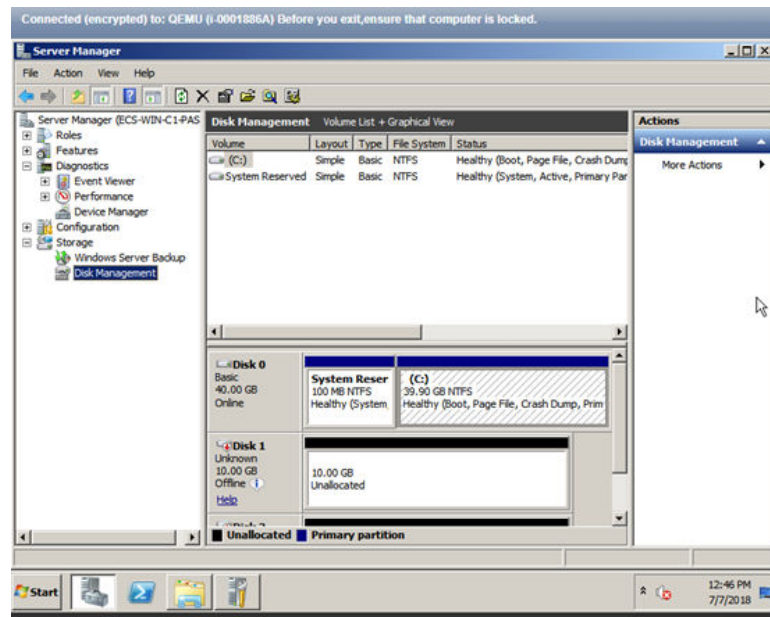
Figure 13-83 Disk attachment after specifications modification



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

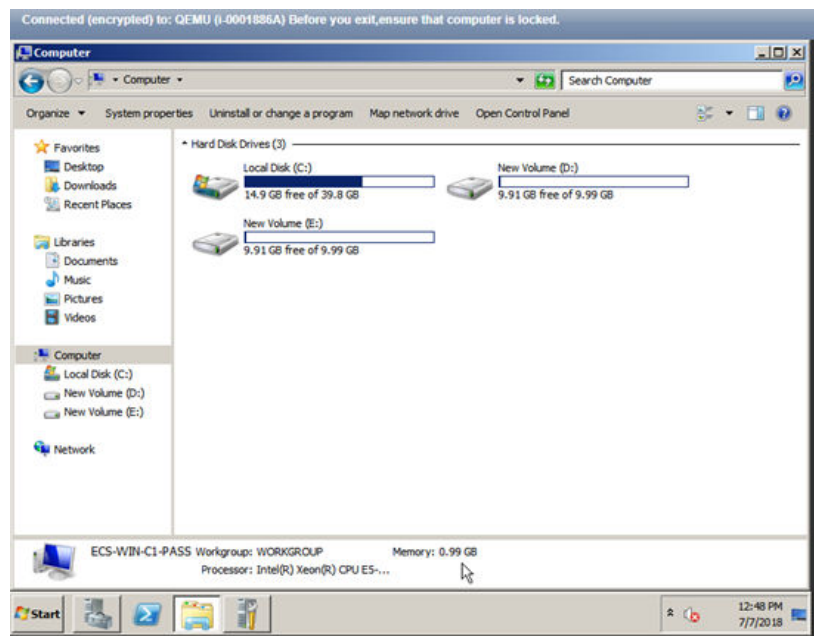
2. Set the affected disks to be online.
 - a. Click **Start** in the task bar. In the displayed **Start** menu, right-click **Computer** and choose **Manage** from the shortcut menu.
The **Server Manager** page is displayed.
 - b. In the navigation pane on the left, choose **Storage > Disk Management**.
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.

Figure 13-84 Making the disk 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.

Figure 13-85 Disk attachment after disk online



13.4.4 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 13-86 Viewing disks attached before specifications modification

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

As shown in [Figure 13-86](#), 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 13-87 Viewing disks attached after specifications modification

```
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# df -h | grep '/dev/'
/dev/vda2    39G  1.4G   35G   4% /
/dev/vda1    976M 146M  764M  16% /boot
```

As shown in [Figure 13-87](#), 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.

NOTICE

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 13-88 Checking the number of disks attached

```
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# mount /dev/vdb1 /mnt/vdb1
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# mount /dev/vdc1 /mnt/vdc1
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]#
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]#
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]#
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]#
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# fdisk -l | grep 'Disk /dev/'
Disk /dev/vda: 42.9 GB, 42949672960 bytes, 83886080 sectors
Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Disk /dev/vdc: 10.7 GB, 10737418240 bytes, 20971520 sectors
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]# df -h | grep '/dev/'
/dev/vda2      39G  1.4G   35G   4% /
/dev/vda1    976M 146M  764M  16% /boot
/dev/vdb1     9.8G  23M   9.2G   1% /mnt/vdb1
/dev/vdc1     9.8G  23M   9.2G   1% /mnt/vdc1
[root@servercf924ffa-da23-4d09-a7e0-416694a68492 ~]#
```

As shown in [Figure 13-88](#), the numbers of disks before and after specifications modification are the same. The disks are `/dev/vda`, `/dev/vdb`, and `/dev/vdc`.

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

Symptom

This section helps you resolve the following issues:

- An error message was displayed on the management console after you performed ECS-related operations.

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 13-3](#).

Table 13-3 Error codes and solution suggestions

Error Code	Message Displayed on the Management Console	Solution Suggestion
Ecs.0000	Request error. Try again later or contact customer service.	Adjust the request structure as directed in <i>Elastic Cloud Server API Reference</i> .
Ecs.0001	The maximum number of ECSs or EVS disks has been reached. Contact the customer service and request an ECS quota increase.	Contact customer service and request an ECS quota increase. NOTE Before requesting for increasing your ECS quota, consider the number of to-be-added ECSs, vCPUs, and memory capacity required.
Ecs.0003	You do not have the permission or your balance is insufficient.	Contact customer service to check your account information.
Ecs.0005	System error. Try again later or contact customer service.	Adjust the request structure as directed in <i>Elastic Cloud Server API Reference</i> .
Ecs.0010	The private IP address is in use. Select an available IP address for ECS creation.	Use an idle IP address for ECS creation.
Ecs.0011	Invalid password. Change the password to make it meet the password complexity requirements, and perform the required operation again.	Input a password that meets password complexity requirements. Then, initial the request again.
Ecs.0012	Insufficient IP addresses in the subnet. Release IP addresses in the subnet or select another subnet for ECS creation.	Release IP addresses in the subnet or select another subnet for ECS creation.
Ecs.0013	Contact customer service and request an EIP quota increase.	Contact customer service and request an EIP quota increase.

Error Code	Message Displayed on the Management Console	Solution Suggestion
Ecs.0015	The disk of this type is not supported by the ECS.	Select a proper disk and attach it to the ECS.
Ecs.0100	Invalid ECS status. Change the status and try again.	Change the ECS status to the desired one and try again.
Ecs.0103	The disk is unavailable.	Change the ECS status to the desired one and try again. If the EVS disk is faulty, contact customer service for troubleshooting.
Ecs.0104	The number of disks to be attached to an ECS exceeds the number allowed.	Detach EVS disks from the ECS before attaching new ones.
Ecs.0105	No system disk found.	Attach the system disk to the ECS and perform the desired operation again.
Ecs.0107	The number of shared disks to be attached to an ECS exceeds the maximum limit.	Detach EVS disks from the ECS before attaching new ones.
Other error codes	Other error messages	Initiate the request again. If the error persists, record the returned error code and contact customer service for troubleshooting.

13.5 OS Management

13.5.1 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.

13.5.2 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 [3.5.3 Changing the OS](#).

13.5.3 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 1 to 2 minutes.

During this process, the ECS is in **Changing OS** state.

13.5.4 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 [3.5.3 Changing the OS](#).

13.5.5 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 1 to 2 minutes.

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

13.5.6 Do ECSs Support GUI?

Windows ECSs are managed through a GUI but Linux ECSs are managed through the CLI. You can configure a GUI if required.

Before installing a GUI on an ECS, ensure that the idle memory is greater than or equal to 2 GB. Otherwise, the GUI installation may fail or the ECS cannot be started after the installation.

13.5.7 How Can I Install a GUI on an ECS Running CentOS 6?

Scenarios

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

Constraints

- Before installing a GUI on an ECS, ensure that the idle memory is greater than or equal to 2 GB. Otherwise, the GUI installation may fail or the ECS cannot be started after the installation.

Procedure

1. Run the following command to obtain the installation component provided by the OS:
yum groupinstall "Desktop"
2. Run the following command to set the default startup level to 5 (GUI):
sed -i 's/id:3:initdefault:/id:5:initdefault:/' /etc/inittab
3. Access GUI and run the following command:
startx

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

Scenarios

This section describes how to install a GUI on an ECS running CentOS 7 series, EulerOS 2.2 or earlier.

Constraints

- EulerOS 2.3 and later versions do not support GUI.
- Before installing a GUI on an ECS, ensure that the idle memory is greater than or equal to 2 GB. Otherwise, the GUI installation may fail or the ECS cannot be started after the installation.

Procedure

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

NOTE

If the following message is displayed after the installation is complete:

```
Failed : python -urllib3.noarch 0:1.10.2-7.e17
```

Run the following command:

```
mv /usr/lib/python2.7/site-packages/urllib3/packages/  
ssl_match_hostname /usr/lib/python2.7/site-packages/urllib3/packages/  
ssl_match_hostname.bak
```

```
yum install python-urllib3 -y
```

2. After the installation is complete, run the following command to set the default startup level to **graphical.target**:
systemctl set-default graphical.target
3. Run the following command to start **graphical.target**:
systemctl start graphical.target
4. Set the language, time zone, username, and password as prompted.

13.5.9 How Can I Install a 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.

- Before installing a GUI on an ECS, ensure that the idle memory is greater than or equal to 2 GB. Otherwise, the GUI installation may fail or the ECS cannot be started after the installation.

Procedure

1. Log in to the ECS and install the GUI desktop component.
 - a. Run the following command to update the software library:
apt-get update
 - b. Run the following command to install the Ubuntu GUI desktop component:
apt-get install xubuntu-desktop

During the installation process, you are required to manually confirm the operation twice. Press **y**.

2. Run the following command to edit the **root/.profile** file:

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:

```
# ~/.profile: executed by Bourne-compatible login shells.

if [ "$BASH" ]; then
  if [ -f ~/.bashrc ]; then
    . ~/.bashrc
  fi
fi
tty -s && mesg n || true
```

3. Restart the ECS. Then, you can log in to the GUI as user **root**.

13.6 File Transferring

13.6.1 How Can I Upload a File to an ECS?

Windows

- Through a transmission tool
Install a data transfer tool on both the local computer and the Windows ECS to transmit data.
- (Recommended) 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.
For details, see [13.6.2 How Can I Transfer Files from a Local Windows Computer to a Windows ECS?](#)
- Through an FTP site
Before transferring files from a local computer to a Windows ECS, set up an FTP site on the ECS and install FileZilla on the local computer. This transmission method is widely used.

For details, see [13.6.6 How Can I Use FTP to Transfer Files from a Local Windows Computer to a Windows or Linux ECS?](#)

Linux

- From a local Windows computer
Use WinSCP to transfer the files to the Linux ECS. For details, see [13.6.3 How Can I Use WinSCP to Transfer Files from a Local Windows Computer to a Linux ECS?](#)
Before transferring files from a local computer to a Linux ECS, set up an FTP site on the ECS and install FileZilla on the local computer. For details, see [13.6.6 How Can I Use FTP to Transfer Files from a Local Windows Computer to a Windows or Linux ECS?](#)
- From a local Linux computer
Use SCP to transfer the files to the Linux ECS. For details, see [13.6.4 How Can I Use SCP to Transfer Files Between a Local Linux Computer and a Linux ECS?](#)
Use SFTP to transfer the files to the Linux ECS. For details, see [13.6.5 How Can I Use SFTP to Transfer Files Between a Local Linux Computer and a Linux ECS?](#)
Use FTP to transfer the files to the Linux ECS. For details, see [13.6.7 How Can I Use FTP to Transfer Files Between a Local Linux Computer and a Linux ECS?](#)

Does an ECS Support FTP-based File Transferring by Default?

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

13.6.2 How Can I Transfer Files from a Local Windows Computer to a Windows ECS?

Scenarios

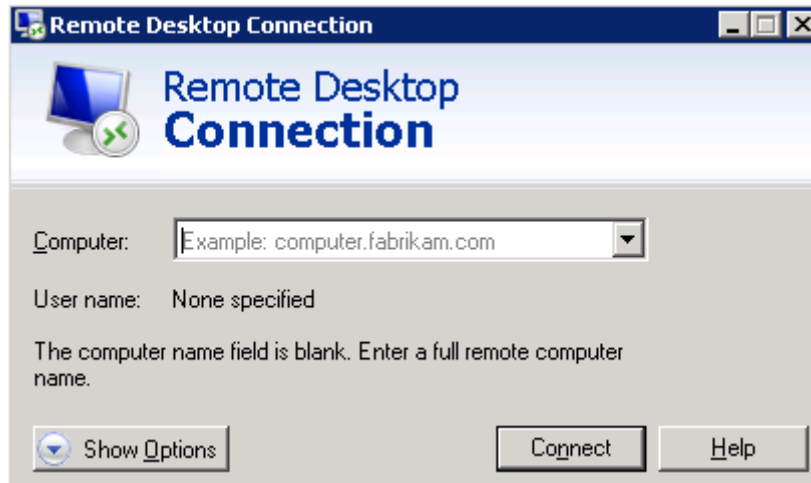
Files are generally transferred to Windows ECSs through MSTSC-based remote desktop connection. This section describes how to transfer files from a local Windows computer to a Windows ECS through remote desktop connection.

Prerequisites

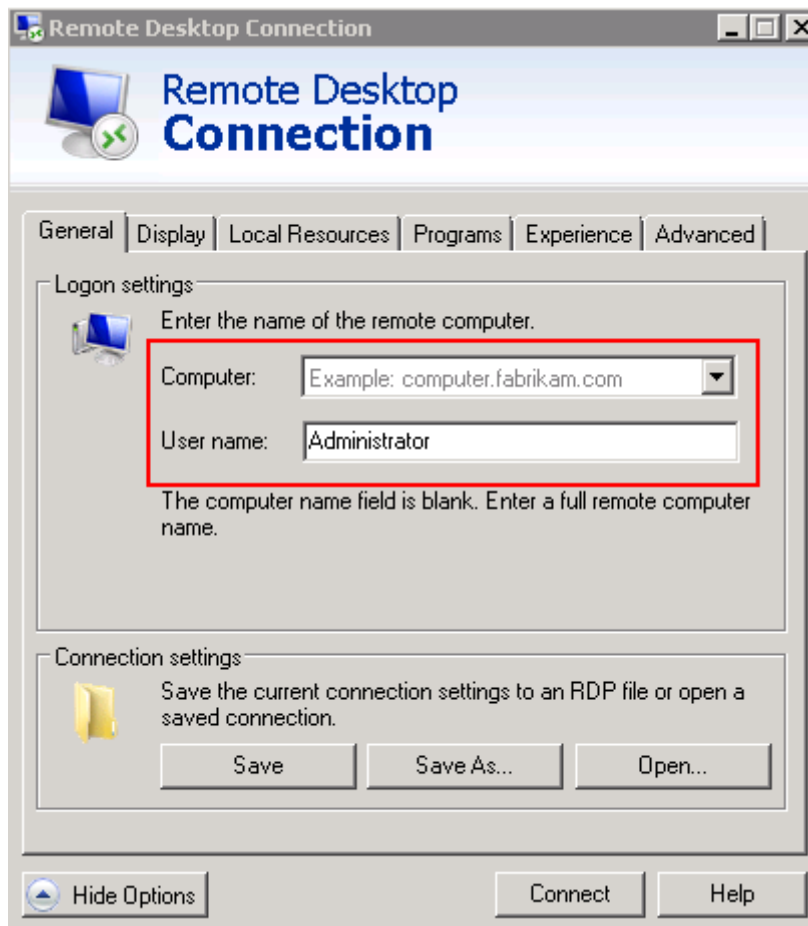
The Windows ECS can access the Internet.

Solution

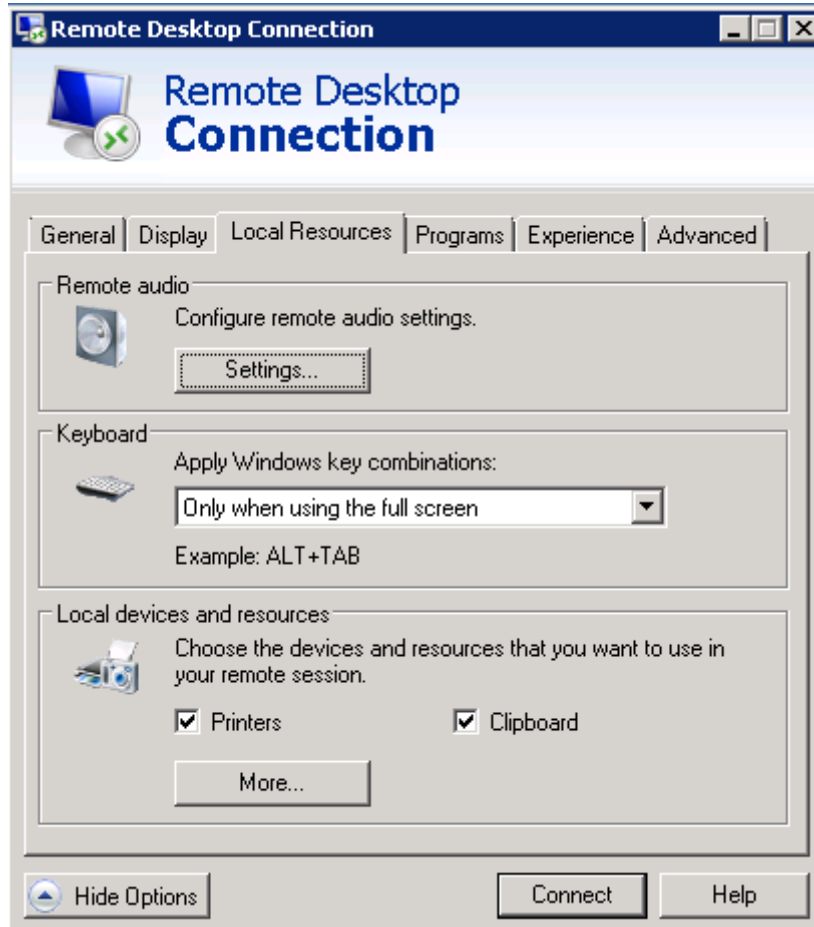
1. On the local Windows computer, click **Start**. In the **Search programs and files** text box, enter **mstsc**.
The **Remote Desktop Connection** window is displayed.
2. Click **Options**.



