Elastic Cloud Server

User Guide

Date 2018-10-30
Contents

1 Service Overview .......................................................................................................................... 8
  1.1 ECS .............................................................................................................................................. 8
  1.2 Regions and AZs .......................................................................................................................... 9
  1.3 Storage ....................................................................................................................................... 10
  1.4 Network and Security ................................................................................................................ 10
  1.4.1 VPC ........................................................................................................................................ 10
  1.4.2 User Encryption .................................................................................................................... 11
  1.4.3 Cloud-Init .............................................................................................................................. 12
  1.4.4 License Type .......................................................................................................................... 14
  1.4.5 Project ..................................................................................................................................... 15
  1.5 IMS ............................................................................................................................................ 15
  1.6 ECS Instances ........................................................................................................................... 16
  1.6.1 Lifecycle ................................................................................................................................. 16
  1.7 Instance Family ........................................................................................................................ 18
  1.7.1 ECS Types ............................................................................................................................ 18
  1.7.2 General-Purpose ECSs .......................................................................................................... 19
  1.7.3 Dedicated General-Purpose ECSs ....................................................................................... 20
  1.7.4 Computing I and II ECSs ..................................................................................................... 21
  1.7.5 Memory-optimized ECSs ...................................................................................................... 22
  1.7.6 Large-Memory ECSs ............................................................................................................. 24
  1.8 Accessing and Using ECSs ......................................................................................................... 26
  1.8.1 Accessing ECSs ..................................................................................................................... 26
  1.8.2 ECSs and Other Services ....................................................................................................... 26
  1.8.3 User Permissions .................................................................................................................... 29

2 Getting Started .............................................................................................................................. 31
  2.1 Creating and Logging In to a Windows ECS ............................................................................ 31
  2.2 Creating and Logging In to a Linux ECS ................................................................................. 38
  2.3 Initializing EVS Data Disks ........................................................................................................ 44
  2.3.1 Scenarios and Disk Partitions ............................................................................................... 44
  2.3.2 Initializing a Windows Data Disk (Windows Server 2008) .................................................... 46
  2.3.3 Initializing a Windows Data Disk (Windows Server 2016) .................................................... 53
  2.3.4 Initializing a Linux Data Disk (fdisk) .................................................................................... 66
6 Configuration Modifications .................................................................................................................. 131
  6.1 Modifying ECS vCPU and Memory Specifications ........................................................................... 131
  6.1.1 General Operations for Modifying Specifications ......................................................................... 131
  6.1.2 Changing a XEN ECS to a KVM ECS (Windows) ........................................................................ 137
  6.1.3 Changing a XEN ECS to a KVM ECS (Linux) ............................................................................. 143
  6.2 Changing the Time Zone for an ECS ............................................................................................. 149
7 Disks ................................................................................................................................................. 153
  7.1 Attaching a Disk to an ECS ............................................................................................................. 153
  7.2 Detaching an EVS Disk from a Running ECS .................................................................................. 154
  7.3 Expanding the Capacity of an EVS Disk ......................................................................................... 156
8 NICs .................................................................................................................................................. 157
  8.1 Adding a NIC .................................................................................................................................. 157
  8.2 Deleting a NIC ............................................................................................................................... 158
  8.3 Managing Virtual IP Addresses .................................................................................................... 159
  8.4 Enabling NIC Multi-Queue ............................................................................................................. 159
9 Security Groups ............................................................................................................................... 163
  9.1 Security Group Configuration Examples ....................................................................................... 163
  9.1.1 Security Group Configuration Examples .................................................................................... 163
  9.1.2 Enabling ECSs in Different Security Groups to Communicate with Each Other Through an Internal Network ........................................................................................................ 164
  9.1.3 Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group ................. 165
  9.1.4 Remotely Connecting to Linux ECSs Using SSH ....................................................................... 165
  9.1.5 Remotely Connecting to Windows ECSs Using RDP ............................................................... 165
  9.1.6 Enabling Communication Between ECSs ................................................................................ 165
  9.1.7 Hosting a Website on ECSs ........................................................................................................ 166
  9.1.8 Enabling an ECS to Function as a DNS Server ......................................................................... 166
  9.1.9 Uploading or Downloading Files using FTP ............................................................................. 166
  9.2 Configuring Security Group Rules ................................................................................................ 167
  9.3 Changing a Security Group ............................................................................................................ 167
10 EIPs .................................................................................................................................................. 169
  10.1 Changing an EIP Bandwidth ......................................................................................................... 169
  10.2 Having an ECS Without a Public IP Address Access the Internet ............................................ 169
11 Monitoring ...................................................................................................................................... 172
  11.1 ECS Monitoring ......................................................................................................................... 172
  11.2 ECS Metrics ............................................................................................................................... 172
  11.3 Setting Alarm Rules .................................................................................................................... 175
  11.4 Viewing ECS Metrics ................................................................................................................ 176
12 Tags .................................................................................................................................................. 177
13 Operation Trace Management ......................................................................................................... 179
  13.1 Supported CTS Operations ........................................................................................................ 179
14 Troubleshooting ................................................................. 182
14.1 What Should I Do When an ECS Remains in the Restarting or Stopping State for a Long Time? .......... 182
14.2 What Should I Do If a NIC Fails to Work? ........................................ 182
14.3 What Can I Do If Switching from a Non-root User to User root Times Out? ................................. 184
14.4 What Should I Do If a Linux ECS with a SCSI Disk Attached Fails to Restart? ......................... 185
14.5 What Should I Do If a Key Pair Cannot Be Imported? ...................................................... 186
14.6 Why Was My Login to a Linux ECS with a Key File Unsuccessful? ........................................ 186
14.7 What Should I Do If Error "command ´gcc´ failed with exit status 1" Occurs During PIP-based Software Installation .. 187
14.8 What Should I Do If Packages Are Downloaded Using PIP or wget at a Low Rate? .................... 188
14.9 What Should I Do When a Disk Goes Offline? ......................................................................... 189
14.10 What Should I Do If a Key Pair Created Using puttygen.exe Cannot Be Imported to the Management Console? ......... 190
14.11 How Do I Handle Error Messages Displayed on the Management Console? ............................... 192
14.12 How Can I Handle Slow ECS Startup? ................................................................................. 194
14.13 What Should I Do If Cloud-Init Does Not Work After Python Is Upgraded? ............................ 195
15 FAQs .................................................................................. 197
15.1 General FAQs ................................................................... 197
15.1.1 What Restrictions Apply to ECSs? ................................................................................. 197
15.1.2 What Can I Do with ECSs? ......................................................................................... 197
15.1.3 How Long Does It Take to Obtain an ECS? ................................................................... 197
15.1.4 What Functions Does the Delete Button Provide? ......................................................... 197
15.1.5 What Is a Deleted ECS? ............................................................................................ 198
15.1.6 Can a Deleted ECS Be Provisioned Again? ..................................................................... 198
15.1.7 Why Does the Task Status Area Show an ECS Creation Failure But the ECS List Displays the Created ECS? .... 198
15.2 Management FAQs ............................................................. 198
15.2.1 Can I Transfer ECS Ownership Between Accounts? ....................................................... 198
15.2.2 What Is the cloudbase-init Account in Windows ECSs? .............................................. 198
15.2.3 How Can a Changed Static Hostname Take Effect Permanently? .................................... 199
15.2.4 Is the ECS Hostname with Suffix novalocal Normal? .................................................. 200
15.2.5 Why Does the System Display a Question Mark When I Attempt to Obtain Console Logs? .......... 201
15.3 VNC FAQs................................................................. 201
15.3.1 Why Cannot I Use the Spanish Keyboard to Enter Characters After I Log In to an ECS Using VNC? ....... 201
15.3.2 Why Cannot I Use the Portuguese Keyboard to Enter Characters After I Log In to an ECS Using VNC? ...... 202
15.3.3 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? ........................... 202
15.3.4 What Should I Do If I Cannot View Data After Logging In to an ECS Using VNC? ............... 202
15.3.5 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? ................. 203
15.4 Login FAQs .................................................................... 203
15.4.1 What Browser Version Is Required to Remotely Log In to an ECS? ................................. 203
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4.2 What Should I Do If I Cannot Log In to an ECS with Cloud-Init Enabled?</td>
<td>203</td>
</tr>
<tr>
<td>15.4.3 What Should I Do If an Authentication Failure Occurs After I Attempt to Remotely Log In to a Windows ECS?</td>
<td>204</td>
</tr>
<tr>
<td>15.4.4 What Should I Do If the System Displays Error Code 0x112f When I Log In to a Windows ECS?</td>
<td>205</td>
</tr>
<tr>
<td>15.4.5 How Can I Log In to an ECS After Its System Disk Is Exchanged with That Attached to Another ECS Running the Same OS?</td>
<td>206</td>
</tr>
<tr>
<td>15.4.6 Why Does the System Display a Message Indicating that the Password for Logging In to a Windows ECS Cannot Be Viewed?</td>
<td>207</td>
</tr>
<tr>
<td>15.5 Key Pair</td>
<td>208</td>
</tr>
<tr>
<td>15.5.1 How Can I Obtain the Key Pair Used by an ECS?</td>
<td>208</td>
</tr>
<tr>
<td>15.6 EIP FAQs</td>
<td>209</td>
</tr>
<tr>
<td>15.6.1 Can Multiple EIPs Be Bound to an ECS?</td>
<td>209</td>
</tr>
<tr>
<td>15.6.2 Will NICs Added to an ECS Start Automatically?</td>
<td>210</td>
</tr>
<tr>
<td>15.6.3 Can an ECS Without an EIP Access the Internet?</td>
<td>210</td>
</tr>
<tr>
<td>15.6.4 Why Can I Remotely Access an ECS But Cannot Ping It?</td>
<td>210</td>
</tr>
<tr>
<td>15.7 Network</td>
<td>210</td>
</tr>
<tr>
<td>15.7.1 Can the ECSs of Different Accounts Communicate over the Intranet?</td>
<td>210</td>
</tr>
<tr>
<td>15.7.2 How Can I Check Whether Remaining Resources Are Sufficient for Automatic Recovery?</td>
<td>211</td>
</tr>
<tr>
<td>15.7.3 How Can I Receive an Automatic ECS Recovery Event?</td>
<td>211</td>
</tr>
<tr>
<td>15.7.4 How Can I View and Modify Kernel Parameters of a Linux ECS?</td>
<td>211</td>
</tr>
<tr>
<td>15.7.5 How Can I Test Network Performance?</td>
<td>216</td>
</tr>
<tr>
<td>15.8 Disk FAQs</td>
<td>223</td>
</tr>
<tr>
<td>15.8.1 Can Multiple Disks Be Attached to an ECS?</td>
<td>223</td>
</tr>
<tr>
<td>15.8.2 Which ECSs Can Be Attached with SCSI EVS Disks?</td>
<td>223</td>
</tr>
<tr>
<td>15.8.3 What Are the Restrictions for Attaching an EVS Disk to an ECS?</td>
<td>224</td>
</tr>
<tr>
<td>15.8.4 How Can I Adjust System Disk Partitions?</td>
<td>224</td>
</tr>
<tr>
<td>15.8.5 How Can I Add the Empty Partition of an Expanded System Disk to the End Root Partition Online?</td>
<td>229</td>
</tr>
<tr>
<td>15.8.6 How Can I Add the Empty Partition of an Expanded System Disk to the Non-end Root Partition Online?</td>
<td>231</td>
</tr>
<tr>
<td>15.8.7 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Windows ECS?</td>
<td>234</td>
</tr>
<tr>
<td>15.8.8 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Linux ECS?</td>
<td>236</td>
</tr>
<tr>
<td>15.8.9 Who Can Use the Encryption Feature?</td>
<td>238</td>
</tr>
<tr>
<td>15.9 OS FAQs</td>
<td>240</td>
</tr>
<tr>
<td>15.9.1 Can I Install or Upgrade the OS by Myself?</td>
<td>240</td>
</tr>
<tr>
<td>15.9.2 Can the OS of an ECS Be Changed?</td>
<td>240</td>
</tr>
<tr>
<td>15.9.3 Is a GUI Provided for OSs?</td>
<td>240</td>
</tr>
<tr>
<td>15.9.4 Is the FTP Upload Tool Included in the OS?</td>
<td>240</td>
</tr>
<tr>
<td>15.9.5 Can I Select Other OSs During ECS OS Reinstallation?</td>
<td>240</td>
</tr>
<tr>
<td>15.9.6 How Can I Obtain Data Disk Information If Tools Are Deleted?</td>
<td>240</td>
</tr>
<tr>
<td>15.9.7 How Can I Set the Validity Period of the Image Password?</td>
<td>241</td>
</tr>
<tr>
<td>15.9.8 Why Is the Memory of an ECS Obtained by Running the free Command Inconsistent with the Actual Memory?</td>
<td>242</td>
</tr>
<tr>
<td>15.9.9 How to configure the SUSE repository?</td>
<td>243</td>
</tr>
<tr>
<td>15.9.10 How Can I Enable Virtual Memory on a Windows ECS?</td>
<td>248</td>
</tr>
</tbody>
</table>
15.9.11 How Can I Handle Strange Routes and IP Addresses on an ECS? .................................................. 249
15.9.12 How Can I Change the Patch Update Source of an ECS Running a Windows Server OS to an Official Microsoft Patch Server? ................................................................. 251
15.10 Database FAQs .................................................................................................................................. 255
15.10.1 Can a Database Be Deployed on an ECS? ................................................................................ 255
15.10.2 Does an ECS Support Oracle Databases? ............................................................................ 255