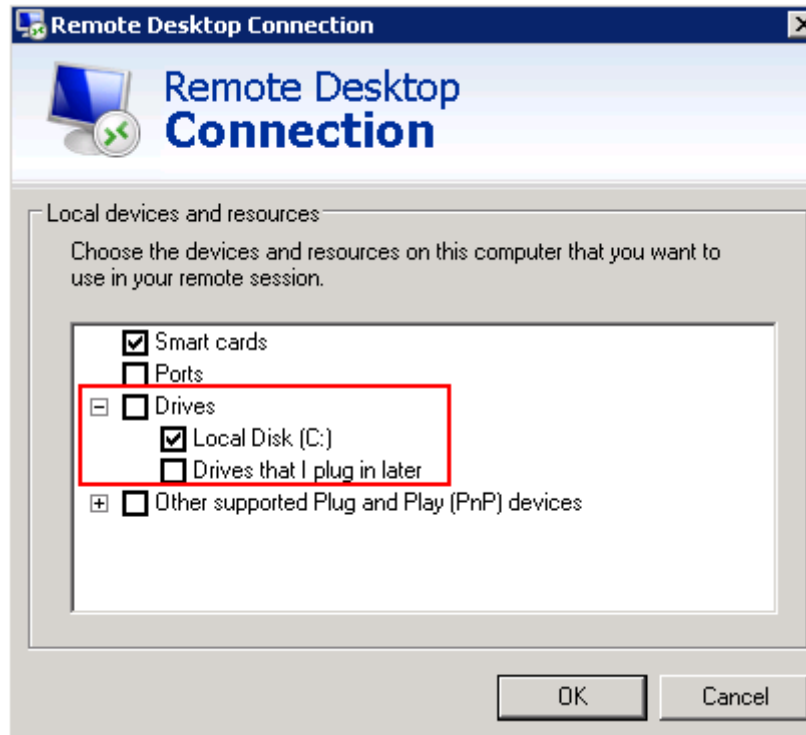
3. On the **General** tab, enter the EIP bound to the ECS and username **Administrator** for logging in to the ECS.



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 transferred 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 transferred to the Windows ECS.

13.6.3 How Can I Use WinSCP to Transfer Files from a Local Windows Computer to a Linux ECS?

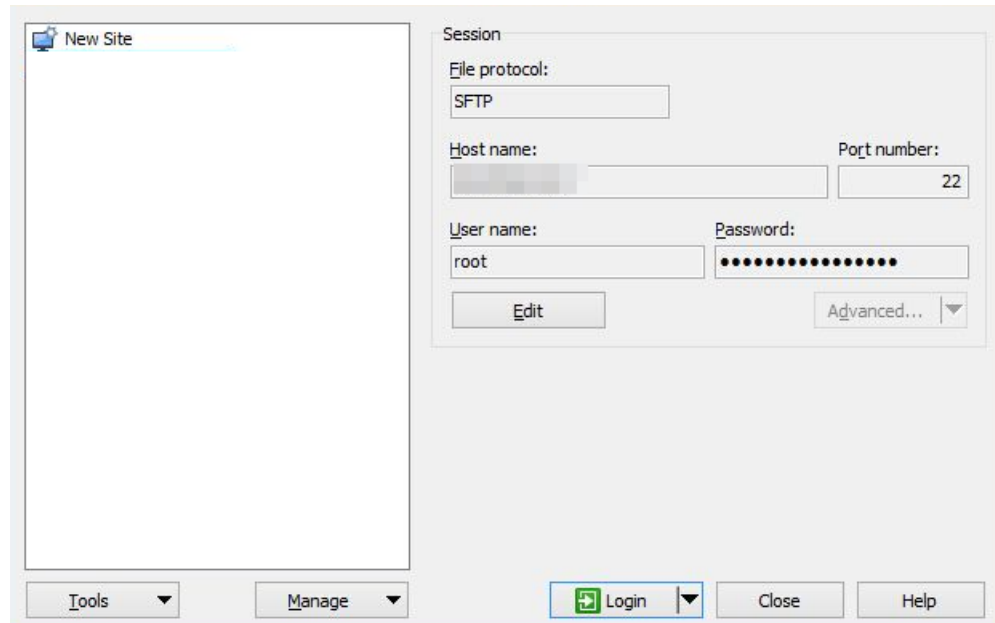
Scenarios

WinSCP can be used to securely copy-paste files across local and remote computers. Compared with FTP, WinSCP allows you to use a username and password to access the destination server without any additional configuration on the server.

To transfer a file from a local Windows computer to a Linux ECS, WinSCP is commonly used. This section describes how to transfer files from a local Windows computer to a Linux ECS using WinSCP. In this example, the ECS running CentOS 7.2 is used as an example.

Solution

1. [Download WinSCP](#).
2. Install WinSCP.
3. Start WinSCP.



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 created 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 transferring.

13.6.4 How Can I Use SCP to Transfer Files Between a Local Linux Computer and a Linux ECS?

Scenarios

This section describes how to use SCP to transfer files between a local Linux computer and a Linux ECS.

Procedure

Log in to the management console. On the **Elastic Cloud Server** page, obtain the EIP bound to the target ECS in the **IP Address** column.

- **Uploading files**

Run the following command on the local Linux computer to upload files to the Linux ECS:

scp *Path in which the files are stored on the local computer*

Username@EIP:Path in which the files are to be stored on the Linux ECS

For example, to transfer the **/home/test.txt** file on the local computer to the **/home** directory on the ECS whose EIP is 139.x.x.x, run the following command:

scp /home/test.txt root@139.x.x.x:/home

Enter the login password as prompted.

Figure 13-89 Setting file uploading

```
[root@ecs-5c83 home]# scp /home/test.txt root@139. :/home
root@139. 's password:
test.txt
```

- **Downloading files**

Run the following command on the local Linux computer to download files from the Linux ECS:

scp *Username@EIP:Path in which the files are stored on the Linux ECS Path in which the files are to be stored on the local computer*

For example, to download the **/home/test.txt** file on the ECS whose EIP is 139.x.x.x to the **/home** directory on the local computer, run the following command:

scp root@139.x.x.x:/home/test.txt /home/

Enter the login password as prompted.

Figure 13-90 Setting file downloading

```
[root@ecs-5c83 home]# scp root@139. :/home/test.txt /home
root@139. 's password:
test.txt
[root@ecs-5c83 home]# ls
test.txt
```

13.6.5 How Can I Use SFTP to Transfer Files Between a Local Linux Computer and a Linux ECS?

Scenarios

This section uses CentOS as an example to describe how to configure and use SFTP to transfer files or folders.

Procedure

1. Log in to the ECS as user **root**.
2. Run the following command to check the OpenSSH version, which is expected to be 4.8p1 or later:

ssh -V

Information similar to the following is displayed:

```
# OpenSSH_7.4p1, OpenSSL 1.0.2k-fips 26 Jan 2017
```

3. Create a user group and a user (for example, **user1**).

```
groupadd sftp
```

```
useradd -g sftp -s /sbin/nologin user1
```

4. Set a password for the user.

```
passwd user1
```

Figure 13-91 Setting a password

```
[root@ecs-9a32-0001 ~]# passwd user1
Changing password for user user1.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ecs-9a32-0001 ~]#
```

5. Assign permissions to directories.

```
chown root:sftp /home/user1
```

```
chmod 755 -R /home/user1
```

```
mkdir /home/user1/upload
```

```
chown -R user1:sftp /home/user1/upload
```

```
chmod -R 755 /home/user1/upload
```

6. Run the following command to edit the **sshd_config** configuration file:

```
vim /etc/ssh/sshd_config
```

Comment out the following information:

```
#Subsystem sftp /usr/libexec/openssh/sftp-server
```

Add the following information:

```
Subsystem sftp internal-sftp
Match Group sftp
ChrootDirectory /home/%u
ForceCommand internal-sftp
AllowTcpForwarding no
X11Forwarding no
```

7. Run the following command to restart the ECS:

```
service sshd restart
```

Alternatively, run the following command to restart sshd:

```
systemctl restart sshd
```

8. Run the following command to set up the connection:

```
sftp root@IP address
```

9. Run the **sftp** command to check the connection.

```
root@ [redacted] 's password:
Connected to [redacted].
sftp> ls
ceshi                print_all_tty.sh
s3fs_1.80_centos6.5_x86_64.rpm  speedtest.py
uploads
sftp> pwd
Remote working directory: /root
sftp> lpwd
Local working directory: /root
sftp> █
```

10. Transfer files or folders.

To upload files or folders, run the **put -r** command.

```
sftp> put -r ceshi/
Uploading ceshi/ to /root/ceshi
Entering ceshi/
ceshi/mysql57-community-release-el 100% 9224      9.0KB/s   00:00
ceshi/haha                          100% 28        0.0KB/s   00:00
sftp> █
```

To download files or folders, run the **get -r** command.

```
sftp> get -r s3fs_1.80_centos6.5_x86_64.rpm
Fetching /root/s3fs_1.80_centos6.5_x86_64.rpm to s3fs_1.80_centos6.5_x86_64.rpm
/root/s3fs_1.80_centos6.5_x86_64.r 100% 3250KB   3.2MB/s   00:00
sftp> █
```

13.6.6 How Can I Use FTP to Transfer Files from a Local Windows Computer to a Windows or Linux ECS?

Scenarios

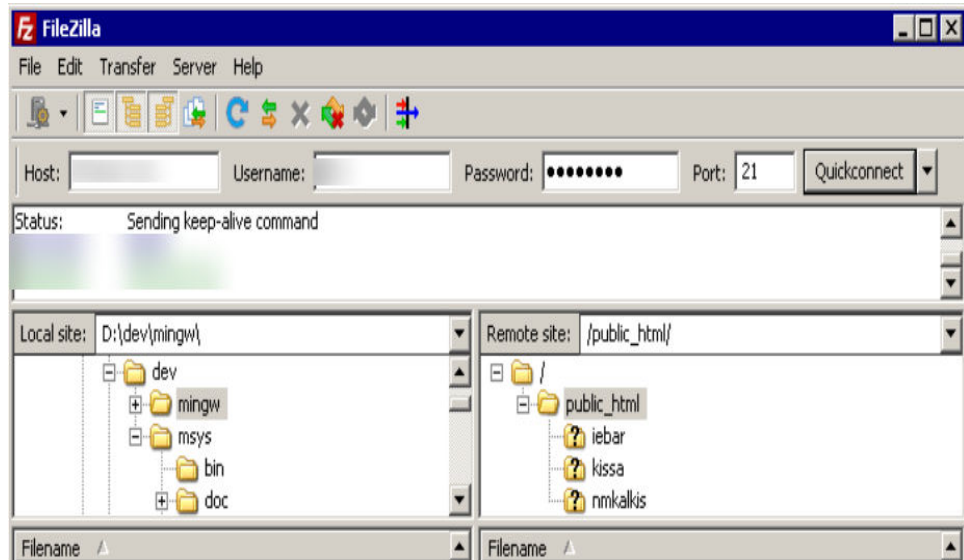
This section describes how to use FTP to transfer files from a local Windows computer to an ECS.

Prerequisites

FTP has been enabled on the target ECS.

Procedure

1. [Download FileZilla](#) and install it on the local Windows computer.
2. On the local Windows computer, open FileZilla, enter the information about the target ECS, and click **Quickconnect**.
 - **Host:** EIP bound to the ECS
 - **Username:** username set when the FTP site was set up
 - **Password:** password of the username
 - **Port:** FTP access port, which is port 21 by default

Figure 13-92 Setting connection parameters

3. Drag files from the local computer on the left to the target ECS on the right for transferring.

13.6.7 How Can I Use FTP to Transfer Files Between a Local Linux Computer and a Linux ECS?

Scenarios

This section describes how to use FTP on a local Linux computer to transfer files between the computer and a Linux ECS.

Prerequisites

FTP has been enabled on the target ECS.

Procedure

1. Install FTP on the local Linux computer.
Take CentOS 7.6 as an example. Run the following command to install FTP:
yum -y install ftp
2. Run the following command to access the ECS:
ftp EIP bound to the ECS
Enter the username and password as prompted for login.
 - **Uploading files**
Run the following command to upload local files to the ECS:
put Path in which files are stored on the local computer
For example, to upload the **/home/test.txt** file on the local Linux computer to the ECS, run the following command:
put /home/test.txt
 - **Downloading files**

Run the following command to download files on the ECS to the local computer:

get *Path in which the files are stored on the ECS Path in which the files are to be stored on the local computer*

For example, to download the **test.txt** file on the ECS to the local Linux computer, run the following command:

get /home/test.txt

13.6.8 What Should I Do If the Connection Between the Client and the Server Times Out When I Upload a File Using FTP?

Symptom

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

Constraints

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

Possible Causes

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

Solution

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

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

Symptom

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

Constraints

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

Possible Causes

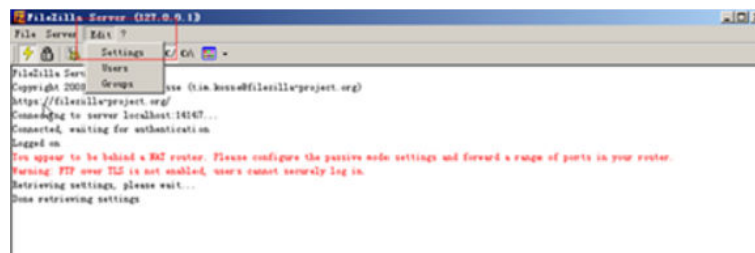
When NAT is enabled on the FTP server, the FTP client must connect to the FTP server in passive mode. In such a case, the public IP address (EIP) of the server cannot be accessed from the router. Therefore, you need to add the EIP to the public IP address list on the server. Additionally, set the port 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.

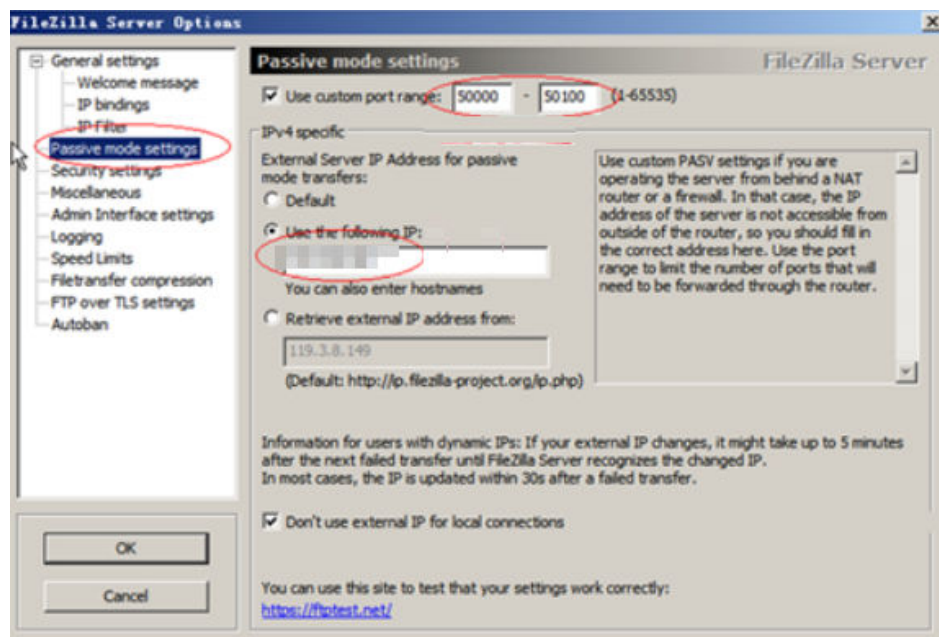
1. Configure the public IP address of the server.
Choose **Edit > Settings**.

Figure 13-93 Setting the public IP address



2. Choose **Passive mode settings**, set the port range (for example, 50000-50100) for transmitting data, and enter the target public IP address.

Figure 13-94 Setting the range of ports for data transmission



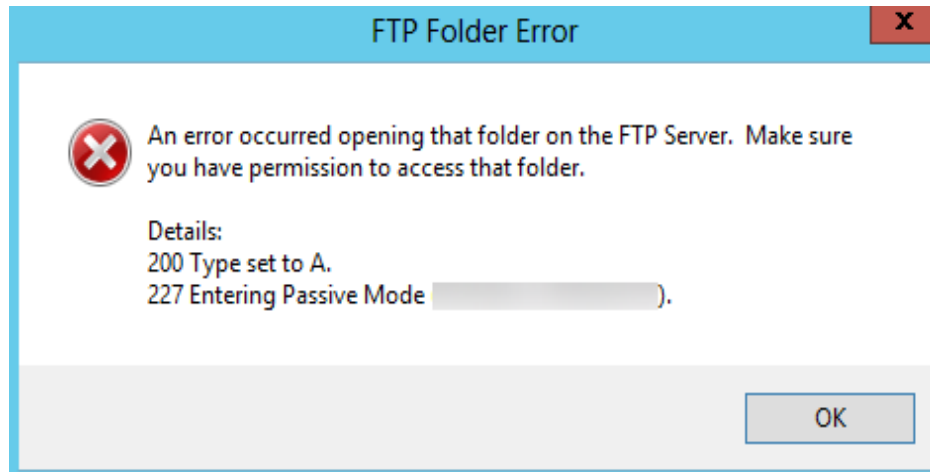
3. Click **OK**.
4. Allow traffic on TCP ports 50000-50100 and 21 in the security group in the inbound direction.
5. Test the connection on the client.