A Change History ....................................................................................................................................... 256
1 Service Overview

1.1 ECS

An Elastic Cloud Server (ECS) is a computing server consisting of vCPUs, memory, image, and Elastic Volume Service (EVS) disks that allow on-demand allocation and elastic scaling. ECSs integrate Virtual Private Cloud (VPC), virtual firewalls, and multi-data-copy capabilities to create an efficient, reliable, and secure computing environment. This ensures the stable and uninterrupted operation of services. After creating an ECS, you can use it like using your local computer or physical server.

ECSs support self-service creation, modification, and operation. You can create ECSs by specifying the vCPU, memory, image specifications, and login authentication. After creating an ECS, you can modify its specifications as required.

System Architecture

ECS works with other products and services to provide computing, storage, network, and image installation 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 the subnet and security group, 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 and deploy services quickly.
- The Elastic Volume Service (EVS) provides storage and Volume Backup Service (VBS) provides data backup and recovery functions.
1.2 Regions and AZs

A region is a geographic area where resources used by your ECSs are located.

ECSs in the same region can communicate with each other over an intranet, but ECSs in different regions cannot.

Public cloud data centers are deployed worldwide in places, such as Europe, and Asia. Creating ECSs in different regions can better suit certain user requirements. For example, applications can be designed to meet user requirements in specific regions or comply with local laws or regulations. ECS pricing also changes based on region.

Each region contains many AZs where power and networks are physically isolated. AZs in the same region can communicate with each other over an intranet. Each AZ provides cost-effective and low-latency network connections that are unaffected by faults that may occur in other AZs.
1.3 Storage

**EVS Disk Types**

ECSs support the following types of EVS disks for storing data:

- **Common I/O**: EVS disks of this type deliver a maximum of 1,000 IOPS. This disk type is suitable for application scenarios that require large capacity, a medium read/write rate, and fewer transactions, such as enterprise office applications and small-scale testing.

- **Ultra-high I/O**: EVS disks of this type deliver a maximum of 20,000 IOPS and a minimum of 1 ms read/write latency. This disk type is excellent for ultra-high I/O, ultra-high bandwidth, and read/write-intensive application scenarios, such as distributed file systems in HPC scenarios or NoSQL/RDS in I/O-intensive scenarios.

- **Ultra-high I/O (latency-optimized)**: EVS disks of this type deliver a maximum of 1 GB/s throughput and a minimum of 1 ms read/write latency. They can be used for key enterprise services, such as SAP HANA.

EVS disks with different I/O capacities provide different features at different prices. Choose EVS disks based on your requirements. For more information about EVS disk specifications and performance, see *Elastic Volume Service User Guide*.

**EVS Disk 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, such as installing a driver for a SCSI EVS disk, see FAQs > Do I Need to Install a Driver for EVS Disks with Device Type SCSI? in *Elastic Volume Service User Guide*.

**Related Links**

- 15.8.2 Which ECSs Can Be Attached with SCSI EVS Disks?

1.4 Network and Security

1.4.1 VPC

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 strengthen ECS security protection. For more information, see *Virtual Private Cloud User Guide*.

### 1.4.2 User Encryption

User encryption allows you to use the encryption feature provided on the public cloud platform to encrypt ECS resources, improving data security. User encryption includes image encryption and EVS disk encryption.

#### Image Encryption

Key encryption supports encrypting private images. When creating an ECS, if you select an encrypted image, the system disk of the created ECS automatically has encryption enabled, implementing system disk encryption and improving data security.

Use either of the following methods to create an encrypted image:

- Create an encrypted image using an existing encrypted ECS.
- Create an encrypted image using an external image file.

For more information about image encryption, see *Image Management Service User Guide*.

#### EVS Disk Encryption

EVS disk encryption supports system disk encryption and data disk encryption.

- When creating an ECS, you can encrypt added data disks.
- System disk encryption relies on the image. When creating an ECS, if you select an encrypted image, the system disk of the created ECS automatically has encryption enabled, and the encryption mode complies with the image encryption mode.

For more information about EVS disk encryption, see *Elastic Volume Service User Guide*.

#### Impact on AS

If you use an encrypted ECS to create an Auto Scaling (AS) configuration, the encryption mode of the created AS configuration complies with the ECS encryption mode.

#### About Keys

The key used for encryption relies on the Key Management Service (KMS). KMS uses a data encryption key (DEK) to encrypt data and a customer master key (CMK) to encrypt the DEK.
Figure 1-2 Data encryption process

Table 1-1 describes the keys involved in the data encryption process.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEK</td>
<td>An encryption key that is used for encrypting data.</td>
<td>Encrypts specific data.</td>
</tr>
<tr>
<td>CMK</td>
<td>An encrypted key that is created using KMS. A CMK encrypts and protects DEKs.</td>
<td>Supports CMK disabling and scheduled deletion.</td>
</tr>
</tbody>
</table>
| Default CMK | A type of CMK with suffix /default. The default CMK is automatically generated by the system when you use KMS for encryption for the first time. For example, evs/default | • Supports viewing details of the default CMK on the KMS console.  
  • Does not support CMK disabling or scheduled deletion. |

NOTE
After disabling a CMK or scheduling the deletion of a CMK takes effect, the EVS disk encrypted using this CMK can still be used until the disk is detached from and then attached to an ECS again. During this process, the disk fails to be attached to the ECS because the CMK cannot be obtained. Therefore, the EVS disk becomes unavailable.

For details about KMS, see Key Management Service User Guide.

1.4.3 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 private images support customized configurations, you must install Cloud-Init or Cloudbase-Init before creating private images.

- 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 how to install Cloud-Init or Cloudbase-Init, 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. For details, see section 3.4.2 Injecting User Data into ECSs.
- After Cloud-Init is supported, ECSs do not support password authentication any more. All newly created ECSs use key pair authentication. This change will influence your ECS logins. For details, see the following sections:
  - 4.2.1 Login Overview
  - 15.2.2 What Is the cloudbase-init Account in Windows ECSs?
  - 14.6 Why Was My Login to a Linux ECS with a Key File Unsuccessful?
  - 15.4.6 Why Does the System Display a Message Indicating that the Password for Logging In to a Windows ECS Cannot Be Viewed?
- After Cloud-Init is supported, you can view and use metadata to configure and manage running ECSs. For more information, see section 3.4.1 Managing ECS Metadata.