13.6.10 What Should I Do If an Error Occurs When I Open a Folder on an FTP Server?

Symptom

An error occurred when I opened a folder on an FTP server. The system displayed a message for checking permissions.

Figure 13-95 FTP Folder Error



Possible Causes

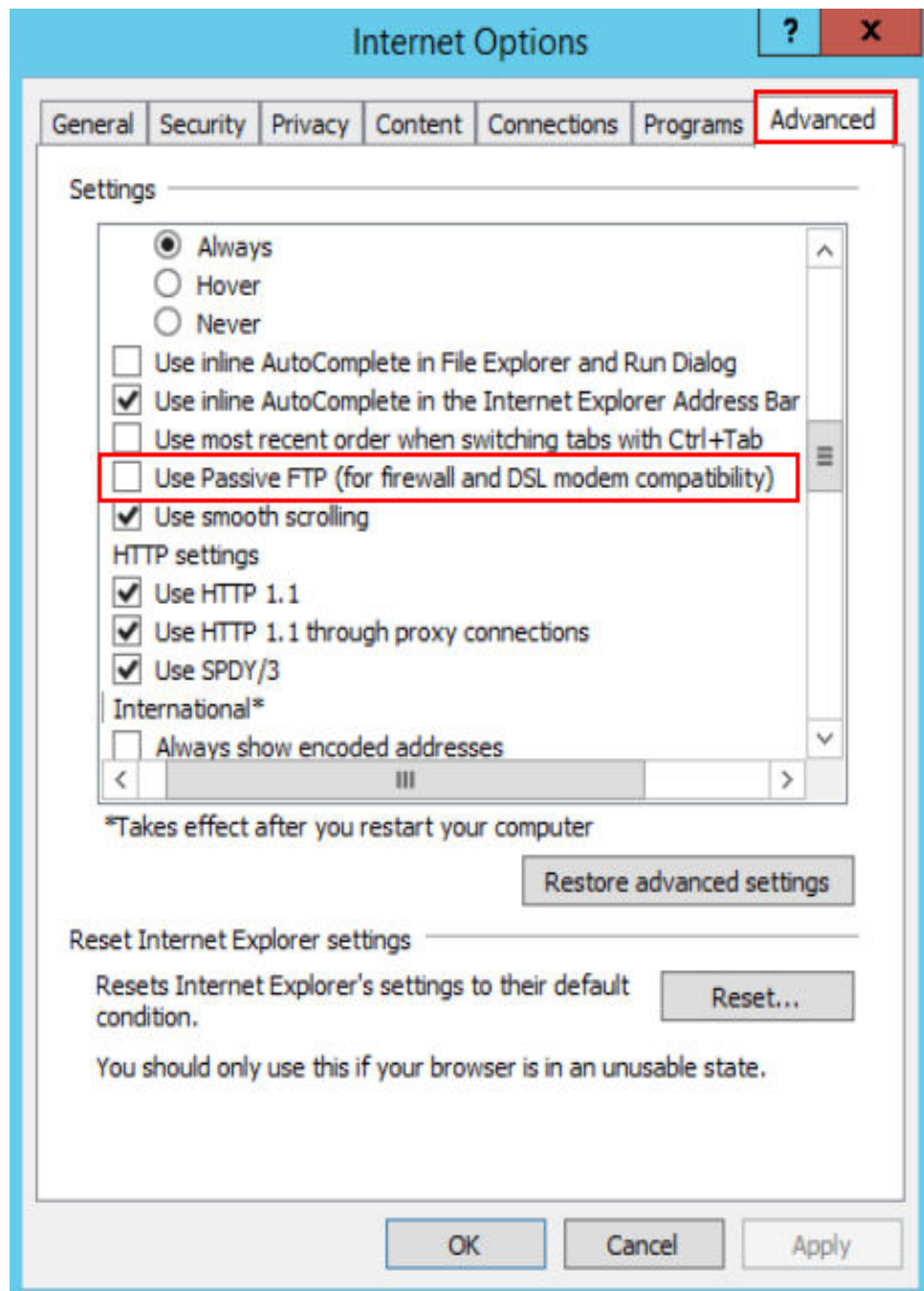
The FTP firewall configured for the browser blocked the file opening.

Solution

The following uses Internet Explorer as an example.

1. Open the Internet Explorer and choose **Tools > Internet options**.
2. Click the **Advanced** tab.
3. Deselect **Use Passive FTP (for firewall and DSL modem compatibility)**.

Figure 13-96 Internet Options



4. Click **OK**, restart Internet Explorer, and open the folder on the FTP server again.

13.7 Application Migration

13.7.1 Can an ECS Be Migrated to Another Region or Account?

After an ECS is created, it cannot be migrated to another region or account.

To migrate an ECS to another region, create a private image using the ECS and use cross-region image replication to copy the image to the target region. Then, use the image to provision the same ECSs.

To migrate an ECS to another account, create a private image using the ECS and share the private image with the target account. After accepting the shared image, the account user can use this image to create the same ECSs.

13.8 Disk Management

13.8.1 What Should I Do If the Data Disk Attached a Windows ECS Is Unavailable?

Symptom

After logging in to my Windows ECS, I cannot find the attached data disk.



Formatting a disk will cause data loss. Therefore, before formatting a disk, create a backup for it.

Possible Causes

- A newly added data disk has not been partitioned or initialized.
- The disk becomes offline after the ECS OS is changed or the ECS specifications are modified.

Newly Added Data Disk Has Not Been Partitioned or Initialized

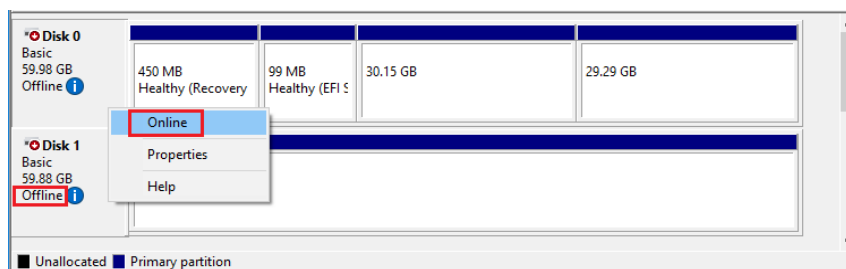
A new data disk does not have partitions and file systems by default. That is why it is unavailable in **My Computer**. To resolve this issue, manually initialize the disk.

Disk Becomes Offline After the ECS OS Is Changed or the ECS Specifications Are Modified

After the ECS OS is changed, data disks may become unavailable due to file system inconsistency. After the specifications of a Windows ECS are modified, data disks may be offline.

1. Log in to the ECS, open the **cmd** window, and enter **diskmgmt.msc** to switch to the **Disk Management** page.
Check whether the affected disk is offline.
2. Set the affected disk to be online.
In the disk list, right-click the affected disk and choose **Online** from the shortcut menu to make it online.

Figure 13-97 Setting disk online



3. In **My Computer**, check whether the data disk is displayed properly.
If the fault persists, initialize and partition the disk again. Before initializing the disk, create a backup for it.

13.8.2 How Can I Adjust System Disk Partitions?

Scenarios

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

There are two ways to expand a system disk:

- 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:
 - [13.8.7 How Can I Add the Empty Partition of an Expanded System Disk to the End Root Partition Online?](#)
 - [13.8.8 How Can I Add the Empty Partition of an Expanded System Disk to the Non-end Root Partition Online?](#)

Procedure

This section uses an ECS running CentOS 7.3 64bit as an example. A 60 GB system disk was created with the ECS. However, the displayed capacity of the system disk partition 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.

Figure 13-98 Viewing details about the disk

```
[root@ecs-8d6c ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1      38G  1.2G   35G   4% /
devtmpfs        899M    0   899M   0% /dev
tmpfs           908M    0   908M   0% /dev/shm
tmpfs           908M  8.4M   900M   1% /run
tmpfs           908M    0   908M   0% /sys/fs/cgroup
tmpfs          182M    0   182M   0% /run/user/0
[root@ecs-8d6c ~]# fdisk -l

Disk /dev/xvda: 64.4 GB, 64424509440 bytes, 125829120 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0004d5e5

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1 *          2048     79980543   39989248    83  Linux
/dev/xvda2             79980544   83886079    1952768    82  Linux swap / Solaris
[root@ecs-8d6c ~]# _
```

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

Figure 13-99 Viewing disk partitions

```
[root@ecs-8d6c ~]# parted -l /dev/xvda
Model: Xen Virtual Block Device (xvd)
Disk /dev/xvda: 64.4GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

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

Step 2 Create a partition for the expanded system disk capacity.

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

fdisk /dev/xvda

Information similar to the following is displayed:

```
[root@ecs-8d6c ~]# fdisk /dev/xvda
Welcome to fdisk (util-linux 2.23.2).
```

```
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.
```

```
Command (m for help):
```

2. Enter **n** and press **Enter** to create a new partition.

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

Information similar to the following is displayed.

Figure 13-100 Creating a new partition

```
[root@ecs-8d6c ~]# fdisk /dev/xvda
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): n
Partition type:
   p   primary (2 primary, 0 extended, 2 free)
   e   extended
Select (default p):
Using default response p
Partition number (3,4, default 3):
First sector (83886080-125829119, default 83886080):
Using default value 83886080
Last sector, +sectors or +size{K,M,G} (83886080-125829119, default 125829119):
Using default value 125829119
Partition 3 of type Linux and of size 20 GiB is set

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
[root@ecs-8d6c ~]#
```

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

Figure 13-101 Specifying the new partition's start cylinder number

```
First sector (83886080-125829119, default 83886080):
Using default value 83886080
Last sector, +sectors or +size{K,M,G} (83886080-125829119, default 125829119):
```

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

Figure 13-102 Specifying the new partition's end cylinder number

```
Last sector, +sectors or +size{K,M,G} (83886080-125829119, default 125829119):
Using default value 125829119
Partition 3 of type Linux and of size 20 GiB is set
```

5. Enter **p** and press **Enter** to view the created partition.
Information similar to the following is displayed.

Figure 13-103 Viewing the created partition

```
Command (m for help): p
Disk /dev/xvda: 64.4 GB, 64424509440 bytes, 125829120 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0004d5e5

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1    *          2048     79980543   39989248   83   Linux
/dev/xvda2                79980544     83886079    1952768   82   Linux swap / Solaris
/dev/xvda3                83886080    125829119   20971520   83   Linux
```

6. Enter **w** and press **Enter**. The system saves and exits the partition. The system automatically writes the partition result into the partition list. Then, the partition is created. Information similar to the following is displayed.

Figure 13-104 Completing the partition creation

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

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

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

Figure 13-105 Viewing disk partitions

```
Disk Flags:
Number  Start   End     Size    Type    File system  Flags
  1      1049kB  41.0GB  40.9GB  primary ext4          boot
  2      41.0GB  42.9GB  2000MB  primary linux-swap(v1)
  3      42.9GB  64.4GB  21.5GB  primary ext4
```

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

partprobe

- Step 4** Configure the type of the new partition file system.

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

Figure 13-106 Viewing the file system type

```
[root@ecs-8d6c ~]# df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/xvda1      ext4      41G   1.3G   37G    4% /
devtmpfs        devtmpfs  943M    0   943M    0% /dev
tmpfs           tmpfs     952M    0   952M    0% /dev/shm
tmpfs           tmpfs     952M   8.8M   944M    1% /run
tmpfs           tmpfs     952M    0   952M    0% /sys/fs/cgroup
tmpfs           tmpfs     191M    0   191M    0% /run/user/0
[root@ecs-8d6c ~]#
```

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

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

NOTE

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

Information similar to the following is displayed:

```
[root@ecs-86dc ]# mkfs -t ext4 /dev/xvda3
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
1790544 inodes, 7156992 blocks
357849 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2155872256
219 block groups
32768 blocks per group, 32768 fragments per group
8176 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Step 5 Mount the new partition to the target directory.

If 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:

```
mkdir /root/new
```

2. Run the following command to mount the new partition to the **/root/new** directory:

```
mount /dev/xvda3 /root/new
```

Information similar to the following is displayed:

```
[root@ecs-86dc ]# mount /dev/xvda3 /root/new
[root@ecs-86dc ]#
```

- Run the following command to view the mounted file systems:

df -TH

Information similar to the following is displayed:

Figure 13-107 Viewing the mounted file systems

```
[root@ecs-8d6c ~]# df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/xvda1      ext4      41G   1.3G   37G    4% /
devtmpfs        devtmpfs  943M    0   943M    0% /dev
tmpfs           tmpfs     952M    0   952M    0% /dev/shm
tmpfs           tmpfs     952M   8.8M   944M    1% /run
tmpfs           tmpfs     952M    0   952M    0% /sys/fs/cgroup
/dev/xvda3      ext4      22G    47M    20G    1% /root/new
tmpfs           tmpfs     191M    0   191M    0% /run/user/0
[root@ecs-8d6c ~]# b1
```

- 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.

- Run the following command to obtain the file system type and UUID:

blkid

Figure 13-108 Viewing the file system type

```
[root@ecs-8d6c ~]# blkid
/dev/xvda1: UUID="7c4fce5d-f8f7-4ed6-8463-f2bd22d0ddea" TYPE="ext4"
/dev/xvda2: UUID="5de3cf2c-30c6-4fb2-9e63-830439d4e674" TYPE="swap"
/dev/xvda3: UUID="96e5e028-60fb-4547-a82a-35ace1086c4f" TYPE="ext4"
[root@ecs-8d6c ~]#
```