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 section "How Does Cloud-Init Influence the AS Service?" in Auto Scaling User Guide.

For more information about AS, see 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:
1.4.4 License Type

Use License from the System

You can use the license provided by the public cloud platform. After creating an ECS with a license authorized, you can use the authorized OS and pay on demand.

BYOL

What Is BYOL?

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

How to Use BYOL?

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

The OSs supporting BYOL are as follows:

- SUSE Linux Enterprise Server
- Oracle Enterprise Linux
- Red Hat Enterprise Linux
- Windows Server OS (BYOL can be used on an ECS that is created on a DeH and runs a Windows Server OS.)

Statement

When creating an ECS on a DeH, if you use a commercial image registered using an external image file, you are required to select BYOL to use your existing OS license.

- For Microsoft Windows Server: Bring your own licenses to the Dedicated Hosts: Open Cloud offers Dedicated Hosts, which allows you to access physical servers that are fully dedicated for your use. You can use your own licensed software on dedicated infrastructure, even without Software Assurance.
- For Microsoft SQL Server: Bring your own licenses with License Mobility: Open Cloud allows you to bring your own licenses with License Mobility to Open Cloud based on Microsoft License Mobility agreement authorized by Microsoft. According to the terms of Microsoft License Mobility, you should purchase the Software Assurance with your Microsoft SQL Server license.

For more details about the official Microsoft software License Mobility, refer to:


https://www.redhat.com/en/technologies/cloud-computing/cloud-access


You are responsible for complying with Microsoft licensing requirements. This document is only a guide for your convenience and does not constitute legal advice. You are not entitled to rely on descriptions in this document. If you have any questions about your licenses or rights to Microsoft software, please consult your legal team, Microsoft, or your Microsoft reseller.

Application Scenarios

The system does not support dynamic license type changing. ECSs support BYOL in the following scenarios:

- Creating an ECS
  After creating an ECS, you cannot change its license type. If the license type must be changed, reinstall or change the ECS OS.

- Reinstalling an ECS OS
  When reinstalling an ECS OS, you can set the license type for the ECS.

- Changing an ECS OS
  When changing an ECS OS, you can set the license type for the ECS.

- Attaching a system disk
  The license type of a system disk is determined by the ECS license type after the ECS is created, the ECS OS is reinstalled, or the ECS OS is changed. If the system disk is detached and then attached to a new ECS or the original ECS, ensure that the ECS license type is the same as the system disk license type.

1.4.5 Project

A project groups and isolates OpenStack computing, storage, and network resources. A project can be a department or a team.

Multiple projects can be created for one account.

1.5 IMS

Introduction

IMS allows you to create ECSs using images. An image is an ECS template that contains an OS and may also contain proprietary software and application software, such as database software.

Images can be public, private, or shared. Public images are provided by the system by default, private images are manually created, and shared images are private images that are shared by another user. 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 a web server, static configurations, and dynamic page code. When you use this image to create an ECS, your web server and applications will be available for use immediately.
Image Types

### Table 1-2 Image types

<table>
<thead>
<tr>
<th>Image Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public image</td>
<td>A standard, widely used image. It contains an OS, comes with preinstalled public applications, and is available to all users.</td>
</tr>
</tbody>
</table>
| Private image| An image available only to the user who created it. It contains an OS, preinstalled public applications, and the user's private applications. Using a private image to create ECSs removes the need to configure multiple ECSs repeatedly. A private image can be created using:  
  - An ECS  
  - An external image file  
  You can upload external image files and register the images on the public cloud platform to make them function as private images. External image files can be in VMDK, VHD, QCOW2, or ZVHD format. |
| Shared image| A private image shared by another user.                                                                               |

### Conversion Between Images and ECSs

You can use images to create ECSs and you can convert ECS configurations into images.

### 1.6 ECS Instances

#### 1.6.1 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 1-3 ECS statuses

<table>
<thead>
<tr>
<th>Status</th>
<th>Status Attribute</th>
<th>Description</th>
<th>API Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating</td>
<td>Intermediate</td>
<td>The ECS has been created but is not running.</td>
<td>BUILD or BUILDING</td>
</tr>
<tr>
<td>Starting</td>
<td>Intermediate</td>
<td>The ECS is between the <strong>Stopped</strong> and <strong>Running</strong> states.</td>
<td>SHUTOFF</td>
</tr>
<tr>
<td>Running</td>
<td>Stable</td>
<td>The ECS is running properly. An ECS in this state can provide services.</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>Stopping</td>
<td>Intermediate</td>
<td>The ECS is between the <strong>Running</strong></td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>
### Status Overview

<table>
<thead>
<tr>
<th>Status</th>
<th>Status Attribute</th>
<th>Description</th>
<th>API Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped</td>
<td>Stable</td>
<td>The ECS has been properly stopped. An ECS in this state cannot provide services.</td>
<td>SHUTOFF</td>
</tr>
<tr>
<td>Restarting</td>
<td>Intermediate</td>
<td>The ECS is being restarted.</td>
<td>REBOOT</td>
</tr>
<tr>
<td>Resizing</td>
<td>Intermediate</td>
<td>The ECS has received a resizing request and has started to resize.</td>
<td>RESIZE</td>
</tr>
<tr>
<td>Verifying</td>
<td>Intermediate</td>
<td>The ECS is verifying the modified configuration.</td>
<td>VERIFY_RESIZE</td>
</tr>
<tr>
<td>Deleting</td>
<td>Intermediate</td>
<td>The ECS is being deleted. If the ECS remains in this state for a long time, exceptions may have occurred. In such an event, contact the administrator.</td>
<td>ACTIVE, SHUTOFF, REBOOT, RESIZE, VERIFY_RESIZE, HARD_REBOOT, REVERT_RESIZE, or ERROR</td>
</tr>
<tr>
<td>Deleted</td>
<td>Intermediate</td>
<td>The ECS has been deleted. An ECS in this state cannot provide services and will be promptly cleared from the system.</td>
<td>DELETED</td>
</tr>
<tr>
<td>Faulty</td>
<td>Stable</td>
<td>An exception has occurred on the ECS. An ECS in this state cannot provide services. Contact the administrator.</td>
<td>ERROR</td>
</tr>
<tr>
<td>Reinstalling OS</td>
<td>Intermediate</td>
<td>The ECS has received a request to reinstall the OS and has begun the reinstalliation.</td>
<td>SHUTOFF</td>
</tr>
<tr>
<td>Reinstalling OS failed</td>
<td>Stable</td>
<td>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.</td>
<td>SHUTOFF</td>
</tr>
<tr>
<td>Changing OS</td>
<td>Intermediate</td>
<td>The ECS received a request to change the OS and has begun implementing the changes.</td>
<td>SHUTOFF</td>
</tr>
<tr>
<td>OS Change failed</td>
<td>Stable</td>
<td>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.</td>
<td>SHUTOFF</td>
</tr>
<tr>
<td>Forcibly restarting</td>
<td>Intermediate</td>
<td>The ECS is being forcibly restarted.</td>
<td>HARD_REBOOT</td>
</tr>
</tbody>
</table>
### 1.7 Instance Family

#### 1.7.1 ECS Types

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

- General-purpose
- Dedicated general-purpose
- Computing I
- Computing II
- Memory-optimized
- Large-memory

#### ECS FlavorNaming Rules

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

The format is defined as follows:

- **A** specifies the ECS type. For example, s indicates a general-purpose ECS, c a computing ECS, and m a memory-optimized ECS.
- **B** specifies the type ID. For example, the 2 in c2 indicates a computing II ECS.
- **C** can be any of the following options:
  - medium
  - large
  - xlarge
  - 2xlarge
  - 4xlarge
  - 8xlarge

#### Network Bandwidth

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

- 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.
**NOTE**
- For instructions about how to test PPS, see section 15.7.5 How Can I Test Network Performance?
- For instructions about how to enable NIC multi-queue, see section 8.4 Enabling NIC Multi-Queue.

### 1.7.2 General-Purpose ECSs

**Overview**

General-purpose ECSs provide basic vCPU performance and a balance of computing, memory, and network resources. These ECSs are suitable for many applications, such as web servers, enterprise R&D, and small-scale databases.

Compared with S1 ECSs, S3 ECSs are developed based on KVM virtualization and use latest-generation Intel Xeon Skylake CPUs, which significantly improve the comprehensive performance. They provide basic vCPU performance and a balance of computing, memory, and network resources. These ECSs are suitable for many applications.