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

- Run the following command to open the **fstab** file using the vi editor:
vi /etc/fstab
- Press **i** to enter editing mode.
- 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
```

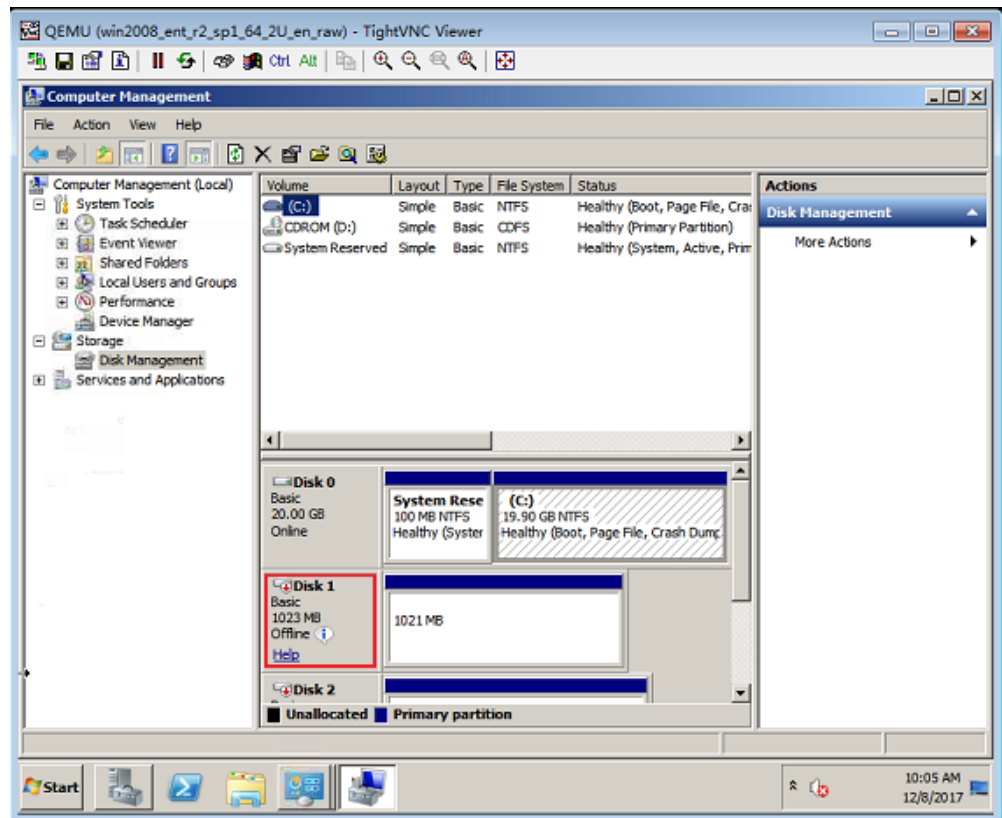
----End

13.8.3 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.

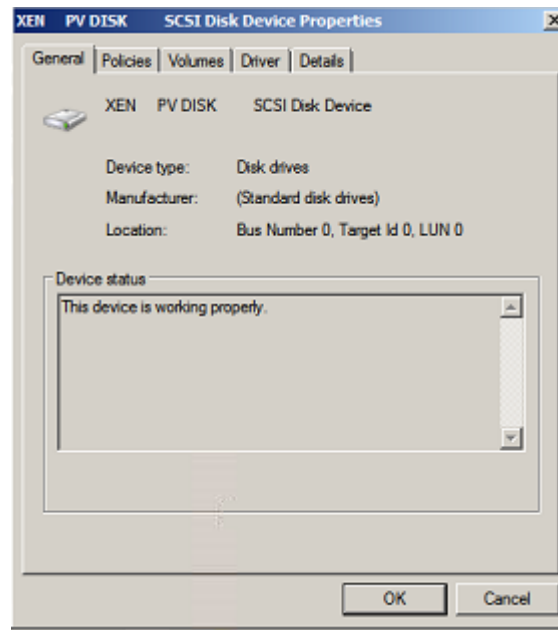
1. Log in to the Windows ECS.
2. Click **Start** in the lower left corner of the desktop.
3. Choose **Control Panel > Administrative Tools > Computer Management**.
4. In the navigation pane on the left, choose **Storage > Disk Management**.

Figure 13-109 Disk Management



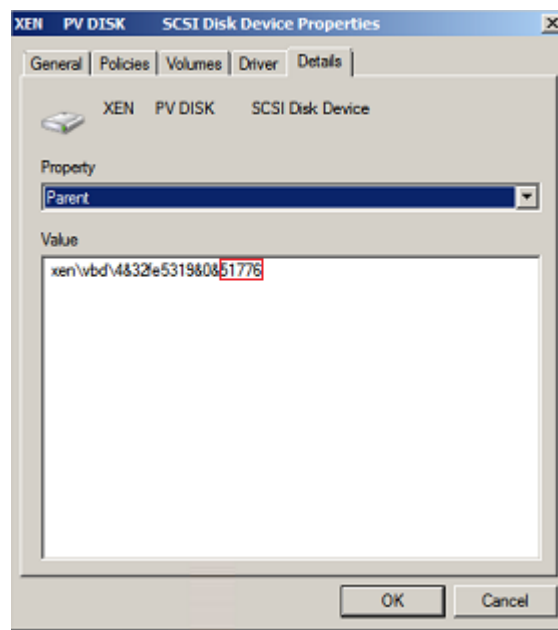
5. Taking disk 1 marked in [Figure 13-109](#) as an example, view the disk device for disk 1.
 - a. Right-click the gray area where disk 1 is located, as shown in the red box in [Figure 13-109](#).
 - b. Click **Properties**.
The **SCSI Disk Device Properties** dialog box is displayed, as shown in [Figure 13-110](#).

Figure 13-110 Disk properties



- c. Click the **Details** tab and set **Property** to **Parent**.

Figure 13-111 Disk device details



- d. Record the digits following **&** in the parameter value, for example, **51776**, which is the master and slave device number corresponding to the disk partition.
- e. Obtain the disk device according to the information listed in [Table 13-4](#). The disk device corresponding to **51776** is **xvde**. The disk device used by disk 1 is xvde.

Table 13-4 Mapping between disk partitions and disk devices

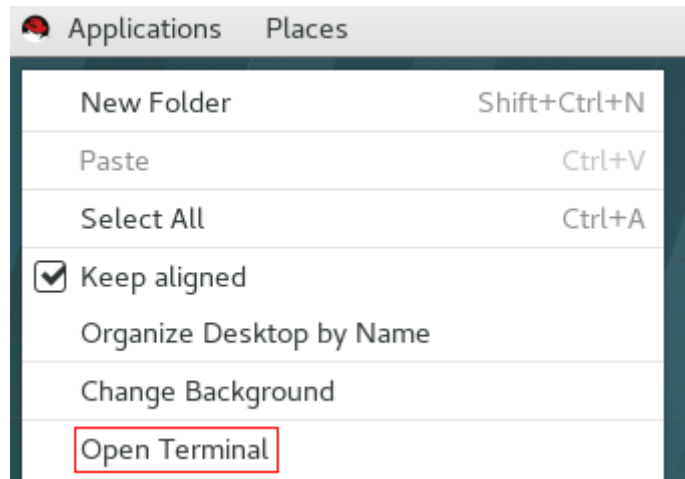
Master and Slave Device Number for a Disk Partition	Disk Device
51712	xvda
51728	xvdb
51744	xvdc
51760	xvdd
51776	xvde
51792	xvdf
51808	xvdg
51824	xvdh
51840	xvdi
51856	xvdj
51872	xvdk
51888	xvdl
51904	xvdm
51920	xvdn
51936	xvdo
51952	xvdp
268439552	xvdq
268439808	xvdr
268440064	xvds
268440320	xvdt
268440576	xvdu
268440832	xvdv
268441088	xvdw
268441344	xvdx

13.8.4 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.

Figure 13-112 open terminal



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

Figure 13-113 Viewing disk partitions and disk devices

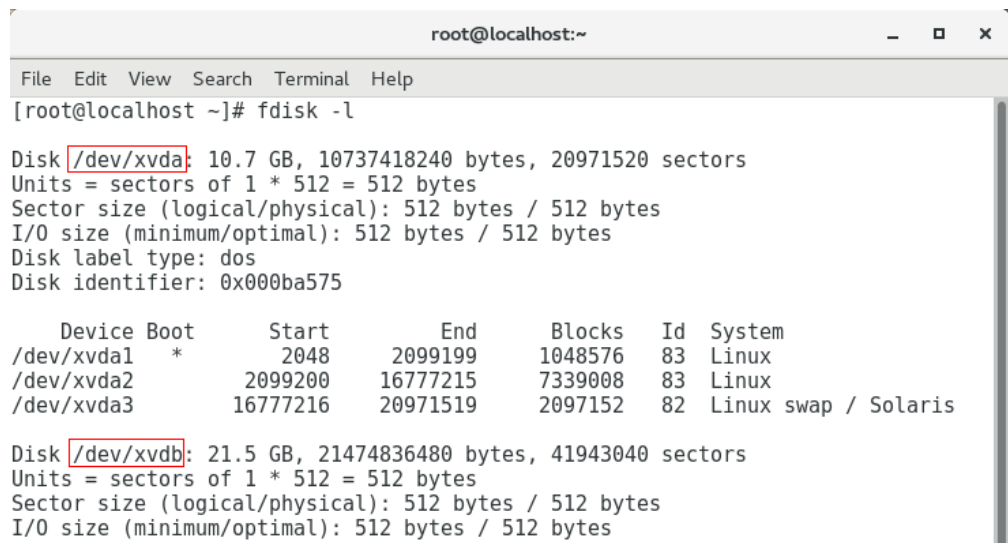


Table 13-5 lists the mapping between disk partitions and disk devices.

Table 13-5 Mapping between disk partitions and disk devices

Disk Partition	Disk Device
xvda	xvda
xvdb	xvdb

Disk Partition	Disk Device
xvdc	xvdc
xvdd	xvdd
xvde	xvde
xvdf	xvdf
xvdg	xvdg
xvdh	xvdh
xvdi	xvdi
xvdj	xvdj
xvdk	xvdk
xvdl	xvdl
xvdm	xvdm
xvdn	xvdn
xvdo	xvdo
xvdp	xvdp
xvdq	xvdq
xvdr	xvdr
xvds	xvds
xvdt	xvdt
xvdu	xvdu
xvdv	xvdv
xvdw	xvdw
xvdx	xvdx

13.8.5 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.

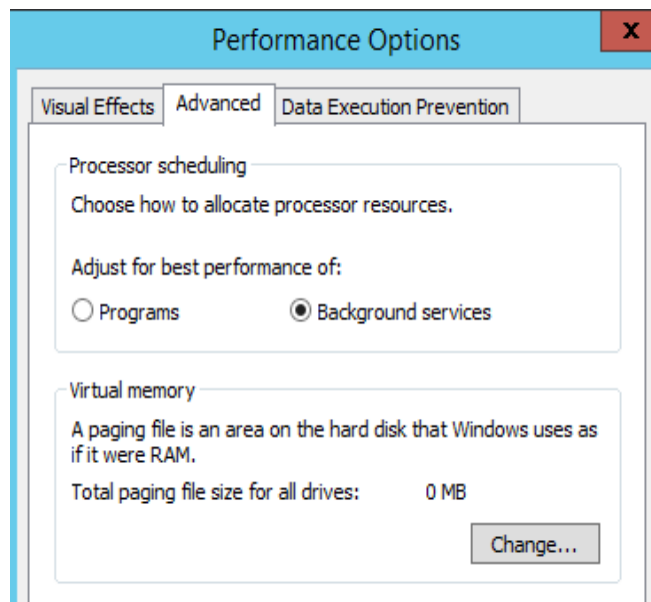
NOTE

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.

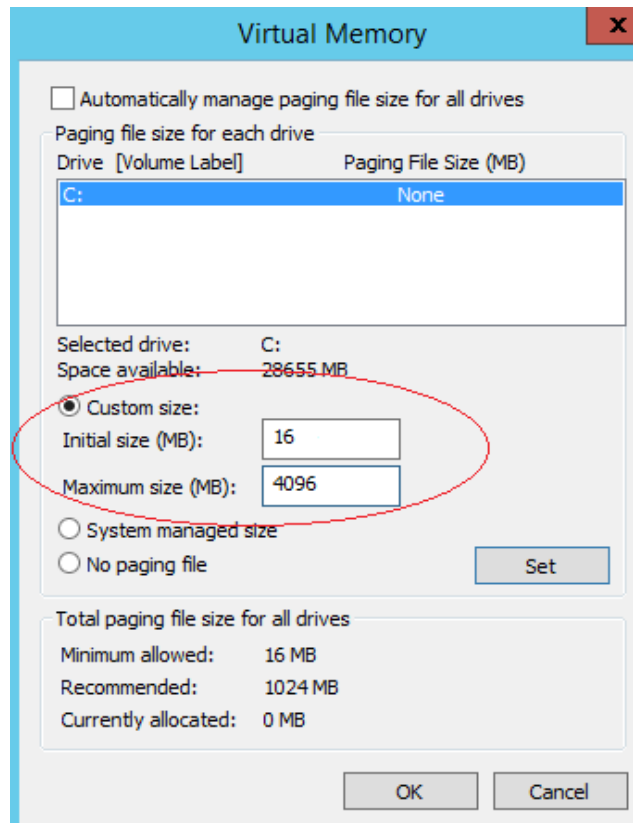
1. Right-click **Computer** and choose **Properties** from the shortcut menu.
2. In the navigation pane on the left, choose **Advanced system settings**.
The **System Properties** dialog box is displayed.
3. Click the **Advanced** tab and then **Settings** in the **Performance** pane.
The **Performance Options** dialog box is displayed.

Figure 13-114 Performance Options



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**.

Figure 13-115 Virtual Memory



7. Click **Set** and then **OK** to complete the configuration.
8. Restart the ECS for the configuration to take effect.

13.8.6 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 (4,096 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.

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

Scenarios

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

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

Procedure

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

1. Run the following command to view disk partitions:

parted -l /dev/xvda

```
[root@sluo-ecs-5e7d ~]# parted -l /dev/xvda
Model: Xen Virtual Block Device (xvd)
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-swaps(v1)
 2    4296MB 42.9GB 38.7GB primary ext4 boot
```

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

blkid

```
/dev/xvda1: UUID="25ec3bdb-ba24-4561-bcdc-802edf42b85f" TYPE="swap"
/dev/xvda2: UUID="1a1ce4de-e56a-4e1f-864d-31b7d9dfb547" TYPE="ext4"
```

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

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

yum install cloud-utils-growpart

4. Run the following command to expand the root partition (the second partition) using growpart:

growpart /dev/xvda 2

```
[root@sluo-ecs-5e7d ~]# growpart /dev/xvda 2
CHANGED: partition=2 start=8390656 old: size=75495424 end=83886080 new:
size=96465599,end=104856255
```

5. Run the following command to verify that online capacity expansion is successful:

parted -l /dev/xvda

```
[root@sluo-ecs-5e7d ~]# parted -l /dev/xvda
Model: Xen Virtual Block Device (xvd)
Disk /dev/xvda: 53.7GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number Start End Size Type File system Flags
```



```
1 1049kB 4296MB 4295MB primary linux-swap(v1)
2 4296MB 53.7GB 49.4GB primary ext4 boot
```

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

resize2fs -f \$Partition name

Suppose the partition name is **/dev/xvda2**, run the following command:

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

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

Scenarios

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

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

Procedure

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

1. Run the following command to view disk partitions:

parted -l /dev/xvda

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

tail -n 3 /etc/fstab

```
[root@sluo-ecs-a611 ~]# tail -n 3 /etc/fstab
#
UUID=7c4fce5d-f8f7-4ed6-8463-f2bd22d0ddea / ext4 defaults 1 1
UUID=5de3cf2c-30c6-4fb2-9e63-830439d4e674 swap swap defaults 0 0
```

- b. Run the following command to edit the fstab partition table and delete the swap partition attaching information.

vi /etc/fstab

tail -n 3 /etc/fstab

```
[root@sluo-ecs-a611 ~]# vi /etc/fstab
[root@sluo-ecs-a611 ~]# tail -n 3 /etc/fstab
#
UUID=7c4fce5d-f8f7-4ed6-8463-f2bd22d0ddea /                ext4 defaults 1 1
```

3. Run the following command to disable the swap partition:

swapoff -a

4. Delete the swap partition.

- a. Run the following command to view the partition:

parted /dev/xvda

```
[root@sluo-ecs-a611 ~]# parted /dev/xvda
GNU Parted 3.1
Using /dev/xvda
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) help
align-check TYPE N                check partition N for TYPE(min|opt) alignment
help [COMMAND]                    print general help, or help on COMMAND
mklabel,mktable LABEL-TYPE        create a new disklabel (partition table)
mkpart PART-TYPE [FS-TYPE] START END make a partition
name NUMBER NAME                   name partition NUMBER as NAME
print [devices|free|list,all|NUMBER] display the partition table, available devices, free space,
all found partitions, or a
particular partition
quit                                exit program
rescue START END                   rescue a lost partition near START and END
rm NUMBER                           delete partition NUMBER
select DEVICE                       choose the device to edit
disk_set FLAG STATE                 change the FLAG on selected device
disk_toggle [FLAG]                 toggle the state of FLAG on selected device
set NUMBER FLAG STATE               change the FLAG on partition NUMBER
toggle [NUMBER [FLAG]]             toggle the state of FLAG on partition NUMBER
unit UNIT                           set the default unit to UNIT
version                             display the version number and copyright information of GNU
Parted
(parted)
```

- b. Press **p**.

```
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)
```

- c. Run the following command to delete the partition:

rm 2

```
(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:

Number Start End Size Type File system  Flags
 1   1049kB 41.0GB 40.9GB primary ext4      boot
```

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

quit

```
(parted) quit
Information: You may need to update /etc/fstab.
```

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

parted -l /dev/xvda

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

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

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

yum install cloud-utils-growpart

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

growpart /dev/xvda 1

```
[root@sluo-ecs-a611 ~]# growpart /dev/xvda 1
CHANGED: partition=1 start=2048 old: size=79978496 end=79980544 new:
size=209710462,end=209712510
```

8. Run the following command to verify that online capacity expansion is successful:

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

resize2fs -f \$Partition name

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

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

13.8.9 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.

Table 13-6 Numbers of disks that can be attached to a newly created ECS

ECS Type	Maximum VBD Disks	Maximum SCSI Disks	Constraint
KVM (excepting D3 ECSs)	24	59	VBD disks + SCSI disks \leq 60 (This constraint does not apply to local disks.) The number of local disks is determined based on the ECS flavor.
D3	24	30	VBD disks + SCSI disks \leq 54 (This constraint does not apply to local disks.) The number of local disks is determined based on the ECS flavor.

 **NOTE**

- The system disk of an ECS is of VBD type. Therefore, the maximum number of SCSI disks is 59.
- For a D-series KVM ECS, its local disks use two SCSI controllers, indicating that 30 SCSI drive letters are used. Therefore, a maximum of 30 SCSI disks can be attached to such an ECS.

The maximum number of disks attached to an ECS that is created before the disk function upgrade remains unchanged, as shown in [Table 13-7](#).

Table 13-7 Numbers of disks that can be attached to an existing ECS

ECS Type	Maximum VBD Disks	Maximum SCSI Disks	Maximum Local Disks	Constraint
Xen	60	59	59	VBD disks + SCSI disks + Local disks \leq 60
KVM	24	23	59	VBD disks + SCSI disks \leq 24

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.

13.8.10 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.
- Certain ECSs support SCSI EVS disk attachment. For details, see [13.8.11 Which ECSs Can Be Attached with SCSI EVS Disks?](#)

13.8.11 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.

13.8.12 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.
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 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.
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.

 NOTE

A serial number is the first 20 digits of the disk UUID.

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

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

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

Or:

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

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

The following information is displayed:

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

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

Using a VBD to Obtain a Disk Device Name

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

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

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

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

The following information is displayed:

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

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

Using a WWN to Obtain a Disk Device Name

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

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

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

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

The following information is displayed:

```
[root@host-192-168-133-148 block]# ll /dev/disk/by-id/ |grep 6888603000008b32fa16688d09368506 |
grep scsi-3
lrwxrwxrwx 1 root root 9 May 21 20:22 scsi-36888603000008b32fa16688d09368506 -> ../sda
```

13.8.13 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:

```
ll /dev/disk/by-id|grep Disk drive letter
```

For example, if the drive letter of the SCSI disk is **/dev/sdb**, run the following command:

```
ll /dev/disk/by-id|grep sdb
```

```
CNA64_22:/opt/galax/eucalyptus/ecs_scripts # ll /dev/disk/by-id/ | grep sdb
lrwxrwxrwx 1 root root 9 Dec 6 11:26 scsi-3688860300001436b005014f890338280 -> ../../sdb
lrwxrwxrwx 1 root root 9 Dec 6 11:26 wwn-0x688860300001436b005014f890338280 -> ../../sdb
```

3. Change the drive letter (for example, **/dev/sdb**) of the SCSI disk to the corresponding SCSI ID in the **/etc/fstab** file.

/dev/disk/by-id/SCSI ID

For example, if the SCSI ID obtained in step 2 is `scsi-3688860300001436b005014f890338280`, use the following data to replace **/dev/sdb**:

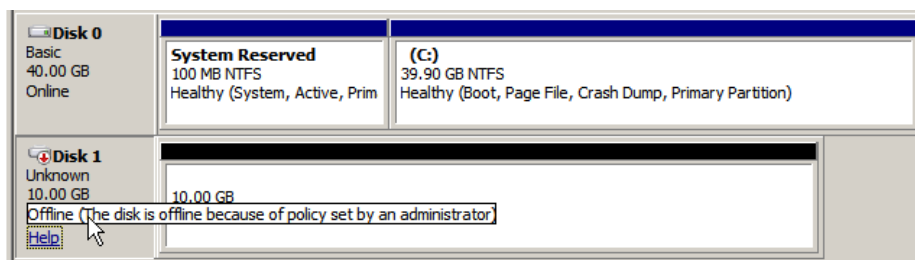
/dev/disk/by-id/scsi-3688860300001436b005014f890338280

13.8.14 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."

Figure 13-116 Offline disk



Possible Causes

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

Table 13-8 SAN policies

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

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

Solution

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

1. Log in to the Windows ECS.
2. Press **Win+R** to run **cmd.exe**.
3. Run the following command to access DiskPart:
diskpart
4. Run the following command to view the SAN policy on the ECS:
san
 - If the SAN policy is **OnlineAll**, run the **exit** command to exit DiskPart.
 - If the SAN policy is not **OnlineAll**, go to step 5.
5. Run the following command to change the SAN policy to **OnlineAll**:
san policy=onlineall
6. (Optional) Use the ECS with the SAN policy changed to create a private image for the configuration to 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.

13.8.15 What Should I Do If the Drive Letter Changes After the ECS Is Restarted?

Symptom

For a Linux ECS, the drive letter may change after an EVS disk is detached and then attached again, or after an EVS disk is detached and then the ECS is restarted. This is a normal case due to the drive letter allocation mechanism of the Linux system.

For example, an ECS has three disks attached: **/dev/vda1**, **/dev/vdb1**, and **/dev/vdc1**. The mounting parameters in **/etc/fstab** are as follows:

```
cat /etc/fstab
```

```
UUID=b9a07b7b-9322-4e05-ab9b-14b8050bdc8a / ext4 defaults 0 1
/dev/vdb1 /data1 ext4 defaults 0 0
/dev/vdc1 /data2 ext4 defaults 0 0
```

If **/dev/vdb1** is detached, **/dev/vdc1** becomes **/dev/vdb1** and is mounted to **/data1** after the ECS is restarted. In such a case, no disk is mounted to **/data2**.

Solution

To prevent this issue, use a UUID, a unique character string provided by the Linux system for disk partitions, to replace the **/dev/vdx** device.

1. Run the following command to obtain the partition UUID:
blkid Disk partition
In this example, run the following command to obtain the UUID of the **/dev/vdb1** partition:

blkid /dev/vdb1

Information similar to the following is displayed:

```
[root@ecs-test-0001 ~]# blkid /dev/vdb1
/dev/vdb1: UUID="b9a07b7b-9322-4e05-ab9b-14b8050cd8cc" TYPE="ext4"
```

The UUID of the **/dev/vdb1** partition is displayed.

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

```
vi /etc/fstab
```

3. Press **i** to enter the editing mode.
4. Move the cursor to the end of the file and press **Enter**. Then, add the following information:

```
UUID=b9a07b7b-9322-4e05-ab9b-14b8050cd8cc /mnt/sdc ext4 defaults 0 0
```

Repeat the preceding operations to add the UUID of the **/dev/vdc1** partition and run the following command to check the disk mounting parameters:

```
cat /etc/fstab
```

The following information is displayed:

```
UUID=b9a07b7b-9322-4e05-ab9b-14b8050bdc8a / ext4 defaults 0 1
UUID=b9a07b7b-9322-4e05-ab9b-14b8050cd8cc /data1 ext4 defaults 0 0
UUID=b9a07b7b-9322-4e05-ab9b-14b8050ab6bb /data2 ext4 defaults 0 0
```

13.8.16 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 click **Yes** 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.

13.9 Passwords and Key Pairs

13.9.1 How Can I Set the Validity Period of the Image Password?

If an ECS cannot be logged in because of expired image password, you can contact the administrator for handling.

If the ECS can still be logged in, you can perform the following operations to set the password validity period.

Procedure

The following operations use EulerOS 2.2 as an example.

1. Log in to the ECS.
2. Run the following command to check the password validity period:

```
vi /etc/login.defs
```

The value of parameter **PASS_MAX_DAYS** is the password validity period.

3. Run the following command to change the value of parameter **PASS_MAX_DAYS**:

```
chage -M 99999 user_name
```

99999 is the password validity period, and *user_name* is the system user, for example, user **root**.

NOTE

You are advised to configure the password validity period as needed and change it at a regular basis.

4. Run command **vi /etc/login.defs** to verify that the configuration has taken effect.

Figure 13-117 Configuration verification


```
# Password aging controls:
#
#     PASS_MAX_DAYS    Maximum number of days a password may be used.
#     PASS_MIN_DAYS    Minimum number of days allowed between password changes.
#     PASS_MIN_LEN     Minimum acceptable password length.
#     PASS_WARN_AGE    Number of days warning given before a password expires.
#
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_MIN_LEN 5
PASS_WARN_AGE 7
```

13.9.2 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 target ECS.
The page providing details about the ECS is displayed.
6. Obtain the **Key Pair** value.
The value is the key pair used by the ECS.

13.9.3 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:

1. Click  in the upper right corner of the browser.
2. Select **Internet Options**.
3. Click the **Security** tab in the displayed dialog box.
4. Click **Internet**.
5. If the security level indicates **Custom**, click **Default Level** to restore to the default settings.
6. Move the scroll bar to set the security level to **Medium** and click **Apply**.
7. Click **Custom Level**.
8. Set **Initialize and script ActiveX controls not marked as safe for scripting** to **Prompt**.
9. Click **Yes**.

13.9.4 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 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 the login failed, contact customer service for technical support.

13.9.5 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.

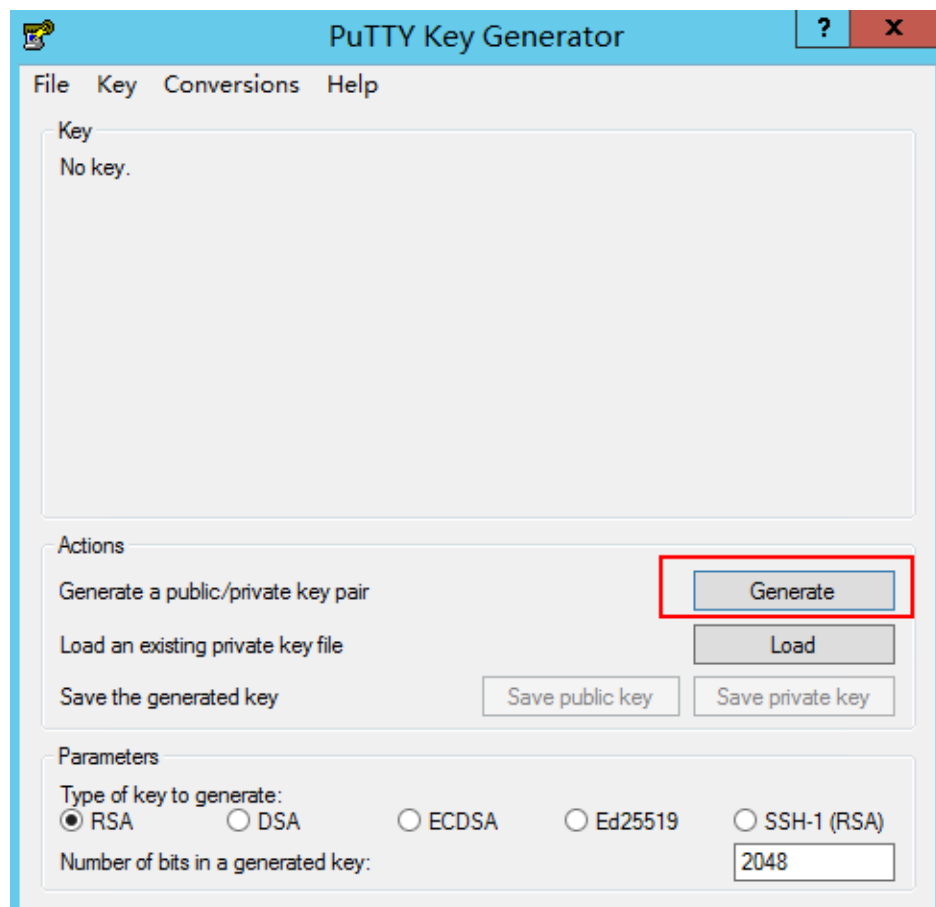
Storing a public key by clicking **Save public key** of **puttygen.exe** will change the format of the public key content. Such a key cannot be imported to the management console.

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.

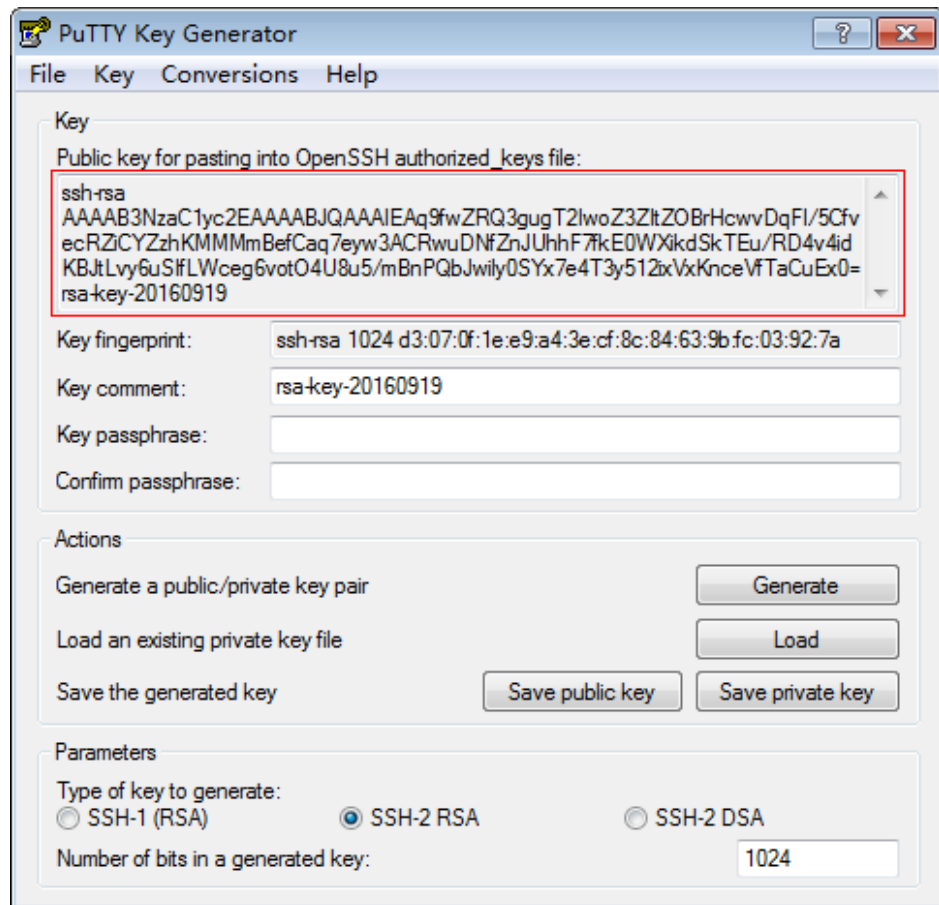
1. Double-click **puttygen.exe** to switch to the **PuTTY Key Generator** page.


Figure 13-118 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 13-119** is the public key with the format meeting system requirements.

Figure 13-119 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**.

13.9.6 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 that is 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:683020925C5D8569C23AA724774CE9CC:::",

- Username: **Administrator**
- RID: **500**
- LM-HASH value: **C8825DB10F2590EAAAD3B435B51404EE**
- NT-HASH value: **683020925C5D8569C23AA724774CE9CC**

Use an image to create two ECSs, ecs01 and ecs02. Then, verify that the hash values of the **cloudbase-init** account for the two ECSs are different.

- LM-HASH and NTLM-HASH values of the **cloudbase-init** account for ecs01

Figure 13-120 ecs01

```
----- BEGIN DUMP -----
c\l\o\u\i\n\i\t\:\1003\:\AAD3B435B51404EEAAD3B435B51404EE\:\CCA38DDEB517A0E2342AEB34C0473C39\:\:
Guest\:\501\:\AAD3B435B51404EEAAD3B435B51404EE\:\31D6CFE0D16AE931B73C59D7E0C089C0\:\:
Administrator\:\500\:\AAD3B435B51404EEAAD3B435B51404EE\:\27CF57575EB83D9A6D7D27831157A947\:\:
----- END DUMP -----
3 dumped accounts
```

- LM-HASH and NTLM-HASH values of the **cloudbase-init** account for ecs02

Figure 13-121 ecs02

```
----- BEGIN DUMP -----
c\l\o\u\i\n\i\t\:\1003\:\AAD3B435B51404EEAAD3B435B51404EE\:\5B635D5F5306E26E0EE66915D7C1CA9B\:\:
Guest\:\501\:\AAD3B435B51404EEAAD3B435B51404EE\:\31D6CFE0D16AE931B73C59D7E0C089C0\:\:
Administrator\:\500\:\AAD3B435B51404EEAAD3B435B51404EE\:\0501525C0083243750D23927A82070B6\:\:
----- END DUMP -----
3 dumped accounts
```

13.9.7 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 13-122](#).

Figure 13-122 Improper running of Cloud-Init

```
[root@ecs-8560 ~]# cloud-init -v
Traceback (most recent call last):
  File "/usr/bin/cloud-init", line 39, in <module>
    from cloudinit import patcher
ImportError: No module named cloudinit
[root@ecs-8560 ~]# cloud-init init --local
Traceback (most recent call last):
  File "/usr/bin/cloud-init", line 39, in <module>
    from cloudinit import patcher
ImportError: No module named cloudinit
[root@ecs-8560 ~]#
```

Possible Causes

The Python version used by Cloud-Init was incorrect.

Solution

Change the Python version used by Cloud-Init to the source version. To do so, change the environment variable value of `/usr/bin/cloud-init` from the default value `#!/usr/bin/python` to `#!/usr/bin/python2.6`.

Figure 13-123 Changing the Python version

```
[root@ecs-8560 ~]# head -n 1 /usr/bin/cloud-init
#!/usr/bin/python2.6
[root@ecs-8560 ~]# ls /usr/bin/python* -lh
lrwxrwxrwx 1 root root 24 Jul 19 10:55 /usr/bin/python -> /usr/local/bin/python2.7
lrwxrwxrwx 1 root root 6 Jun 9 2017 /usr/bin/python2 -> python
-rwxr-xr-x 1 root root 8.9K Aug 18 2016 /usr/bin/python2.6
```

13.10 Network Configurations

13.10.1 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 13-9 lists ECS configurations.

Table 13-9 ECS configurations

Parameter	Configuration
Name	ecs_test

Parameter	Configuration
Image	CentOS 6.5 64bit
EIP	2
Primary NIC	eth0
Secondary NIC	eth1

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**.

13.10.2 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*.

13.10.3 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.

Fault Locating

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

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

Figure 13-124 Method of locating the failure to ping an EIP

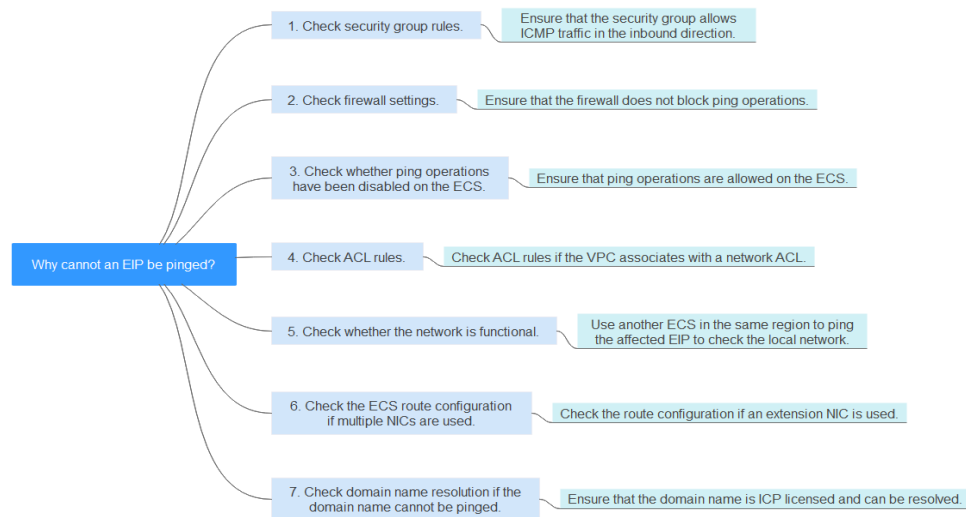


Table 13-10 Method of locating the failure to ping an EIP

Possible Cause	Solution
ICMP access rules are not added to the security group.	Add ICMP access rules to the security group. For details, see Checking Security Group Rules .
Ping operations are prohibited on the firewall.	Allow ping operations on the firewall. For details, see Checking Firewall Settings .
Ping operations are prohibited on the ECS.	Allow ping operations on the ECS. For details, see Checking Whether Ping Operations Have Been Disabled on the ECS .
Network ACL is associated.	If the VPC is associated with a network ACL, check the network ACL rules. For details, see Checking ACL Rules .
A network exception occurred.	Use another ECS in the same region to check whether the local network is functional. For details, see Checking Whether the Network Is Functional .

Possible Cause	Solution
Routes are incorrectly configured if multiple NICs are used.	If the network is inaccessible due to an extension NIC, the fault is generally caused by incorrect route configurations. To resolve this issue, see Checking the ECS Route Configuration If Multiple NICs Are Used .

Checking Security Group Rules

The ping operations use the ICMP protocol. Check whether the security group accommodating the ECS allows ICMP traffic in the inbound direction.

1. Under **Computing**, click **Elastic Cloud Server**.
2. On the **Elastic Cloud Server** page, click the name of the target ECS.
The page providing details about the ECS is displayed.
3. Click the **Security Groups** tab, expand the information of the security group, and view security group rules.
4. Click the security group ID.
The system automatically switches to the **Security Group** page.
5. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

Table 13-11 Security group rules

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

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

Checking Firewall Settings

If a firewall is enabled on the ECS, check whether the firewall blocks the ping operations.

Linux

1. Run the following command to check the firewall status, taking CentOS 7 as an example:
firewall-cmd --state
If **running** is displayed in the command output, the firewall has been enabled.
2. Check whether there is any ICMP rule blocking the ping operations.
iptables -L

If the command output shown in [Figure 13-125](#) is displayed, there is no ICMP rule blocking the ping operations.

Figure 13-125 Checking firewall rules

```
[root@ecs-3c4e ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    icmp -- anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    icmp -- anywhere             anywhere             icmp echo-reply
[root@ecs-3c4e ~]#
```

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

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

Windows

1. Log in to the Windows ECS, click the Windows icon in the lower left corner of the desktop, and choose **Control Panel > Windows Firewall**.
2. Click **Turn Windows Firewall on or off**.
View and set the firewall status.
3. If the firewall is **On**, go to **4**.
4. Check the ICMP rule statuses in the firewall.
 - a. In the navigation pane on the **Windows Firewall** page, click **Advanced settings**.
 - b. Enable the following rules:
Inbound Rules: File and Printer Sharing (Echo Request - ICMPv4-In)
Outbound Rules: File and Printer Sharing (Echo Request - ICMPv4-Out)
If IPv6 is enabled, enable the following rules:
Inbound Rules: File and Printer Sharing (Echo Request - ICMPv6-In)
Outbound Rules: File and Printer Sharing (Echo Request - ICMPv6-Out)

Figure 13-126 Inbound Rules

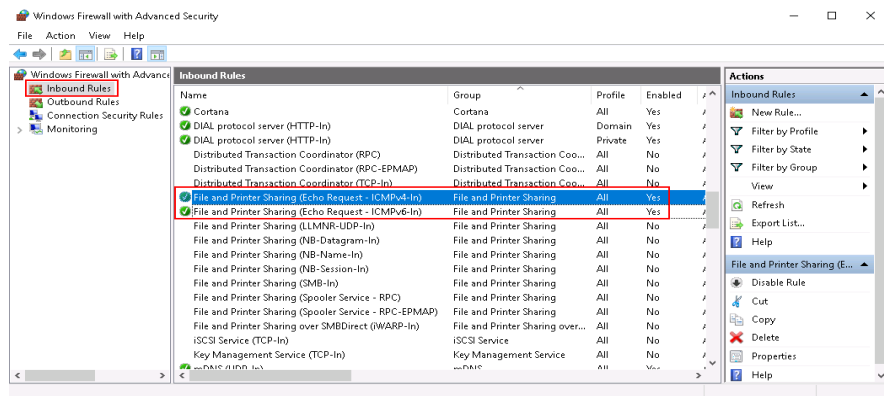
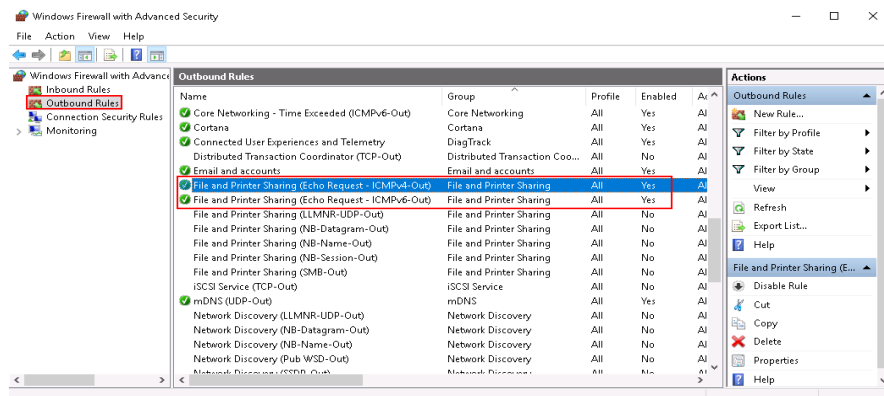


Figure 13-127 Outbound Rules



Checking Whether Ping Operations Have Been Disabled on the ECS

Windows

Enable ping operations using the CLI.

1. Start the **Run** dialog box. Enter **cmd** and press **Enter**.
2. Run the following command to enable ping operations:
netsh firewall set icmpsetting 8

Linux

Check the ECS kernel parameters.

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

Checking ACL Rules

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

1. Check whether the subnet of the ECS has been associated with a network ACL.
If an ACL name is displayed, the network ACL has been associated with the ECS.
2. Click the ACL name to view its status.
3. 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.

Checking Whether the Network Is Functional

1. Use another ECS in the same region to check whether the local network is functional.
Use another ECS in the same region to ping the affected EIP. If the EIP can be pinged, the VPC is functional. In such a case, rectify the local network fault and ping the affected EIP again.
2. Check whether the link is accessible.
A ping failure is caused by packet loss or long delay, which may be caused by link congestion, link node faults, or heavy load on the ECS.

Checking the ECS Route Configuration If Multiple NICs Are Used

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

- If the ECS has multiple NICs, check whether the default route is available.
 - a. Log in to the ECS and run the following command to check whether the default route is available:

ip route

Figure 13-128 Default route

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

- b. If the route is unavailable, run the following command to add it:
ip route add default via XXXX dev eth0

NOTE

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

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

13.10.4 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**

13.10.5 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.

13.10.6 How Can I Obtain the MAC Address of My ECS?

This section describes how to obtain the MAC address of an ECS.

NOTE

The MAC address of an ECS cannot be changed.

Linux (CentOS 6)

1. Log in to the Linux ECS.
2. Run the following command to view the MAC address of the ECS:
ifconfig

Figure 13-129 Obtaining the MAC address

```
[root@CentOS68-XEN ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr FA:16:3E:2A:36:DE
          inet addr:192.168.22.227  Bcast:192.168.22.255  Mask:255.255.255.0
          inet6 addr: fe80::f816:3eff:fe2a:36de/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4699 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2213 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:472826 (461.7 KiB)  TX bytes:438396 (428.1 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28 (28.0 b)  TX bytes:28 (28.0 b)
```

Linux (CentOS 7)

1. Log in to the Linux ECS.
2. Run the following command to view the MAC address of the ECS:

ifconfig

Figure 13-130 Obtaining the NIC information

```
[root@ecs-683a ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.65  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::f816:3eff:fec3:46fc  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:c3:46:fc  txqueuelen 1000  (Ethernet)
        RX packets 14457  bytes 20617950 (19.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1867  bytes 245185 (239.4 KiB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

3. Run the following command to view the MAC address of NIC **eth0**:

ifconfig eth0 |grep "ether"

Figure 13-131 Obtaining the MAC address of eth0

```
[root@ecs-683a ~]# ifconfig eth0 |grep "ether"
ether fa:16:3e:c3:46:fc txqueuelen 1000  (Ethernet)
[root@ecs-683a ~]#
```

4. Obtain the returned MAC address.

ifconfig eth0 |grep "ether" |awk '{print \$2}'

Figure 13-132 Obtaining the MAC address of eth0

```
[root@ecs-683a ~]# ifconfig eth0 |egrep "ether" |awk '{print $2}'  
fa:16:3e:c3:46:fc  
[root@ecs-683a ~]#
```

Windows

1. Press **Win+R** to start the **Run** text box.
2. Enter **cmd** and click **OK**.
3. Run the following command to view the MAC address of the ECS:

ipconfig /all

```
Ethernet adapter Ethernet 2:  
Connection-specific DNS Suffix . . . . . :  
Description . . . . . :  
Physical Address. . . . . :  
DHCP Enabled. . . . . :  
Autoconfiguration Enabled . . . . . :  
Link-Local IPv6 Address . . . . . :  
IPv4 Address. . . . . :  
Subnet Mask . . . . . :  
Lease Obtained. . . . . :  
Lease Expires . . . . . :  
Default Gateway . . . . . :  
DHCP Server . . . . . :  
DHCPv6 IAID . . . . . :  
DHCPv6 Client DUID. . . . . :  
DNS Servers . . . . . :  
NetBIOS over Tcpi. . . . . :
```

13.10.7 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 13-12](#) and [Table 13-13](#) list common test tool parameters.

Table 13-12 Common netperf parameters

Parameter	Description
-p	Port number
-H	IP address of the RX end
-t	Protocol used in packet transmitting, the value of which is TCP_STREAM in bandwidth tests
-l	Test duration

Parameter	Description
-m	Data packet size, which is suggested to be 1440 in bandwidth tests

Table 13-13 Common iperf3 parameters

Parameter	Description
-p	Port number
-c	IP address of the RX end
-u	UDP packets
-b	TX bandwidth
-t	Test duration
-l	Data packet size, which is suggested to be 16 in PPS tests
-A	ID of the vCPU used by iperf3 In this section, the maximum number of 16 vCPUs is used as an example for each ECS. If an ECS has 8 vCPUs, the -A value ranges from 0 to 7.

Test Preparations

Step 1 Prepare ECSs.

Ensure that both type and specifications of the tested ECS and auxiliary ECSs are the same. In addition, these ECSs are deployed in the same ECS group with anti-affinity enabled.

Table 13-14 Preparations

Category	Quantity	Image	Specifications	IP Address
Tested ECS	1	CentOS 7.4 64bit (recommended)	At least eight vCPUs	192.168.2.10
Auxiliary ECS	8	CentOS 7.4 64bit (recommended)	At least 8 vCPUs	192.168.2.11-19 2.168.2.18

Step 2 Install the netperf, iperf3, and sar test tools on both the tested ECS and auxiliary ECSs.

[Table 13-15](#) lists the procedures for installing these tools.

Table 13-15 Installing test tools

Tool	Procedure
netperf	<ol style="list-style-type: none"> 1. Run the following command to install gcc: yum -y install unzip gcc gcc-c++ 2. Run the following command to download the netperf installation package: wget --no-check-certificate https://github.com/HewlettPackard/netperf/archive/netperf-2.7.0.zip -O netperf-2.7.0.zip 3. Run the following commands to decompress the installation package and install netperf: unzip netperf-2.7.0.zip cd netperf-netperf-2.7.0/ ./configure && make && make install
iperf3	<ol style="list-style-type: none"> 1. Run the following command to download the iperf3 installation package: wget --no-check-certificate https://codeload.github.com/esnet/iperf/zip/master -O iperf3.zip 2. Run the following commands to decompress the installation package and install iperf3: unzip iperf3.zip cd iperf-master/ ./configure && make && make install
sar	Run the following command to install sar: yum -y install sysstat

Step 3 Enable NIC multi-queue.

Perform the following operations on both tested ECS and auxiliary ECSs.

1. Run the following command to check the number of queues supported by the ECSs:

```
ethtool -l eth0 | grep -i Pre -A 5 | grep Combined
```

2. Run the following command to enable NIC multi-queue:

```
ethtool -L eth0 combined X
```

In the preceding command, *X* is the number of queues obtained in [Step 3.1](#).

----End

TCP Bandwidth Test (Using netperf)

Perform the test on multiple flows. This section 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:

```
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 13-12](#).

```
##The IP address is for the first auxiliary ECS.
```

```
netperf -H 192.168.2.11 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.11 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
##The IP address is for the second auxiliary ECS.
```

```
netperf -H 192.168.2.12 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.12 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
##The IP address is for the third auxiliary ECS.
```

```
netperf -H 192.168.2.13 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.13 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
##The IP address is for the fourth auxiliary ECS.
```

```
netperf -H 192.168.2.14 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.14 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
##The IP address is for the fifth auxiliary ECS.
```

```
netperf -H 192.168.2.15 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.15 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
##The IP address is for the sixth auxiliary ECS.
```

```
netperf -H 192.168.2.16 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.16 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
##The IP address is for the seventh auxiliary ECS.
```

```
netperf -H 192.168.2.17 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.17 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
##The IP address is for the eighth auxiliary ECS.
```

```
netperf -H 192.168.2.18 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.18 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

Step 2 Test the TCP RX bandwidth.

1. Start the netserver process on the tested ECS.

```
##The port number is for the first auxiliary ECS.
```

```
netserver -p 12001
```

```
netserver -p 12002
```

```
##The port number is for the second auxiliary ECS.
```

```
netserver -p 12003
```

```
netserver -p 12004
```

```
##The port number is for the third auxiliary ECS.
```

```
netserver -p 12005
```

```
netserver -p 12006
```

##The port number is for the fourth auxiliary ECS.

```
netserver -p 12007
```

```
netserver -p 12008
```

##The port number is for the fifth auxiliary ECS.

```
netserver -p 12009
```

```
netserver -p 12010
```

##The port number is for the sixth auxiliary ECS.

```
netserver -p 12011
```

```
netserver -p 12012
```

##The port number is for the seventh auxiliary ECS.

```
netserver -p 12013
```

```
netserver -p 12014
```

##The port number is for the eighth auxiliary ECS.

```
netserver -p 12015
```

```
netserver -p 12016
```

2. Start the netperf process on all auxiliary ECSs.

Log in to auxiliary ECS 1.

```
netperf -H 192.168.2.10 -p 12001 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.10 -p 12002 -t TCP_STREAM -l 300 -- -m 1440 &
```

Log in to auxiliary ECS 2.

```
netperf -H 192.168.2.10 -p 12003 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.10 -p 12004 -t TCP_STREAM -l 300 -- -m 1440 &
```

Log in to auxiliary ECS 3.

```
netperf -H 192.168.2.10 -p 12005 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.10 -p 12006 -t TCP_STREAM -l 300 -- -m 1440 &
```

Log in to auxiliary ECS 4.

```
netperf -H 192.168.2.10 -p 12007 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.10 -p 12008 -t TCP_STREAM -l 300 -- -m 1440 &
```

Log in to auxiliary ECS 5.

```
netperf -H 192.168.2.10 -p 12009 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.10 -p 12010 -t TCP_STREAM -l 300 -- -m 1440 &
```

Log in to auxiliary ECS 6.

```
netperf -H 192.168.2.10 -p 12011 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.10 -p 12012 -t TCP_STREAM -l 300 -- -m 1440 &
```

Log in to auxiliary ECS 7.

```
netperf -H 192.168.2.10 -p 12013 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.10 -p 12014 -t TCP_STREAM -l 300 -- -m 1440 &
```

Log in to auxiliary ECS 8.

```
netperf -H 192.168.2.10 -p 12015 -t TCP_STREAM -l 300 -- -m 1440 &
```

```
netperf -H 192.168.2.10 -p 12016 -t TCP_STREAM -l 300 -- -m 1440 &
```

Step 3 Analyze the test result.

After the test is complete, the output of the netperf process on one TX end is shown in [Figure 13-133](#). The final result is the sum of the test results of the netperf processes on all TX ends.

Figure 13-133 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 &
```

```
iperf3 -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 13-13](#).

```
##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 13-13](#).

```
##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 &
```

```
iperf3 -s -p 12008 -A 7 -i 60 &
```



```
##Auxiliary ECS 5  
iperf3 -s -p 12009 -A 8 -i 60 &  
iperf3 -s -p 12010 -A 9 -i 60 &
```

```
##Auxiliary ECS 6  
iperf3 -s -p 12011 -A 10 -i 60 &  
iperf3 -s -p 12012 -A 11 -i 60 &
```

```
##Auxiliary ECS 7  
iperf3 -s -p 12013 -A 12 -i 60 &  
iperf3 -s -p 12014 -A 13 -i 60 &
```

```
##Auxiliary ECS 8  
iperf3 -s -p 12015 -A 14 -i 60 &  
iperf3 -s -p 12016 -A 15 -i 60 &
```

2. Start the client process on all auxiliary ECSs. For details about common iperf3 parameters, see [Table 13-13](#).

Log in to auxiliary ECS 1.

```
iperf3 -c 192.168.2.10 -p 12001 -u -b 100M -t 300 -l 16 -A 0 &  
iperf3 -c 192.168.2.10 -p 12002 -u -b 100M -t 300 -l 16 -A 1 &
```

Log in to auxiliary ECS 2.

```
iperf3 -c 192.168.2.10 -p 12003 -u -b 100M -t 300 -l 16 -A 0 &  
iperf3 -c 192.168.2.10 -p 12004 -u -b 100M -t 300 -l 16 -A 1 &
```

Log in to auxiliary ECS 3.

```
iperf3 -c 192.168.2.10 -p 12005 -u -b 100M -t 300 -l 16 -A 0 &  
iperf3 -c 192.168.2.10 -p 12006 -u -b 100M -t 300 -l 16 -A 1 &
```

Log in to auxiliary ECS 4.

```
iperf3 -c 192.168.2.10 -p 12007 -u -b 100M -t 300 -l 16 -A 0 &  
iperf3 -c 192.168.2.10 -p 12008 -u -b 100M -t 300 -l 16 -A 1 &
```

Log in to auxiliary ECS 5.

```
iperf3 -c 192.168.2.10 -p 12009 -u -b 100M -t 300 -l 16 -A 0 &  
iperf3 -c 192.168.2.10 -p 12010 -u -b 100M -t 300 -l 16 -A 1 &
```

Log in to auxiliary ECS 6.

```
iperf3 -c 192.168.2.10 -p 12011 -u -b 100M -t 300 -l 16 -A 0 &  
iperf3 -c 192.168.2.10 -p 12012 -u -b 100M -t 300 -l 16 -A 1 &
```

Log in to auxiliary ECS 7.

```
iperf3 -c 192.168.2.10 -p 12013 -u -b 100M -t 300 -l 16 -A 0 &  
iperf3 -c 192.168.2.10 -p 12014 -u -b 100M -t 300 -l 16 -A 1 &
```

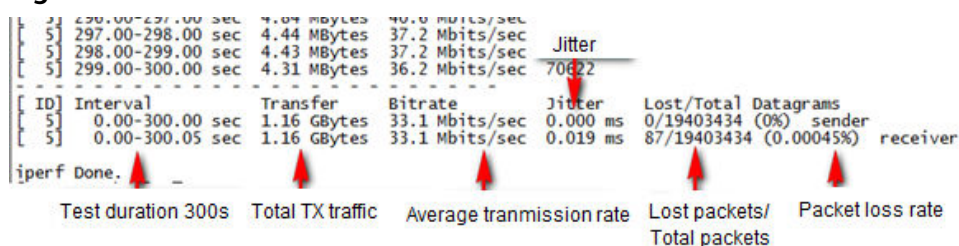
Log in to auxiliary ECS 8.