**Specifications**

**Table 1-4 S1 ECS specifications**

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximum/Assured Bandwidth</th>
<th>Maximum PPS</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1.medium</td>
<td>1</td>
<td>4</td>
<td>Low</td>
<td>Low</td>
<td>XEN</td>
</tr>
<tr>
<td>s1.large</td>
<td>2</td>
<td>8</td>
<td>Low</td>
<td>Low</td>
<td>XEN</td>
</tr>
<tr>
<td>s1.xlarge</td>
<td>4</td>
<td>16</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
<tr>
<td>s1.2xlarge</td>
<td>8</td>
<td>32</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
<tr>
<td>s1.4xlarge</td>
<td>16</td>
<td>64</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
<tr>
<td>s1.8xlarge</td>
<td>32</td>
<td>128</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
</tbody>
</table>

**Table 1-5 S3 ECS specifications**

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximum/Assured Bandwidth (Gbit/s)</th>
<th>Maximum PPS (10,000)</th>
<th>NIC Multi-Queue</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>s3.medium, 2</td>
<td>1</td>
<td>2</td>
<td>0.5/0.1</td>
<td>5</td>
<td>1</td>
<td>KVM</td>
</tr>
<tr>
<td>s3.large, 2</td>
<td>2</td>
<td>4</td>
<td>0.8/0.2</td>
<td>10</td>
<td>1</td>
<td>KVM</td>
</tr>
<tr>
<td>s3.xlarge, 2</td>
<td>4</td>
<td>8</td>
<td>1.5/0.4</td>
<td>15</td>
<td>1</td>
<td>KVM</td>
</tr>
</tbody>
</table>
### Flavors and Specifications

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximal/Assured Bandwidth (Gbit/s)</th>
<th>Maximum PPS (10,000)</th>
<th>NIC Multi-Queue</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>s3.2xlarge.2</td>
<td>8</td>
<td>16</td>
<td>3/0.8</td>
<td>20</td>
<td>2</td>
<td>KVM</td>
</tr>
<tr>
<td>s3.4xlarge.2</td>
<td>16</td>
<td>32</td>
<td>4/1.5</td>
<td>30</td>
<td>4</td>
<td>KVM</td>
</tr>
<tr>
<td>s3.medium.4</td>
<td>1</td>
<td>4</td>
<td>0.5/0.1</td>
<td>5</td>
<td>1</td>
<td>KVM</td>
</tr>
<tr>
<td>s3.large.4</td>
<td>2</td>
<td>8</td>
<td>0.8/0.2</td>
<td>10</td>
<td>1</td>
<td>KVM</td>
</tr>
<tr>
<td>s3.xlarge.4</td>
<td>4</td>
<td>16</td>
<td>1.5/0.4</td>
<td>15</td>
<td>1</td>
<td>KVM</td>
</tr>
<tr>
<td>s3.2xlarge.4</td>
<td>8</td>
<td>32</td>
<td>3/0.8</td>
<td>20</td>
<td>2</td>
<td>KVM</td>
</tr>
<tr>
<td>s3.4xlarge.4</td>
<td>16</td>
<td>64</td>
<td>4/1.5</td>
<td>30</td>
<td>4</td>
<td>KVM</td>
</tr>
</tbody>
</table>

### Scenarios

- **Applications**
  General-purpose ECSs are suitable for applications that have no special requirements on CPU performance, memory, disk capacity, or bandwidth, but have high requirements on security and reliability. They feature low initial investment and maintenance costs.

- **Application scenarios**
  Enterprise website deployment, enterprise office environment setup, enterprise R&D and testing activities, Web servers, R&D and testing environments for developers, and small-scale databases

### 1.7.3 Dedicated General-Purpose ECSs

#### Overview

C3 ECSs are newly released. They are developed based on KVM virtualization, use latest-generation Intel Xeon Skylake CPUs and Data Plane Development Kit (DPDK) rapid packet processing mechanism, and feature high and stable computing performance. Working in high-performance networks, the C3 ECSs provide higher performance and stability, meeting enterprise-class application requirements.

#### Specifications

**Table 1-6 C3 ECS specifications**

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximal/Assured Bandwidth (Gbit/s)</th>
<th>Maximum PPS (10,000)</th>
<th>NIC Multi-Queue</th>
<th>Virtualization Type</th>
</tr>
</thead>
</table>
### Flavors

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximum/Assured Bandwidth (Gbit/s)</th>
<th>Maximum PPS (10,000)</th>
<th>NIC Multi-Queue</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3.large.4</td>
<td>2</td>
<td>8</td>
<td>1.5/0.6</td>
<td>30</td>
<td>2</td>
<td>KVM</td>
</tr>
<tr>
<td>c3.xlarge.4</td>
<td>4</td>
<td>16</td>
<td>3/1</td>
<td>50</td>
<td>2</td>
<td>KVM</td>
</tr>
<tr>
<td>c3.2xlarge.4</td>
<td>8</td>
<td>32</td>
<td>5/2</td>
<td>90</td>
<td>4</td>
<td>KVM</td>
</tr>
<tr>
<td>c3.4xlarge.4</td>
<td>16</td>
<td>64</td>
<td>10/4</td>
<td>130</td>
<td>4</td>
<td>KVM</td>
</tr>
<tr>
<td>c3.8xlarge.4</td>
<td>32</td>
<td>128</td>
<td>15/8</td>
<td>260</td>
<td>8</td>
<td>KVM</td>
</tr>
<tr>
<td>c3.16xlarge.4</td>
<td>60</td>
<td>256</td>
<td>17/16</td>
<td>500</td>
<td>16</td>
<td>KVM</td>
</tr>
</tbody>
</table>

### Scenarios

- **Applications**
  
  Dedicated general-purpose ECSs are suitable for applications that have no special requirements on CPU performance, memory, disk capacity, or bandwidth, but have high requirements on security and reliability. They feature low initial investment and maintenance costs.

- **Application scenarios**
  
  Enterprise website deployment, enterprise office environment setup, enterprise R&D and testing activities, Web servers, R&D and testing environments for developers, and small-scale databases

### 1.7.4 Computing I and II ECSs

#### Overview

Computing I and II ECSs provide a large number of vCPUs. These ECSs are suitable for scenarios that require scaling out CPU resources, such as distributed analysis and engineering applications.

#### Specifications

**Table 1-7** Computing I C1 and computing II C2 ECS specifications

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximum/Assured Bandwidth</th>
<th>Maximum PPS</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1.medium</td>
<td>1</td>
<td>1</td>
<td>Low</td>
<td>Low</td>
<td>XEN</td>
</tr>
</tbody>
</table>
### 1.7.5 Memory-optimized ECSs

**Overview**

- M1 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.

- M3 ECSs are developed based on the KVM virtualization platform and designed for processing large-scale data sets in the memory. They use latest-generation Intel Xeon Skylake CPUs, network acceleration engines, and DPDK rapid packet processing mechanism to provide higher network performance, providing a maximum memory size of 512 GB based on DDR4 for high-memory computing applications.

**Specifications**

#### Table 1-8 M1 ECS specifications

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximum/Assured Bandwidth</th>
<th>Maximum PPS</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>m1.medium</td>
<td>1</td>
<td>8</td>
<td>Low</td>
<td>Low</td>
<td>XEN</td>
</tr>
<tr>
<td>m1.large</td>
<td>2</td>
<td>16</td>
<td>Low</td>
<td>Low</td>
<td>XEN</td>
</tr>
<tr>
<td>m1.xlarge</td>
<td>4</td>
<td>32</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
</tbody>
</table>
### Service Overview

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximum/ Assured Bandwidth</th>
<th>Maximum PPS</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>m1.2xlarge</td>
<td>8</td>
<td>64</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
<tr>
<td>m1.4xlarge</td>
<td>16</td>
<td>128</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximum/ Assured Bandwidth (Gbit/s)</th>
<th>Maximum PPS (10,000)</th>
<th>NIC Multi-Queue</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>m3.large.8</td>
<td>2</td>
<td>16</td>
<td>1.5/0.6</td>
<td>30</td>
<td>2</td>
<td>KVM</td>
</tr>
<tr>
<td>m3.xlarge.8</td>
<td>4</td>
<td>32</td>
<td>3/1.1</td>
<td>50</td>
<td>2</td>
<td>KVM</td>
</tr>
<tr>
<td>m3.2xlarge.8</td>
<td>8</td>
<td>64</td>
<td>5/2</td>
<td>90</td>
<td>4</td>
<td>KVM</td>
</tr>
<tr>
<td>m3.4xlarge.8</td>
<td>16</td>
<td>128</td>
<td>10/4.5</td>
<td>130</td>
<td>4</td>
<td>KVM</td>
</tr>
<tr>
<td>m3.8xlarge.8</td>
<td>32</td>
<td>256</td>
<td>15/9</td>
<td>260</td>
<td>8</td>
<td>KVM</td>
</tr>
<tr>
<td>m3.16xlarge.8</td>
<td>60</td>
<td>512</td>
<td>17/17</td>
<td>500</td>
<td>16</td>
<td>KVM</td>
</tr>
</tbody>
</table>

**Table 1-9 M3 ECS specifications**

**Scenarios**

- High-performance relational (MySQL) and NoSQL (MongoDB and Cassandra) databases
- Distributed web scale cache stores that provide in-memory caching of key-value type data (Memcached and Redis)
- Applications processing big unstructured data in real time (financial services, Hadoop/Spark clusters)
- High-performance computing (HPC) and electronic design automation (EDA)

**Notes on Using M3 ECSs**

- M3 ECSs support all rollout OSs.
- M3 ECSs do not have InfiniBand or SSD NICs configured.
- M3 ECSs support modifying specifications if the source and target ECSs are of the same type.
1.7.6 Large-Memory ECSs

Overview

Large-memory ECSs provide an even larger amount of memory than memory-optimized ECSs. They are used for applications that require a large amount of memory, rapid data switching, low latency, and process large volumes of data. Large-memory ECSs provide large memory and high computing, storage, and network performance.

- Applications
  Large-memory ECSs are suitable for applications that require a large amount of memory, rapid data switching, and low latency, and process large volumes of data.

- Application scenarios
  E1 ECSs: OLAP applications, such as in-memory databases (SAP HANA BWoH, SAP HANA applications, including Business Suite S/4HANA, Business Suite on HANA, and Business Warehouse on HANA), big data processing engines (Apache Spark), and data mining
  E2 ECSs: OLTP applications, such as in-memory databases (SAP HANA SoH, SAP HANA applications, including Business Suite S/4HANA, Business Suite on HANA, and Business Warehouse on HANA), big data processing engines (Apache Spark), high-performance databases, and distributed memory cache
  E3 ECSs: OLAP and OLTP applications with hyper-threading enabled

Specifications

Table 1-10 E1 ECS specifications

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximum/ Assured Bandwidth</th>
<th>Maximum PPS</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>e1.4xlarge</td>
<td>16</td>
<td>470</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
<tr>
<td>e1.8xlarge</td>
<td>32</td>
<td>940</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
</tbody>
</table>

Table 1-11 E2 ECS specifications

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Maximum/ Assured Bandwidth</th>
<th>Maximum PPS</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>e2.3xlarge</td>
<td>12</td>
<td>256</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
<tr>
<td>e2.4xlarge</td>
<td>18</td>
<td>445</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
<tr>
<td>e2.9xlarge</td>
<td>36</td>
<td>890</td>
<td>Medium</td>
<td>Medium</td>
<td>XEN</td>
</tr>
</tbody>
</table>
## Table 1-12 E3 ECS specifications

<table>
<thead>
<tr>
<th>Flavor</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Virtualization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>e3.7xlarge.12</td>
<td>28</td>
<td>348</td>
<td>KVM</td>
</tr>
<tr>
<td>e3.14xlarge.12</td>
<td>56</td>
<td>696</td>
<td>KVM</td>
</tr>
</tbody>
</table>

### Features

Large-memory ECSs use SR-IOV+OVS networks to provide a bandwidth as high as 10 Gbit/s.

### Notes

- Large-memory ECSs do not support NIC hot swapping.
- Large-memory ECSs support only the following OSs:
  - CentOS 6.6 64bit
  - CentOS 6.7 64bit
  - CentOS 6.8 64bit
  - CentOS 7.1 64bit
  - CentOS 7.2 64bit
  - CentOS 7.3 64bit
  - SUSE Enterprise Linux Server 11 SP3 64bit
  - SUSE Enterprise Linux Server 11 SP4 64bit
  - SUSE Enterprise Linux Server 12 SP1 64bit
  - SUSE Enterprise Linux Server 12 SP2 64bit
  - Red Hat Enterprise Linux 6.8 64bit
  - Red Hat Enterprise Linux 7.3 64bit
- E3 ECSs support the following OS that has been verified:
  - SUSE Enterprise Linux Server 12 SP2 64bit
- E1 and E2 ECSs can use the following types of EVS disks as system disk and data disk:
  - High I/O (performance-optimized I)
  - Ultra-high I/O (latency-optimized)
- E3 ECSs can use ultra-high I/O EVS disks as the system disk and data disks.
- The primary and extension NICs of a large-memory ECS have specified application scenarios. For details, see Table 1-13.

### Table 1-13 Application scenarios of the NICs of a large-memory ECS

<table>
<thead>
<tr>
<th>NIC Type</th>
<th>Application Scenario</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary NIC</td>
<td>Applies to vertical layer 3 communication.</td>
<td>N/A</td>
</tr>
<tr>
<td>Extension NIC</td>
<td>Applies to horizontal layer 2</td>
<td>To improve network performance, you can set the MTU of the extension NIC to</td>
</tr>
</tbody>
</table>
1.8 Accessing and Using ECSs

1.8.1 Accessing ECSs

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. These two access modes differ as follows:

- **Accessing ECSs through APIs**
  Use this mode 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 mode if you are not required to integrate ECSs with a third-party system. After registering on the public cloud, log in to the management console and click *Elastic Cloud Server* under *Computing* on the homepage.

1.8.2 ECSs and Other Services

*Figure 1-3* shows the relationships between ECS and other services.
Figure 1-3 Relationships between ECS and other services

- **Auto Scaling (AS)**
  Automatically adjusts ECS service 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 strengthen ECS security protection.

- **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. Table 1-14 lists the ECS metrics supported by Cloud Eye.
### Table 1-14 ECS metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Formula</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Usage</td>
<td>Indicates the vCPU usage (%) of an ECS.</td>
<td>vCPU usage of an ECS/Number of vCPUs in the ECS</td>
<td>N/A</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>Indicates the memory usage (%) of an ECS.</td>
<td>Used memory of an ECS/Total memory of the ECS</td>
<td>This metric is unavailable if the image has no vmtools installed.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>Indicates the disk usage (%) of an ECS.</td>
<td>Used capacity of an ECS disk/Total capacity of the ECS disk</td>
<td>This metric is unavailable if the image has no vmtools installed.</td>
</tr>
<tr>
<td>Disks Read Rate</td>
<td>Indicates the number of bytes read from an ECS per second.</td>
<td>Total number of bytes read from an ECS disk/Monitoring period</td>
<td>byte_out = (rd_bytes - last_rd_bytes) / Time difference</td>
</tr>
<tr>
<td>Disks Write Rate</td>
<td>Indicates the number of bytes written to an ECS per second.</td>
<td>Total number of bytes written to an ECS disk/Monitoring period</td>
<td>N/A</td>
</tr>
<tr>
<td>Disks Read Requests</td>
<td>Indicates the number of read requests sent to an ECS per second.</td>
<td>Total number of read requests sent to an ECS disk/Monitoring period</td>
<td>req_out = (rd_req - last_rd_req)/Time difference</td>
</tr>
<tr>
<td>Disks Write Requests</td>
<td>Indicates the number of write requests sent to an ECS per second.</td>
<td>Total number of write requests sent to an ECS disk/Monitoring period</td>
<td>req_in = (wr_req - last_wr_req)/Time difference</td>
</tr>
<tr>
<td>Inband Incoming Rate</td>
<td>Indicates the number of incoming bytes on an ECS per second.</td>
<td>Total number of inband incoming bytes on an ECS/Monitoring period</td>
<td>N/A</td>
</tr>
<tr>
<td>Inband Outgoing Rate</td>
<td>Indicates the number of outgoing bytes on an ECS per second.</td>
<td>Total number of inband outgoing bytes on an ECS/Monitoring period</td>
<td>N/A</td>
</tr>
<tr>
<td>Outband Incoming Rate</td>
<td>Indicates the number of incoming bytes on an ECS per second on the hypervisor.</td>
<td>Total number of outband incoming bytes on an ECS/Monitoring period</td>
<td>This metric is unavailable if SR-IOV is enabled.</td>
</tr>
</tbody>
</table>
### 1 Service Overview

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Formula</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outband Outgoing Rate</td>
<td>Indicates the number of outgoing bytes on an ECS per second on the hypervisor.</td>
<td>Total number of outband outgoing bytes on an ECS/Monitoring period</td>
<td>This metric is unavailable if SR-IOV is enabled.</td>
</tr>
<tr>
<td>System Status Check</td>
<td>Check the status of the cloud platform for running ECSs. The check result is 0 or 1.</td>
<td>The system periodically checks the status and returns check results using value 0 or 1.</td>
<td>When the power source of the physical host fails or the hardware/software becomes faulty, the check result is 1.</td>
</tr>
</tbody>
</table>

- **Key Management Service (KMS)**
  The encryption feature relies on KMS. You can use an encrypted image or EVS disks when creating an ECS. In such a case, you are required to use the key provided by KMS to improve data security.
- **Cloud Trace Service (CTS)**
  Allows you to record ECS-related operations for later query, audit, and backtrack.
- **Cloud Server Backup Service (CSBS)**
  Protects ECS backups. CSBS backs up all EVS disks of an ECS, including the system disk and data disks, and uses the backup to restore the ECS.

### 1.8.3 User Permissions

Two types of permissions are provided by default: user management and resource management.
• User management refers to the management of users, user groups, and user group rights.
• Resource management refers to the control operations that can be performed by users on cloud service resources.

For further details, see Permission Description.
2 Getting Started

2.1 Creating and Logging In to a Windows ECS

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.

Step 1: Create an ECS
Step 2: Log In to the ECS

Step 1: Create an ECS

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. Click Create ECS.
   The ECS creation page is displayed.

NOTE
SAP High-Performance Analytic Appliance (HANA) is a high-performance real-time data computing platform based on memory computing technologies. The public cloud provides high-performance IaaS services that comply with SAP HANA requirements. These services include applying for HANA ECSs and public IP addresses as well as installing and configuring SAP HANA. Such services facilitate applications on the public cloud platform of resources required by SAP HANA, improving the efficiency of user operations, reducing operation costs, and enhancing user experience.

HANA ECSs are dedicated for SAP HANA. If you have deployed SAP HANA on cloud servers, you can create HANA ECSs.

For more information about HANA ECS application scenarios and creation methods, see SAP HANA User Guide.

5. Confirm the region.
   If the region is incorrect, click in the upper left corner of the page for correction.
6. 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.

7. **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 section 1.7.1 ECS Types.

8. **Set DeH.**

DeH refers to physical host resources dedicated for a specified user. You can deploy ECSs on DeHs for better isolation, security, and performance of your ECSs. You can continue using your existing server software licenses of ECSs on DeHs to reduce costs.

If you are required to use DeH resources, click **Configure now**. Otherwise, click **Do not configure**. For more details, see *Dedicated Host User Guide*.

**NOTE**

When creating an ECS on a DeH, if you use a commercial image registered using an external image file, you are required to select BYOL to use your existing OS license.

- For Microsoft Windows Server: Bring your own licenses to the Dedicated Hosts:
  - Open Cloud offers Dedicated Hosts, which allows you to access physical servers that are fully dedicated for your use. You can use your own licensed software on dedicated infrastructure, even without Software Assurance.

- For Microsoft SQL Server: Bring your own licenses with License Mobility:
  - Open Cloud allows you to bring your own licenses with License Mobility to Open Cloud based on Microsoft License Mobility agreement authorized by Microsoft. According to the terms of Microsoft License Mobility, you should purchase the Software Assurance with your Microsoft SQL Server license.

For more details about the official Microsoft software License Mobility, refer to:


You are responsible for complying with Microsoft licensing requirements. This document is only a guide for your convenience and does not constitute legal advice. You are not entitled to rely on descriptions in this document. If you have any questions about your licenses or rights to Microsoft software, please consult your legal team, Microsoft, or your Microsoft reseller.

9. **Click 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 creates 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*.

- **Shared image**
A shared image is a private image shared by another user.

10. **(Optional) Set License Type.**

   Specifies a license type for using an OS or software. If the image you selected is free of charge, this parameter is unavailable. If the image you selected is billed, this parameter is available.
   - **Use license from the system**
     Allows you to use the license provided by the public cloud platform. Obtaining the authorization of such a license is billed.
   - **Bring your own license (BYOL)**
     Allows you to use your existing OS license. In such a case, you do not need to apply for a license again.