```
iperf3 -c 192.168.2.10 -p 12015 -u -b 100M -t 300 -l 16 -A 0 &  
iperf3 -c 192.168.2.10 -p 12016 -u -b 100M -t 300 -l 16 -A 1 &
```

Step 3 Analyze the test result.

[Figure 13-134](#) shows an example of the UDP PPS test result.

Figure 13-134 UDP PPS test result

**NOTE**

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

13.10.8 Why Cannot I Use DHCP to Obtain a Private IP Address?**Symptom**

DHCP cannot be used to obtain a private IP address. The symptom varies based on the OS.

- For Linux, a private IP address cannot be assigned.
- For Windows, a private IP address is changed to an IP address in the 169.254 network segment, which is different from the private IP address displayed on the ECS console.

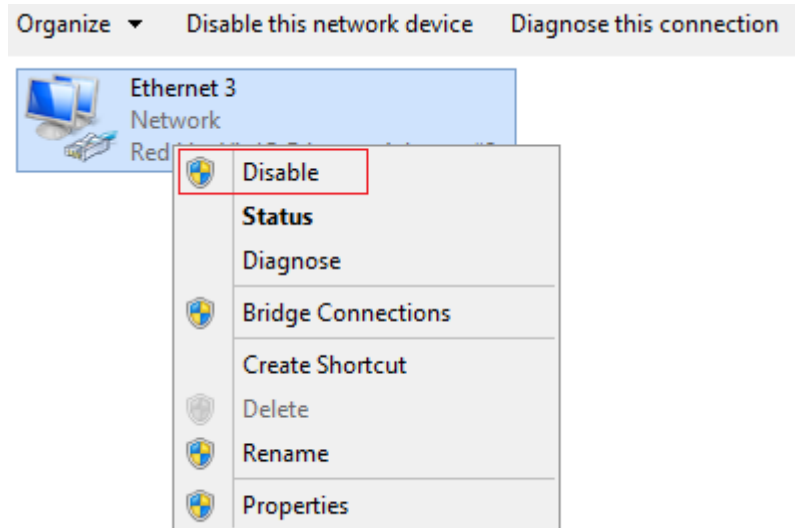
Solution

Step 1 Check whether dhclient is running in the ECS.

1. Log in to the ECS and run the following command:

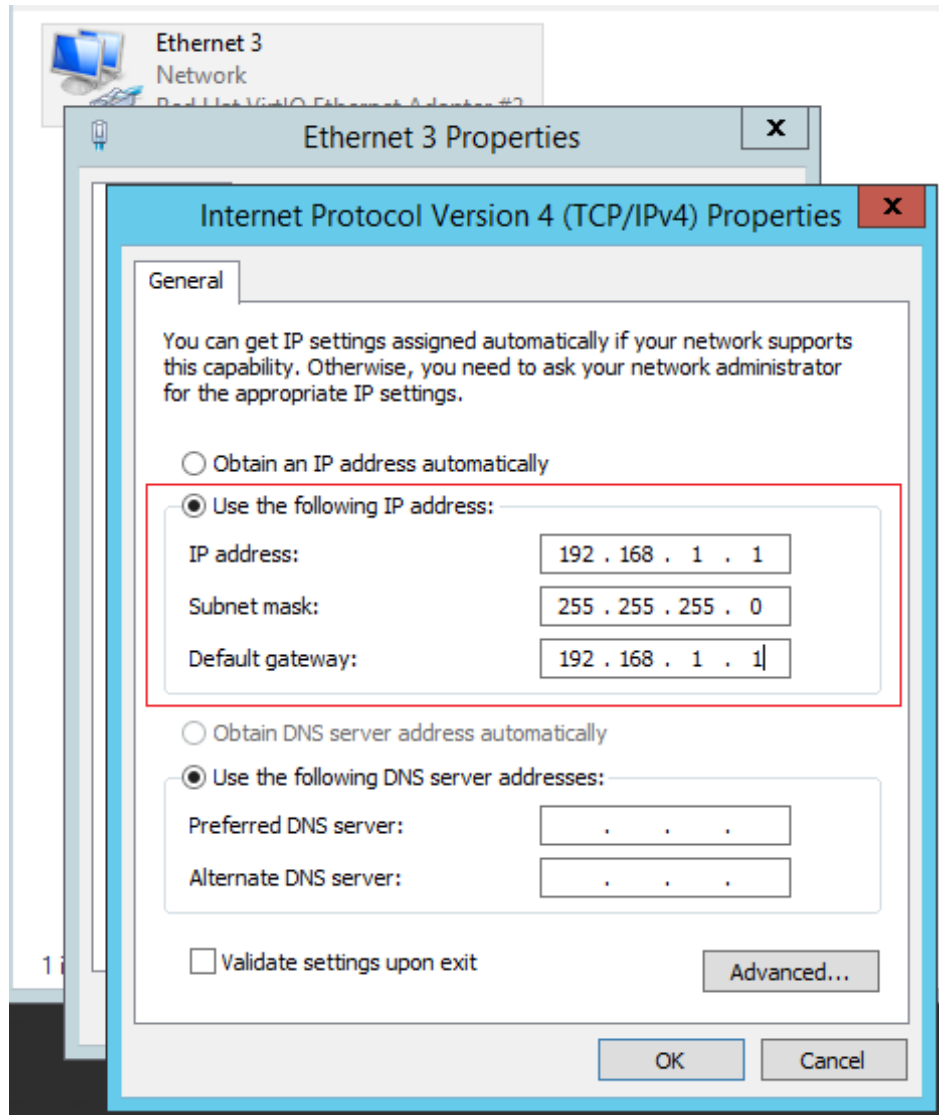
```
ps -ef | grep dhclient
```

2. If the process is not running, log in to the ECS, and restart the ECS NIC or initiate a DHCP request.
 - Linux
Run the **dhclient eth0, ifdown eth0 + ifup eth0, or dhcpcd eth0** command.
 - Windows
Right-click a local area connection and choose **Disable** from the shortcut menu. Then, choose **Enable**.



Step 2 Handle the issue if the DHCP client fails to work for a long time (for example, the issue recurs after the NIC is restarted).

1. Configure a static IP address.
 - Windows
 - a. Right-click **Local Area Connection** and choose **Properties** from the shortcut menu.
 - b. In the displayed dialog box, select **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties**, and modify parameter settings.



- Linux
 - a. Log in to the ECS and run the following command to modify parameter settings:

vi /etc/sysconfig/network-scripts/ifcfg-eth0

```
BOOTPROTO=static
IPADDR=192.168.1.100 #IP address (modified)
NETMASK=255.255.255.0 #Mask (modified)
GATEWAY=192.168.1.1 #Gateway IP address (modified)
```

- b. Run the following command to restart the network:

service network restart

2. Select an image in which DHCP runs stably.

- Native Windows series, such as Windows Web Server 2008 R2 64bit, Windows Server DataCenter 2008 R2 64bit, Windows Server Enterprise 2008 SP2 64bit, or Windows Server Enterprise 2008 R2 64bit
- CentOS series, requiring you to add **PERSISTENT_DHCLIENT="y"** in **/etc/sysconfig/network-scripts/ifcfg-ethX**
- Ubuntu series, such as Ubuntu 1004

Step 3 If the fault persists, obtain the messages in `/var/log/messages` on the affected ECS, use the MAC address of the affected NIC to filter the desired log, and check whether there is any process preventing DHCP from obtaining an IP address.

Step 4 If the fault persists, contact customer service for technical support.

----End

13.10.9 How Can I View and Modify Kernel Parameters of a Linux ECS?

This document describes common Linux kernel parameters and how to view and modify them. 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 13-16](#).
- Back up key ECS data before modifying kernel parameter settings.

Background

Table 13-16 Common Linux kernel parameters

Parameter	Description
<code>net.core.rmem_default</code>	Specifies the default size (in bytes) of the window for receiving TCP data.
<code>net.core.rmem_max</code>	Specifies the maximum size (in bytes) of the window for receiving TCP data.
<code>net.core.wmem_default</code>	Specifies the default size (in bytes) of the window for transmitting TCP data.
<code>net.core.wmem_max</code>	Specifies the maximum size (in bytes) of the window for transmitting TCP data.
<code>net.core.netdev_max_backlog</code>	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.
<code>net.core.somaxconn</code>	Defines the maximum length of the listening queue for each port in the system. This parameter applies globally.
<code>net.core.optmem_max</code>	Specifies the maximum size of the buffer allowed by each socket.

Parameter	Description
net.ipv4.tcp_mem	<p>Uses the TCP stack to show memory usage in memory pages (4 KB generally).</p> <p>The first value is the lower limit of memory usage.</p> <p>The second value is the upper limit of the load added to the buffer when the memory is overloaded.</p> <p>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.</p>
net.ipv4.tcp_rmem	<p>Specifies the memory used by sockets for automatic optimization.</p> <p>The first value is the minimum number of bytes allocated to the socket buffer for receiving data.</p> <p>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.</p> <p>The third value is the maximum number of bytes allocated to the socket buffer for receiving data. This value is overwritten by rmem_max.</p>
net.ipv4.tcp_wmem	<p>Specifies the memory used by sockets for automatic optimization.</p> <p>The first value is the minimum number of bytes allocated to the socket buffer for transmitting data.</p> <p>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.</p> <p>The third value is the maximum number of bytes allocated to the socket buffer for transmitting data. This value is overwritten by wmem_max.</p>
net.ipv4.tcp_keepalive_time	<p>Specifies the interval at which keepalive detection messages are sent in seconds for checking TCP connections.</p>
net.ipv4.tcp_keepalive_intvl	<p>Specifies the interval at which keepalive detection messages are resent in seconds when no response is received.</p>
net.ipv4.tcp_keepalive_probes	<p>Specifies the maximum number of keepalive detection messages that are sent to determine a TCP connection failure.</p>

Parameter	Description
net.ipv4.tcp_sack	Enables selective acknowledgment (value 1 indicates enabled). This configuration allows the transmitter to resend only lost packets, thereby improving system performance. However, this configuration will increase the CPU usage. You are suggested to enable selective acknowledgment for WAN communication.
net.ipv4.tcp_fack	Enables forwarding acknowledgment for selective acknowledgment (SACK), thereby reducing congestion. You are suggested to enable forwarding acknowledgment.
net.ipv4.tcp_timestamps	Specifies a TCP timestamp, which will add 12 bytes in the TCP packet header. This configuration calculates RTT using RFC1323, a more precise retransmission method upon timeout than retransmission. You are suggested to use this configuration for higher system performance.
net.ipv4.tcp_window_scaling	Enables RFC1323-based window scaling by setting the parameter value to 1 if the TCP window is larger than 64 KB. The maximum TCP window is 1 GB. This parameter takes effect only when window scaling is enabled on both ends of the TCP connection.
net.ipv4.tcp_syncookies	Specifies whether to enable TCP synchronization (syncookie). This configuration prevents socket overloading when a large number of connections are attempted to set up. CONFIG_SYN_COOKIES must be enabled in the kernel for compilation. The default value is 0 , indicating that TCP synchronization is disabled.
net.ipv4.tcp_tw_reuse	Specifies whether a TIME-WAIT socket (TIME-WAIT port) can be used for new TCP connections. NOTE This parameter cannot be set to 1 if NAT is enabled. Otherwise, an error will occur in remote ECS logins.
net.ipv4.tcp_tw_recycle	Allows fast recycle of TIME-WAIT sockets. NOTE This parameter cannot be set to 1 if NAT is enabled. Otherwise, an error will occur in remote ECS logins.
net.ipv4.tcp_fin_timeout	Specifies the time (in seconds) during which a socket TCP connection that is disconnected from the local end retains in FIN-WAIT-2 state. Process suspension may be caused by the disconnection from the peer end, continuous connection from the peer end, or unexpected causes.

Parameter	Description
net.ipv4.ip_local_port_range	Specifies local port numbers allowed by TCP/UDP.
net.ipv4.tcp_max_syn_backlog	Specifies the maximum number of connection requests that are not acknowledged by the peer end and that can be stored in the queue. The default value is 1024 . If the server is frequently overloaded, try to increase the value.
net.ipv4.tcp_low_latency	This option should be disabled if the TCP/IP stack is used for high throughput, low latency.
net.ipv4.tcp_westwood	Enables the congestion control algorithm on the transmitter end to evaluate throughput and improve the overall bandwidth utilization. You are suggested to enable the congestion control algorithm for WAN communication.
net.ipv4.tcp_bic	Enables binary increase congestion for fast long-distance networks so that the connections with operations being performed at a rate of Gbit/s can be functional. You are suggested to enable binary increase congestion for WAN communication.
net.ipv4.tcp_max_tw_buckets	Specifies the number of TIME_WAIT buckets, which defaults to 180000 . If the number of buckets exceeds the default value, extra ones will be cleared.
net.ipv4.tcp_synack_retries	Specifies the number of times that SYN+ACK packets are retransmitted in SYN_RECV state.
net.ipv4.tcp_abort_on_overflow	When this parameter is set to 1 , if the system receives a large number of requests within a short period of time but fails to process them, the system will send reset packets to terminate the connections. It is recommended that you improve system processing capabilities by optimizing the application efficiency but not simply performing reset operations. Default value: 0
net.ipv4.route.max_size	Specifies the maximum number of routes allowed by the kernel.
net.ipv4.ip_forward	Forward packets between interfaces.
net.ipv4.ip_default_ttl	Specifies the maximum number of hops that a packet can pass through.
net.netfilter.nf_conntrack_tcp_timeout_established	Clears iptables connections that are inactive for a specified period of time.

Parameter	Description
net.netfilter.nf_conntrack_max	Specifies the maximum value of hash entries.

Viewing Kernel Parameters

- Method 1: Run the cat command in **/proc/sys** to view file content.
/proc/sys/ is a pseudo directory generated after the Linux kernel is started. The **net** folder in this directory stores all kernel parameters that have taken effect in the system. The directory tree structure is determined based on complete parameter names. For example, **net.ipv4.tcp_tw_recycle** corresponds to the **/proc/sys/net/ipv4/tcp_tw_recycle** file, and the content of the file is the parameter value.

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:

```
sysctl -w net.ipv4.tcp_tw_recycle="0"
```

- b. Run the following command to change the parameter value in the **/etc/sysctl.conf** file:

```
vi /etc/sysctl.conf
```

- c. Run the following command for the configuration to take effect:

```
/sbin/sysctl -p
```

13.10.10 How Can I Configure Port Redirection?

Requirement

It is expected that the EIP and port on ECS 1 accessed from the Internet can be automatically redirected to the EIP and port on ECS 2.

Windows

For example, to redirect port 8080 on ECS 1 bound with EIP 192.168.10.43 to port 18080 on ECS 2 bound with EIP 192.168.10.222, perform the following operations on ECS 1.

NOTE

Ensure that the desired ports have been enabled on the ECS security group and firewall.

Open the **cmd** window and run the following command (Windows Server 2012 is used as an example):

```
netsh interface portproxy add v4tov4 listenaddress=192.168.10.43  
listenport=8080 connectaddress=192.168.10.222 connectport=18080
```

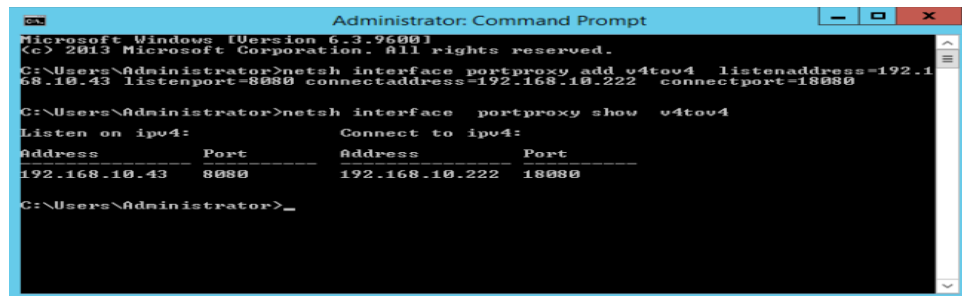
To cancel port redirection, run the following command:

```
netsh interface portproxy delete v4tov4 listenaddress=192.168.10.43  
listenport=8080
```

Run the following command to view all port redirections configured on the ECS:

```
netsh interface portproxy show v4tov4
```

Figure 13-135 Port redirections on Windows



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>netsh interface portproxy add v4tov4 listenaddress=192.168.10.43 listenport=8080 connectaddress=192.168.10.222 connectport=18080

C:\Users\Administrator>netsh interface portproxy show v4tov4

Listen on ipv4:          Connect to ipv4:
-----
Address      Port      Address      Port
-----
192.168.10.43  8080     192.168.10.222  18080

C:\Users\Administrator>_
```

Linux

For example, to redirect port 1080 on ECS 1 to port 22 on ECS 2 with the following configurations:

Private IP address and EIP of ECS 1: 192.168.72.10 and 123.xxx.xxx.456

Private IP address of ECS 2: 192.168.72.20

Step 1 Log in to Linux ECS 1.

1. Run the following command to modify the configuration file:

```
vi /etc/sysctl.conf
```

2. Add **net.ipv4.ip_forward = 1** to the file.

3. Run the following command to complete the modification:

```
sysctl -p /etc/sysctl.conf
```

Step 2 Run the following commands to add rules to the **nat** table in **iptables** so that the access to port 1080 on ECS 1 can be redirected to port 22 on ECS 2:

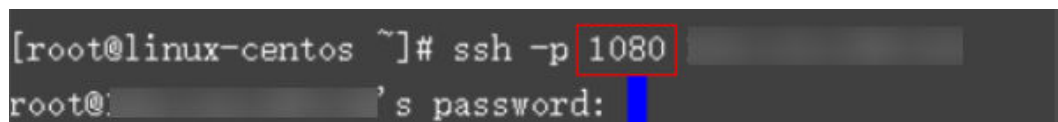
```
iptables -t nat -A PREROUTING -d 192.168.72.10 -p tcp --dport 1080 -j DNAT --to-destination 192.168.72.20:22
```

```
iptables -t nat -A POSTROUTING -d 192.168.72.20 -p tcp --dport 22 -j SNAT --to 192.168.72.10
```

Step 3 Run the following command to log in to port 1080 on ECS 1 for check:

```
ssh -p 1080 123.xxx.xxx.456
```

Figure 13-136 Port redirections on Linux



```
[root@linux-centos ~]# ssh -p 1080 [redacted]
root@[redacted]'s password: [redacted]
```

Enter the password to log in to ECS 2 with hostname **ecs-inner**.

Figure 13-137 Logging in to ECS 2



```
[root@ecs-inner ~]#
```

----End

13.10.11 Can the ECSs of Different Accounts Communicate over an Intranet?

No. The ECSs of different accounts cannot communicate with each other over an intranet.

13.10.12 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.

13.11 Resource Management and Tags

13.11.1 How Can I Create and Delete Tags and Search for ECSs by Tag?

Creating a Tag

1. Log in to the management console.
2. Select the region where the ECS is located.
3. Under **Computing**, click **Elastic Cloud Server**.
4. Click the name of the target ECS.
The page providing details about the ECS is displayed.
5. Click **Tags** and then **Add Tag**.
6. Enter the tag key and value, and click **OK**.