   For more details, see section 1.4.4 License Type.

11. **Set Disk.**

    A disk can be a system disk or a data disk.
    - **System Disk**
      If the image based on which an ECS is created is not encrypted, the system disk of the ECS is not encrypted. In addition, **Unencrypted** is displayed for the system disk on the page. If the image based on which an ECS is created is encrypted, the system disk of the ECS is automatically encrypted. For details, see section *(Optional) Encryption-related parameters.*
    - **Data Disk**
      You can create multiple data disks for an ECS and configure sharing and encryption for each data disk.
      - **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 section 1.3 Storage.
      - **Share:** indicates that the EVS disk is shared. Such an EVS disk can be attached to multiple ECSs.
      - **Encryption:** indicates that the data disk is encrypted. For details, see section *(Optional) Encryption-related parameters.*

    - *(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. For details, see section 15.8.9 Who Can Use the Encryption Feature?
      - **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.

      For details about the disk types supported by the ECS, see section 1.3 Storage. For more information about EVS disks, see *Elastic Volume Service User Guide.*

12. **Set network parameters, including VPC, Security Group, NIC, and EIP.**
When you use VPC for the first time, the system automatically creates a VPC for you, including the security group and NIC.

### Table 2-1 Parameter descriptions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>Provides a network, including subnet and security group, for an ECS. You can select an existing VPC, or click View VPC and create a desired one. For more information about VPC, see Virtual Private Cloud User Guide. <strong>NOTE</strong> Ensure that DHCP is enabled in the VPC to which the ECS belongs.</td>
</tr>
</tbody>
</table>
| 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 |
| NIC       | Includes primary and extension NICs. 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 ECSs are within the subnet, consecutive, and available.  
  - This subnet cannot duplicate a subnet with a specified start IP address.  
  - **MTU Settings**: optional If your ECS is of M2, large-memory, H1, or D1 type, you can click MTU Settings to configure the maximum transmission unit (MTU) for a to-be-added extension NIC for improving network performance. An MTU can only be a number, ranging from 1280 to 8888. |
| EIP       | A static public IP address bound to an ECS in a VPC. Using the EIP, the ECS provides services externally. |
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The following options are provided:</td>
</tr>
<tr>
<td>Not required</td>
<td>Without an EIP, the ECS cannot access the Internet and is used only in the private network or cluster.</td>
</tr>
<tr>
<td>Automatically assign</td>
<td>The system automatically assigns an EIP for the ECS. The EIP provides exclusive bandwidth that is configurable.</td>
</tr>
<tr>
<td>Use existing</td>
<td>An existing EIP is assigned for the ECS. When using an existing EIP, you cannot create ECSs in batches.</td>
</tr>
</tbody>
</table>

13. **Set Login Mode.**

   The login mode is **Key pair**, which allows you to use a key pair for 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.

14. **Configure Auto Recovery.**

   Once a physical host accommodating ECSs breaks down, the ECSs with automatic recovery enabled automatically migrate to a functional host. This minimizes user service interruption. These ECSs will restart in this process. If automatic recovery is not enabled, the affected users must wait for the system administrator to recover ECSs after the physical host becomes faulty. For more information about automatic recovery, see section **3.6 Automatically Recovering ECSs.**

   **NOTE**
   An ECS with any of the following resources cannot be automatically recovered:
   - Local disk
   - Passthrough FPGA card
   - Passthrough InfiniBand NIC

15. **Configure Advanced Settings.**

   To use functions listed in **Advanced Settings**, click **Configure now**. Otherwise, click **Do not configure.**

   - **File Injection**
     Enables the ECS to automatically inject a script file or other files into a specified directory on an ECS when you create the ECS. 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 details about file injection, see section **3.4.3 Injecting Files into ECSs.**

   - **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 section **3.4.2 Injecting User Data into ECSs.**
Elastic Cloud Server
User Guide

2 Getting Started

- ECS Group
  An ECS group applies the anti-affinity policy to the ECSs in it so that the ECSs can be distributed on different hosts. This configuration is optional. For instructions about how to create an ECS group, see section 3.3 Managing ECS Groups.

- Tag
  Tags an ECS, facilitating ECS identification and management. This configuration is optional. You can add up to 10 tags to an ECS.

**NOTE**
Tags added during ECS creation will also be added to the created EIP and EVS disks (including the system disk and data disks) of the ECS. If the ECS uses an existing EIP, the tags will not be added to the EIP.

After creating the ECS, you can view the tags on the pages providing details about the ECS, EIP, and EVS disks.

For detailed operations, see section 12 Tags.

- Agency Name
  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 rights 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 name 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.

16. 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 purchased 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 purchase 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.

17. Configure the number of ECSs to be created.
18. Click **Create Now**.
19. On the ECS specification confirmation page, confirm the ECS specifications, select **I have read the agreement and agree to its terms**, and click **Submit**.
   After the ECS is created, you can view information about it on the **Elastic Cloud Server** page.

**NOTE**
Creating an ECS takes several minutes. You can check the creation progress by viewing the ECS creation status. For details, see section 3.1.1 Viewing ECS Creation Statuses.
Step 2: Log In to the 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. Obtain the password.
   Use the password obtaining function provided by the management console to decrypt the private key file to obtain a password.
   For details, see section 5.4 Obtaining the Password for Logging In to a Windows ECS.

2. Select a login method and log in to the ECS.
   - VNC
     For details, see section 4.1.2 Login Using VNC.
   - MSTSC
     For details, see section 4.1.3 Login Using an MSTSC Password.

Follow-up Procedure

- After an ECS with automatic recovery enabled is created, you can check whether this function has been enabled by viewing Failures. For details, see section 3.1.2 Viewing Failures.
- 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 section 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 section 1.7.1 ECS Types.
2.2 Creating and Logging In to a Linux ECS

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.

Step 1: Create an ECS

Step 2: Log In to the ECS

Step 1: Create an ECS

1. Log in to the management console.

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


4. Click Create ECS.

The ECS creation page is displayed.

NOTE

SAP High-Performance Analytic Appliance (HANA) is a high-performance real-time data computing platform based on memory computing technologies. The public cloud provides high-performance IaaS services that comply with SAP HANA requirements. These services include applying for HANA ECSs and public IP addresses as well as installing and configuring SAP HANA. Such services facilitate applications on the public cloud platform of resources required by SAP HANA, improving the efficiency of user operations, reducing operation costs, and enhancing user experience.

HANA ECSs are dedicated for SAP HANA. If you have deployed SAP HANA on cloud servers, you can create HANA ECSs.

For more information about HANA ECS application scenarios and creation methods, see SAP HANA User Guide.

5. Confirm the region.

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

6. 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.

7. 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 section 1.7.1 ECS Types.

8. Set DeH.

DeH refers to physical host resources dedicated for a specified user. You can deploy ECSs on DeHs for better isolation, security, and performance of your ECSs. You can continue using your existing server software licenses of ECSs on DeHs to reduce costs.
If you are required to use DeH resources, click **Configure now**. Otherwise, click **Do not configure**. For more details, see *Dedicated Host User Guide*.

### NOTE

When creating an ECS on a DeH, if you use a commercial image registered using an external image file, you are required to select BYOL to use your existing OS license.

- **For Microsoft Windows Server: Bring your own licenses to the Dedicated Hosts:**
  
  Open Cloud offers Dedicated Hosts, which allows you to access physical servers that are fully dedicated for your use. You can use your own licensed software on dedicated infrastructure, even without Software Assurance.

- **For Microsoft SQL Server: Bring your own licenses with License Mobility:**
  
  Open Cloud allows you to bring your own licenses with License Mobility to Open Cloud based on Microsoft License Mobility agreement authorized by Microsoft. According to the terms of Microsoft License Mobility, you should purchase the Software Assurance with your Microsoft SQL Server license.

For more details about the official Microsoft software License Mobility, refer to:


https://www.redhat.com/en/technologies/cloud-computing/cloud-access


You are responsible for complying with Microsoft licensing requirements. This document is only a guide for your convenience and does not constitute legal advice. You are not entitled to rely on descriptions in this document. If you have any questions about your licenses or rights to Microsoft software, please consult your legal team, Microsoft, or your Microsoft reseller.

9. **Click 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 creates 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*.

    - **Shared image**
      
      A shared image is a private image shared by another user.

10. **(Optional) Set License Type.**

    Specifies a license type for using an OS or software. If the image you selected is free of charge, this parameter is unavailable. If the image you selected is billed, this parameter is available.

    - **Use license from the system**
      
      Allows you to use the license provided by the public cloud platform. Obtaining the authorization of such a license is billed.

    - **Bring your own license (BYOL)**
      
      Allows you to use your existing OS license. In such a case, you do not need to apply for a license again.

    For more details, see section 1.4.4 License Type.
11. Set Disk.
   A disk can be a system disk or a data disk.
   - System Disk
     If the image based on which an ECS is created is not encrypted, the system disk of
     the ECS is not encrypted. In addition, **Unencrypted** is displayed for the system disk
     on the page. If the image based on which an ECS is created is encrypted, the system
     disk of the ECS is automatically encrypted. For details, see section (Optional)
     Encryption-related parameters.
   - Data Disk
     You can create multiple data disks for an ECS and configure sharing and encryption
     for each data disk.
     - **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 section 1.3 Storage.
     - **Share**: indicates that the EVS disk is shared. Such an EVS disk can be
       attached to multiple ECSs.
     - **Encryption**: indicates that the data disk is encrypted. For details, see section
       (Optional) Encryption-related parameters.
   - (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. For details, see section 15.8.9 Who Can Use the
     Encryption Feature?
     - **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.
     For details about the disk types supported by the ECS, see section 1.3 Storage. For more
     information about EVS disks, see Elastic Volume Service User Guide.

12. Set network parameters, including VPC, Security Group, NIC, and EIP.
   When you use VPC for the first time, the system automatically creates a VPC for you,
   including the security group and NIC.