Searching for ECSs by Tag

1. Log in to the management console.
2. Select the region where the ECS is located.
3. On the **Elastic Cloud Server** page, search for ECSs by tag.
4. In the search bar, select **Tag** and then the tag key and value, and click **OK**.

Deleting a Tag

1. Log in to the management console.
2. Select the region where the ECS is located.
3. Click **Elastic Cloud Server**.
4. Click the name of the target ECS.
5. On the page providing details about the ECS, click **Tags**, locate the row containing the target tag, and click **Delete** in the **Operation** column.

13.12 Resource Monitoring

13.12.1 Troubleshooting High Bandwidth or CPU Usage of a Windows ECS

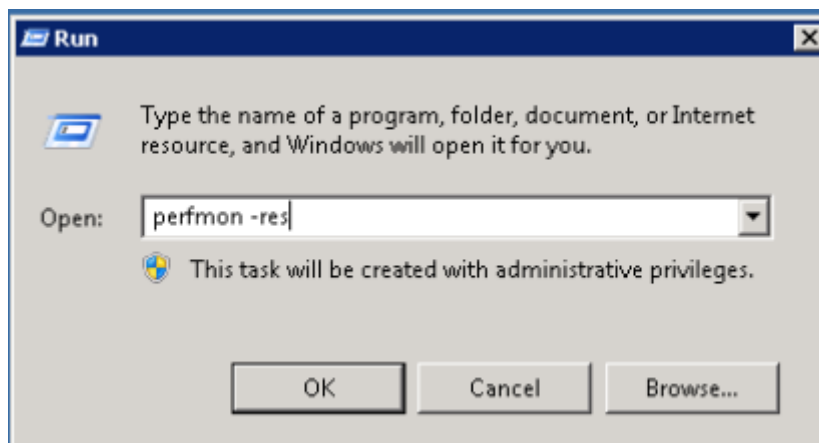
If your Windows ECS runs slowly or is inaccessible unexpectedly, the bandwidth or CPU usage of the ECS may be excessively high. If you have using Cloud Eye, the system automatically sends an alarm to you when the bandwidth or CPU usage reaches the threshold specified in the rule.

To handle this issue, perform the following operations:

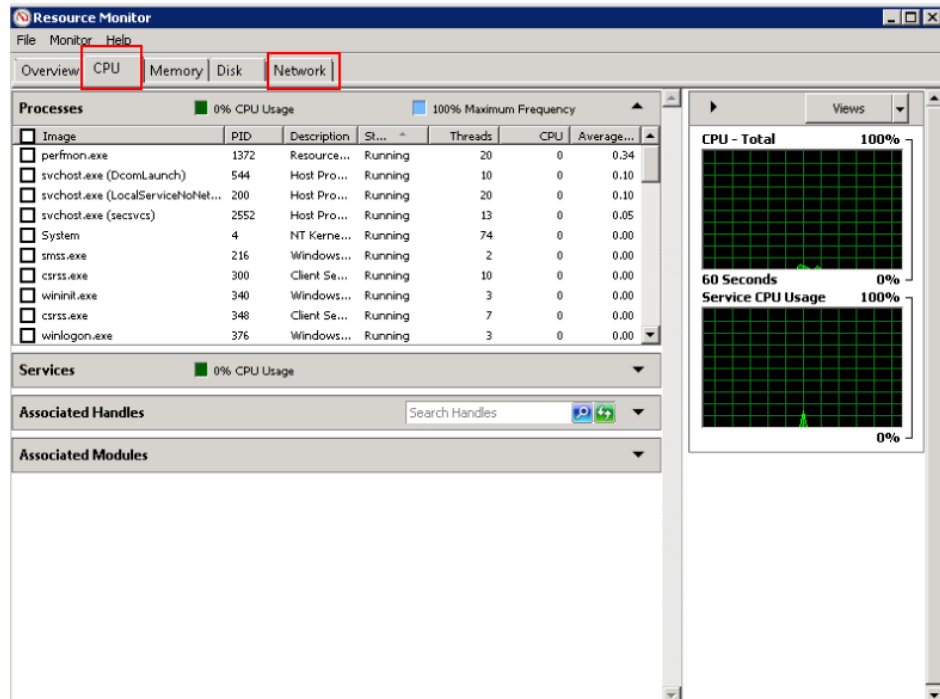
1. **Fault locating:** identifies the processes leading to high bandwidth or CPU usage.
Windows OSs offer multiple tools to locate faults, including Task Manager, Performance Monitor, Resource Monitor, Process Explorer, Xperf (supported by versions later than Windows Server 2008), and obtained full memory dump.
2. **Troubleshooting:** Check whether the processes are malicious and handle the issue accordingly.
 - If the processes are not malicious, optimize their programs or .
 - If the processes are malicious, use a third-party tool to automatically stop the processes.

Locating the Fault

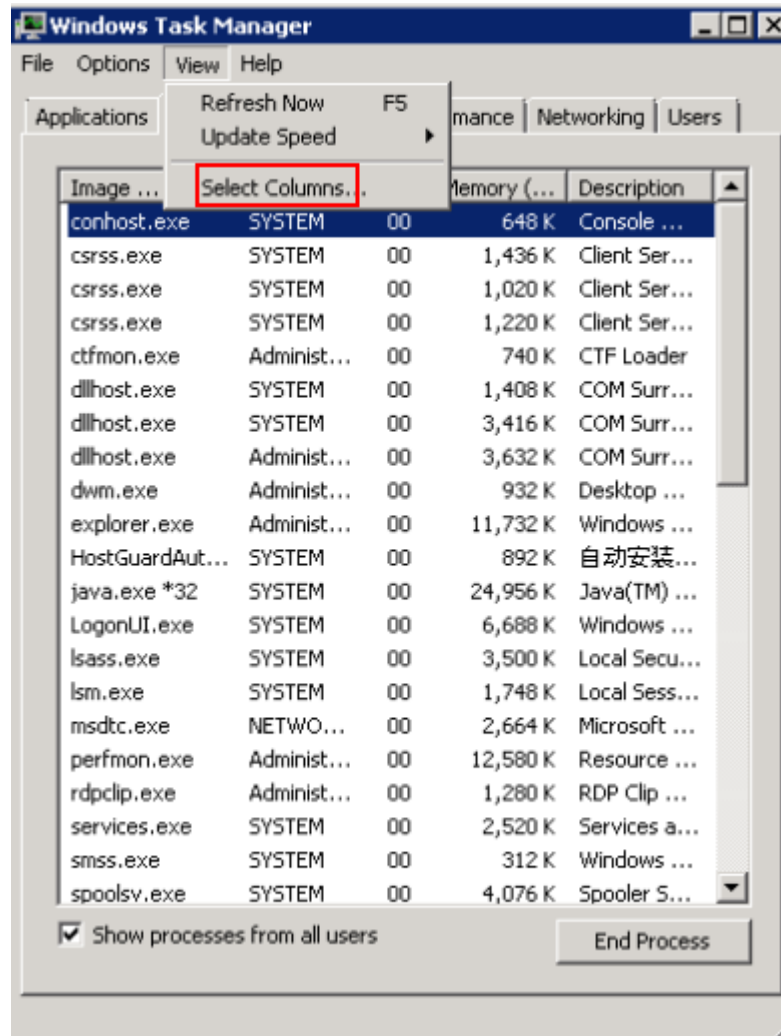
1. In the lower left corner of the ECS desktop, choose **Start > Run**.
2. In the **Open** dialog box, enter **perfmon -res**.



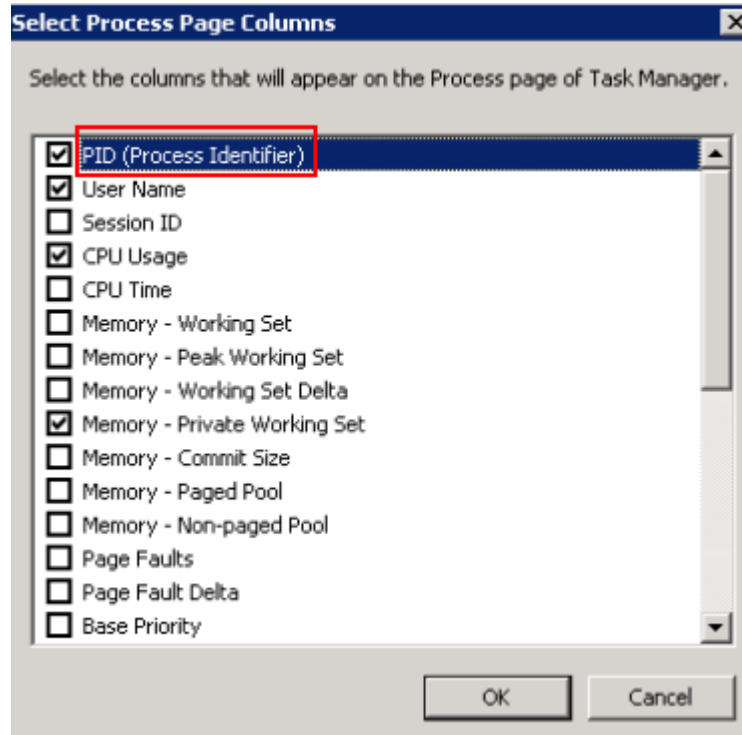
3. On the **Resource Monitor** page, click the **CPU** or **Network** tab to view the CPU or bandwidth usage.



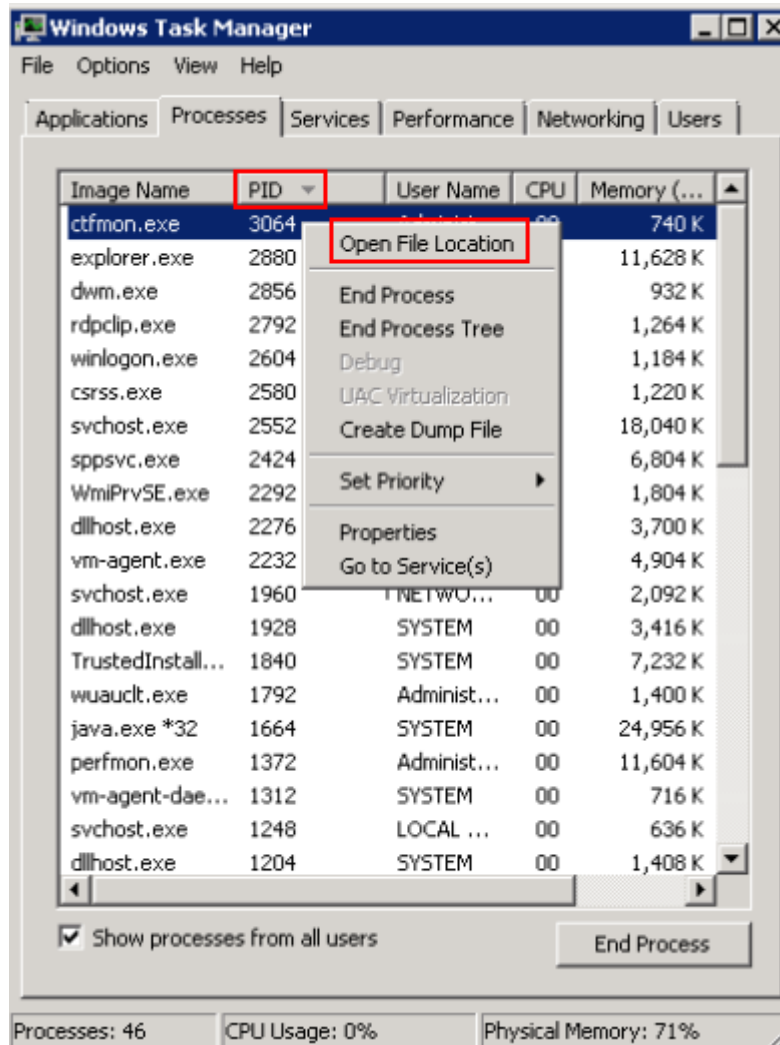
4. Obtain the IDs and names of the processes with high CPU or bandwidth usage.
5. Press **Ctrl+Alt+Delete** to start Windows Task Manager.
The following describes how to display PIDs in Task Manager, locate a process, and check whether it is malicious.
 - a. Click the **Processes** tab.
 - b. Choose **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, or .
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](#).

13.12.2 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 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 .
 - 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, 9:09, 1 user, load average: 0.00, 0.01, 0.05
Tasks: 80 total, 1 running, 79 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.2 us, 0.3 sy, 0.0 ni, 99.5 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 3880024 total, 2963304 free, 178384 used, 738336 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 3434808 avail Mem

  PID USER  PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 8115 root   20   0 161896 2216 1564 R  0.3  0.1   0:00.01 top
    1 root   20   0 125480 3884 2604 S  0.0  0.1   0:11.32 systemd
    2 root   20   0     0     0     0 S  0.0  0.0   0:00.00 kthreadd
    3 root   20   0     0     0     0 S  0.0  0.0   0:00.04 ksoftirqd/0
    5 root    0 -20     0     0     0 S  0.0  0.0   0:00.00 kworker/0:0H
    7 root   rt    0     0     0     0 S  0.0  0.0   0:00.18 migration/0
    8 root   20   0     0     0     0 S  0.0  0.0   0:00.00 rcu_bh
    9 root   20   0     0     0     0 S  0.0  0.0   7:32.18 rcu_sched
   10 root    0 -20     0     0     0 S  0.0  0.0   0:00.00 lru-add-drain
```

3. View the command output.

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

The current system time is 20:56:02; the ECS has been running for 37 days; there is one login user; the last three values indicate the average CPU load in the last 1 minute, 5 minutes, and 15 minutes, respectively.

- The third line in the command output shows the overall CPU usage.
- The fourth line in the command output shows the overall memory usage.
- The lower part of the command output shows the resource usage of each process.

NOTE

1. On the **top** page, enter **q** or press **Ctrl+C** to exit.
2. Alternatively, click **Input Command** in the upper right corner of the VNC login page, paste or enter commands in the displayed dialog box, and click **Send**.
3. Common parameters in top commands are as follows:
 - s: Change the image update frequency.
 - l: Show or hide the first line for the top information.
 - t: Show or hide the second line for tasks and the third line for CPUs.
 - m: Show or hide the fourth line for Mem and the fifth line for Swap.
 - N: Sort processes by PID in ascending or descending order.
 - P: Sort processes by CPU usage in ascending or descending order.
 - M: Sort processes by memory usage in ascending or descending order.
 - h: Show help for commands.
 - n: Set the number of processes displayed in the process list.
4. Run the **ll /proc/PID/exe** command to obtain the program file specified by a PID.

```
lroot@elb-mq01 sysconfigl# ll /proc/4243/exe
lrwxrwxrwx 1 root root 0 Mar 18 11:46 /proc/4243/exe -> /CloudResetPwdUpdateAgent/depend/jre1.8.0_131/bin/java
```

Troubleshooting High CPU Usage

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

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

- For the detected malicious processes

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

- Press the **k** key during the execution of the top command.
- Enter the PID of the process to be stopped.

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

```
top - 21:07:38 up 37 days, 9:21, 1 user, load average: 0.01, 0.02, 0.05
Tasks: 81 total, 1 running, 79 sleeping, 1 stopped, 0 zombie
%Cpu(s): 0.0 us, 3.2 sy, 0.0 ni, 96.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 3880024 total, 2961520 free, 178960 used, 739544 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 3434216 avail Mem
PID to signal/kill [default pid = 1] 52
  PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
   1 root  20  0 125480 3884 2604 S  0.0  0.1 0:11.32 systemd
   2 root  20  0 0 0 0 S  0.0  0.0 0:00.00 kthreadd
```

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

```
top - 21:07:38 up 37 days, 9:21, 1 user, load average: 0.01, 0.02, 0.05
Tasks: 81 total, 1 running, 79 sleeping, 1 stopped, 0 zombie
%Cpu(s): 0.0 us, 3.2 sy, 0.0 ni, 96.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 3880024 total, 2961520 free, 178960 used, 739544 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 3434216 avail Mem
Send pid 52 signal [15/sigterm]
  PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
   1 root  20  0 125480 3884 2604 S  0.0  0.1 0:11.32 systemd
   2 root  20  0 0 0 0 S  0.0  0.0 0:00.00 kthreadd
```

- For the **kswapd0** process

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

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

```
Tasks: 81 total, 1 running, 79 sleeping, 1 stopped, 0 zombie
%Cpu(s): 0.2 us, 52.2 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 3880024 total, 3014820 free, 179024 used, 686180 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 3433948 avail Mem
  PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
   36 root  20  0 0 0 0 S 99.0  0.0 964:10.45 kswapd0
 4595 nginx 20  0 125392 3576 1040 S  0.3  0.1 60:04.91 nginx
   1 root  20  0 125480 3884 2604 S  0.0  0.1 0:11.47 systemd
```

- 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**:

yum install nethogs -y

After the installation, run the **netgos** 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:

nethogs eth1

```
NetHogs version 0.8.5
```

PID	USER	PROGRAM	DEV	SENT	RECEIVED
4596	nginx	nginx: worker process	eth1	34.360	3.267 KB/sec
?	root	192.168.0.92:90-100.125.68.19:17873		0.179	0.246 KB/sec
?	root	192.168.0.92:11211-213.32.10.149:44945		0.000	0.000 KB/sec
?	root	192.168.0.92:20101-105.176.26.66:43408		0.000	0.000 KB/sec
?	root	unknown TCP		0.000	0.000 KB/sec
TOTAL				34.540	3.512 KB/sec

The parameters in the command output are as follows:

- **PID:** ID of the process.
 - **USER:** user who runs the process.
 - **PROGRAM:** IP addresses and port numbers of the process and connection, respectively. The former is for the server and the latter is for the client.
 - **DEV:** Network port to which the traffic is destined.
 - **SENT:** Volume of data sent by the process per second.
 - **RECEIVED:** Volume of data received by the process per second.
- c. Stop malicious programs or blacklist malicious IP addresses.
To stop a malicious process, run the **kill** *PID* command.
To blacklist a malicious IP address or limit its rate, use iptables.

13.13 Database Applications

13.13.1 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.

13.13.2 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.

A Change History

Released On	Description
2020-11-06	This issue is the first official release.