   **Table 2-2 Parameter descriptions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>Provides a network, including subnet and security group, for an ECS. You can select an existing VPC, or click View VPC and create a desired one. For more information about VPC, see Virtual Private Cloud User Guide.</td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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 |
| NIC | Includes primary and extension NICs. 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 ECSs are within the subnet, consecutive, and available.  
- This subnet cannot duplicate a subnet with a specified start IP address.  
- **MTU Settings:** optional  
If your ECS is of M2, large-memory, H1, or D1 type, you can click **MTU Settings** to configure the maximum transmission unit (MTU) for a to-be-added extension NIC for improving network performance. An MTU can only be a number, ranging from 1280 to 8888. |
| EIP | 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:  
- **Not required**  
Without an EIP, the ECS cannot access the Internet and is used only in the private network or cluster.  
- **Automatically assign**  
The system automatically assigns an EIP for the ECS. The EIP provides exclusive bandwidth that is configurable.  
- **Use existing**  
An existing EIP is assigned for the ECS. When using an existing EIP, you cannot create ECSs in batches. |
13. **Set Login Mode.**

The login mode is **Key pair**, which allows you to use a key pair for 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.

14. **Configure Auto Recovery.**

Once a physical host accommodating ECSs breaks down, the ECSs with automatic recovery enabled automatically migrate to a functional host. This minimizes user service interruption. These ECSs will restart in this process. If automatic recovery is not enabled, the affected users must wait for the system administrator to recover ECSs after the physical host becomes faulty. For more information about automatic recovery, see section **3.6 Automatically Recovering ECSs**.

**NOTE**

An ECS with any of the following resources cannot be automatically recovered:

- Local disk
- Passthrough FPGA card
- Passthrough InfiniBand NIC

15. **Configure Advanced Settings.**

To use functions listed in **Advanced Settings**, click **Configure now**. Otherwise, click **Do not configure**.

- **File Injection**

  Enables the ECS to automatically inject a script file or other files into a specified directory on an ECS when you create the ECS. 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 details about file injection, see section **3.4.3 Injecting Files into ECSs**.

- **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 section **3.4.2 Injecting User Data into ECSs**.

- **ECS Group**

  An ECS group applies the anti-affinity policy to the ECSs in it so that the ECSs can be distributed on different hosts. This configuration is optional. For instructions about how to create an ECS group, see section **3.3 Managing ECS Groups**.

- **Tag**

  Tags an ECS, facilitating ECS identification and management. This configuration is optional. You can add up to 10 tags to an ECS.

**NOTE**

Tags added during ECS creation will also be added to the created EIP and EVS disks (including the system disk and data disks) of the ECS. If the ECS uses an existing EIP, the tags will not be added to the EIP.

After creating the ECS, you can view the tags on the pages providing details about the ECS, EIP, and EVS disks.
For detailed operations, see section 12 Tags.

- **Agency Name**

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 rights 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 name 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*.

16. **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 purchased 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 purchase 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.

17. Configure the number of ECSs to be created.

18. Click **Create Now**.

19. On the ECS specification confirmation page, confirm the ECS specifications, select **I have read the agreement and agree to its terms**, and click **Submit**.

After the ECS is created, you can view information about it on the **Elastic Cloud Server** page.

**NOTE**

Creating an ECS takes several minutes. You can check the creation progress by viewing the ECS creation status. For details, see section 3.1.1 **Viewing ECS Creation Statuses**.

**Step 2: Log In to the ECS**

You can log in to a Linux ECS using either VNC or SSH key provided on the management console.

**Figure 2-2** Linux ECS login modes
1. Log in to the management console.
3. Select the ECS you want to log in to.
4. Select a login method and log in to the ECS.
   - VNC
     For details, see section 4.2.4 Login Using VNC.
   - SSH key
     When you log in to the ECS using the SSH key, you need to bind an EIP to the ECS.
     For details, see section 4.2.2 Login Using an SSH Key.

   ![NOTE]
   - If a public image is used, the username of the image is root in the Mexico region and linux in other regions.
   - If you have activated user root permission using user data injection or file injection during ECS creation, you can log in to the ECS as user root.

Follow-up Procedure

- After an ECS with automatic recovery enabled is created, you can check whether this function has been enabled by viewing Failures. For details, see section 3.1.2 Viewing Failures.
- 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 section 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 section 1.7.1 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 an EVS disk is attached to a server, you need to log in to the server to initialize the disk, that is, format the disk. The disk can be used after being initialized.

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

In both cases, the data disk can only be used after being initialized. Choose a proper disk partition style base on your service plans.

**Disk Partition Style**

Table 2-3 lists the common disk partition styles. For Linux OSs, different disk partition styles require different partitioning tools.

<table>
<thead>
<tr>
<th>Disk Partition Style</th>
<th>Maximum Disk Capacity Supported</th>
<th>Maximum Number of Partitions Supported</th>
<th>Linux Partitioning Tool</th>
</tr>
</thead>
</table>
| Master Boot Record (MBR) | 2 TB | • 4 primary partitions  
• 3 primary partitions and 1 extended partition | • fdisk  
• parted |
| Guid Partition Table (GPT) | 18 EB  
**NOTE**  
1 EB = 1048576 TB | Unlimited  
**NOTE**  
Disk partitions allocated using GPT are not categorized. | parted |

**NOTE**

The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Currently, an EVS data disk supports up to 32 TB. Therefore, use the GPT partition style if your disk capacity is greater than 2 TB.
If you change the disk partition style after the disk has been used, the original 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 section 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 greater than 2 TB. For details about disk partition styles, see section 2.3.1 Scenarios and Disk Partitions.

The method for initializing an EVS 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 OSs running on the corresponding servers.

**Prerequisites**

- 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.
- A data disk has been attached to the server and has not been initialized.

**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.
Step 3  Disks are listed 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),
and click OK, as shown in Figure 2-6.
The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Currently, an EVS data disk supports up to 32 TB. Therefore, use the GPT partition style if your disk capacity is greater than 2 TB.

If you change the disk partition style after the disk has been used, the original 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, as shown in Figure 2-7.
Figure 2-7 Creating a 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 simple volume size as required (the default value is the maximum) and click Next.
Figure 2-9 Specify Volume Size

Step 9  Assign the driver letter and click Next.

Figure 2-10 Assigning 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
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** to complete the wizard. 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 section 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 greater than 2 TB. For details about disk partition styles, see section 2.3.1 **Scenarios and Disk Partitions**.

The method for initializing an EVS 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 OSs running on the corresponding servers.
Elastic Cloud Server
User Guide

2 Getting Started

Prerequisites

- 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.
- A data disk has been attached to the server and has not been initialized.

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 navigation tree on the left, choose File and Storage Services.

The Servers page is displayed.
Step 4  In the navigation tree on the left, choose **Disks**.

The **Disks** page is displayed.
**Step 5** Disks are listed in the right pane. If the new disk is in the offline state, bring it online before initialize it.

1. Right-click the new disk and choose **Bring Online** from the shortcut menu. The **Bring Disk Online** dialog box is displayed.

**Figure 2-17 Bring Disk Online**

2. Click **Yes** to confirm the operation.

3. Click ![refresh](image) in the upper area of the page to refresh the disk information. When the disk status changes from **Offline** to **Online**, the disk has been brought online.
Step 6  After the disk has been brought online, initialize the disk.

1. Right-click the new disk and choose Initialize from the shortcut menu. The Initialize Disk dialog box is displayed.

2. Click Yes to confirm the operation.
3. Click ![refresh icon] in the upper area of the page to refresh the disk information. When the disk partition changes from Unknown to GPT, the initialization is complete.

**Figure 2-20 Completing initialization**

![Disk initialization](image)

**Step 7** In the lower left area of the page, click *To create a volume, start the New Volume Wizard* to create a new volume.

The New Volume Wizard window is displayed.
Step 8  Follow the prompts and click Next.

The Select the server and disk page is displayed.

Figure 2-22 Select the server and disk
Step 9  Select the server and disk, and then click Next. The system selects the server attached with
the disk by default. You can specify the server based on your requirements. In this example,
the default setting is used.

The Specify the size of the volume page is displayed.

Figure 2-23 Specify the size of the volume (Windows 2016)

Step 10  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 to a drive letter or folder page is displayed.
Step 11 Assign the volume to a drive letter or folder and click **Next**. The system assigns the volume to drive letter D by default. In this example, the default setting is used.

The **Select file system settings** page is displayed.
Step 12 Specify file system settings and click Next. The system selects the NTFS file system by default. You can specify the file system type based on the actual condition. In this example, the default setting is used.

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

The Confirm selections page is displayed.

Figure 2-26 Confirm selections

Step 13 Confirm the volume location, volume properties, and file system settings. Then click Create to create a volume.

If the page shown in Figure 2-27 is displayed, the volume is successfully created.
Step 14  After the volume is created, click and check whether a new volume appears in File Explorer. 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.
If New Volume (D:) does not appear, perform the following operations to assign the volume to another drive letter or folder:

a. Click , enter cmd, and press Enter.
   The Administrator: Command Prompt window is displayed.

b. Run the diskmgmt command.
   The Disk Management page is displayed.
c. In the right pane of Disk 1, right-click and choose **Change Drive Letter and Paths**.

The **Change Drive Letter and Paths for New Volume** dialog box is displayed.

**Figure 2-30 Change Drive Letter and Paths for New Volume**

![Change Drive Letter and Paths for New Volume](image)

- Click **Add**.
The **Add Drive Letter or Path** dialog box is displayed.

**Figure 2-31 Add Drive Letter or Path**

Add Drive Letter or Path

![Add Drive Letter or Path](image)

1. Select **Assign the following drive letter** to re-assign the volume to a drive letter. Then, click **OK**. Drive letter D is used in this example.

2. After assigning the drive letter, you can view New Volume (D:) in File Explorer.

### 2.3.4 Initializing a Linux Data Disk (fdisk)

#### Scenarios

This section uses CentOS 7.0 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 greater than 2 TB. In Linux OSs, if the GPT partition style is used, the fdisk partitioning tool cannot be used. The parted partitioning tool must be used. For details about disk partition styles, see section 2.3.1 Scenarios and Disk Partitions.

The method for initializing an EVS 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 OSs running on the corresponding servers.

#### Prerequisites

- 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*.
- A data disk has been attached to the server and has not been initialized.
Creating Partitions and Mounting a Disk

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 ext3 file system, mounted on `/mnt/sdc`, and configured automatic mounting upon system start.

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

```bash
fdisk -l
```

Information similar to the following is displayed:

```
[root@ecs-b656 test]# fdisk -l
Disk /dev/xvda: 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: 0x000cc4ad

Device Boot Start End Blocks Id System
/dev/xvda1 * 2048 2050047 1024000 83 Linux
/dev/xvda2 2050048 22530047 10240000 83 Linux
/dev/xvda3 22530048 24578047 1024000 83 Linux
/dev/xvda4 24578048 83886079 29654016 5 Extended
/dev/xvda5 24580096 26628095 1024000 82 Linux swap / Solaris
```

In the command output, the server contains two disks. `/dev/xvda` is the system disk, and `/dev/xvdb` is the added data disk.

**Step 2** Run the following command to enter fdisk to partition the added data:

```bash
fdisk /dev/xvdb
```

In this example, `/dev/xvdb` is the added data disk.

**fdisk /dev/xvdb**

Information similar to the following is displayed:

```
[root@ecs-b656 test]# fdisk /dev/xvdb
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 0xb00005bd.
Command (m for help):
```

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

Information similar to the following is displayed:
There are two types of disk partitions:

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

**Step 4** Enter p and press Enter to create a primary partition.

Information similar to the following is displayed:

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

Partition number indicates the serial number of the primary partition. The value can be 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:

```plaintext
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048):

First sector indicates the first sector. The value can be 2048 to 20971519, and the default value is 2048.
```

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

Information similar to the following is displayed:

```plaintext
First sector (2048-20971519, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):

Last sector indicates the last sector. The value can be 2048 to 20971519, and the default value is 20971519.
```

**Step 7** Select the default last sector 20971519 and press Enter.

Information similar to the following is displayed:

```plaintext
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):
Using default value 20971519
Partition 1 of type Linux and of size 10 GiB is set
Command (m for help):
```

A primary partition has been created for a 10-GB data disk.

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

Information similar to the following is displayed:

```plaintext
Command (m for help): p
Disk /dev/xvdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
```
Elastic Cloud Server
User Guide

2 Getting Started

Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xb00005bd

Device          Start     End      Blocks   Id  System
/dev/xvdb1      2048  20971519  10484736   83  Linux

Command (m for help):

Details about the /dev/xvdb1 partition are displayed.

**Step 9** Enter `w` and press `Enter` to write the changes into 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 successfully 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:

```bash
partprobe
```

**Step 11** Run the following command to set the format for the file system of the newly created partition:

```bash
mkfs -t File system format /dev/xvdb1
```

For example, run the following command to set the `ext3` file system for the `/dev/xvdb1` partition:

```
mkfs -t ext3 /dev/xvdb1
```

Information similar to the following is displayed:

```
[root@ecs-b656 test]# mkfs -t ext3 /dev/xvdb1
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
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 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
```
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
```

For 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 /dev/xvdb1 Mount point
```

For example, run the following command to mount the newly created partition on /mnt/sdc:

```
mount /dev/xvdb1 /mnt/sdc
```

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

```
ls -TH
```

Information similar to the following is displayed:

```
[root@ecs-b656 test]# df -TH
Filesystem   Type         Size  Used  Avail Use% Mounted on
/dev/xvda2   xfs          11G   7.4G  3.2G  71% /
devtmpfs     devtmpfs     4.1G   0   4.1G  0% /dev
tmpfs        tmpfs        4.1G  8.2k   4.1G  1% /dev/shm
tmpfs        tmpfs        4.1G   9.2M   4.1G  1% /run
tmpfs        tmpfs        4.1G   0   4.1G  0% /sys/fs/cgroup
/dev/xvda3   xfs          1.1G   39M   1.1G  4% /home
/dev/xvda1   xfs          1.1G  131M   915M 13% /boot
/dev/xvdb1   ext3         11G  38M   9.9G  1% /mnt/sdc
```

The newly created /dev/xvdb1 is mounted on /mnt/sdc.

----

**Setting Automatic Disk Mounting at System Start**

To automatically mount a disk when a server starts, you should not specify its partition, for example /dev/xvdb1, 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 automatically mount a disk at system start.

**NOTE**

The UUID is the unique character string for disk partitions in a Linux system.
2.3.5 Initializing a Linux Data Disk (parted)

Scenarios

This section uses CentOS 7.0 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 greater than 2 TB. In Linux OSs, if the GPT partition style is used, the fdisk partitioning tool cannot be used. The parted partitioning tool must be used. For details about disk partition styles, see section 2.3.1 Scenarios and Disk Partitions.

The method for initializing an EVS 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 OSs running on the corresponding servers.

Prerequisites

- 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.
- A data disk has been attached to the server and has not been initialized.
Creating Partitions and Mounting a Disk

The following example shows you how new partitions can be created on a new data disk that has been attached to a server. The partitions will be created using parted, and GPT is used as the partition style. Furthermore, the partitions will be formatted using the ext3 file system, mounted on `/mnt/sdc`, and configured automatic mounting at system start.

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

```
lsblk
```

Information similar to the following is displayed:

```
lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0   40G  0 disk
├─xvda1 202:1    0    4G  0 part [SWAP]
└─xvda2 202:2    0   36G  0 part /
xvdb    202:16   0  10G  0 disk
```

In the command output, the server contains two disks. `/dev/xvda` is the system disk, and `/dev/xvdb` is the added data disk.

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

```
parted
```

Information similar to the following is displayed:

```
parted /dev/xvdb
```

**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/xvdb: unrecognised disk label
Model: Xen Virtual Block Device (xvd)
Disk /dev/xvdb: 10.7GB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:
```

In the command output, the Partition Table value is unknown, indicating that the disk partition style is unknown.

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

```
mklabel
```

**Disk partition style**

For example, run the following command to set the partition style to GPT: (Disk partition styles include MBR and GPT.)

```
mklabel gpt
```
The maximum disk capacity supported by MBR is 2 TB, and that supported by GPT is 18 EB. Currently, an EVS data disk supports up to 32 TB. Therefore, use the GPT partition style if your disk capacity is greater than 2 TB.

If you change the disk partition style after the disk has been used, the original 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: Xen Virtual Block Device (xvd)
Disk /dev/xvdb: 20971520s
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:
Number  Start   End        Size       File system  Name  Flags
```

**Step 6** Enter `units` and press Enter to set the measurement unit of the disk to sector numbers.

**Step 7** Enter `mkpart opt 2048s 100%` and press Enter.

In this example, one partition is created for the added data disk. Variable `2048s` indicates the disk start capacity, and variable `100%` indicates the disk end capacity. The two values are used for reference only. You can determine the number of partitions and the partition capacity 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 the details about the created partition.

Information similar to the following is displayed:

```
(parted) p
Model: Xen Virtual Block Device (xvd)
Disk /dev/xvdb: 20971520s
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:
Number  Start   End        Size       File system  Name  Flags
1      2048s   20969471s  20967424s               opt
```

Details about the `/dev/xvdb1` 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:

```
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda   202:0   0  40G  0 disk
├─xvda1 202:1   0  4G  0 part [SWAP]
└─xvda2 202:2   0  36G  0 part /
```

In the command output, `/dev/xvdb1` is the partition you created.

Step 11  Run the following command to set the format for the file system of the newly created partition:

```
mkfs -t File system format /dev/xvdb1
```

For example, run the following command to set the `ext3` file system for the `/dev/xvdb1` partition:

```
mkfs -t ext3 /dev/xvdb1
```

Information similar to the following is displayed:

```
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
655360 inodes, 26214391 blocks
1310719 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:
732768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
74096000, 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
```

For 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 /dev/xvdb1 Mount point
```

For example, run the following command to mount the newly created partition on `/mnt/sdc`:

```
mount /dev/xvdb1 /mnt/sdc
```

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

```
df -TH
```

Information similar to the following is displayed:

```
[root@ecs-centos-70 linux]# df -TH
Filesystem Type Size Used Avail Use% Mounted on
/dev/xvda2 xfs 39G 4.0G 35G 11% /
devtmpfs devtmpfs 946M 0 946M 0% /dev
tmpfs tmpfs 954M 0 954M 0% /dev/shm
tmpfs tmpfs 954M 9.1M 945M 1% /run
tmpfs tmpfs 954M 0 954M 0% /sys/fs/cgroup
/dev/xvdb1 ext3 11G 38M 101G 1% /mnt/sdc
```

The newly created `/dev/xvdb1` is mounted on `/mnt/sdc`.

```
----
End
```

### Setting Automatic Disk Mounting at System Start

To automatically mount a disk when a server starts, you should not specify its partition, for example `/dev/xvdb1`, 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 automatically mount a disk at system start.

**NOTE**
The 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
```

For example, run the following command to query the UUID of `/dev/xvdb1`:

```
blkid /dev/xvdb1
```

Information similar to the following is displayed:

```
[root@ecs-b656 test]# blkid /dev/xvdb1
/dev/xvdb1: UUID="1851e23f-1c57-40ab-86bb-5fc5fe606f6a" TYPE="ext3"
```

The UUID of `/dev/xvdb1` 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:

<table>
<thead>
<tr>
<th>UUID</th>
<th>Mount Point</th>
<th>File System</th>
<th>Options</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUID=1851e23f-1c57-40ab-86bb-5fc5fc606ffa</td>
<td>/mnt/sdc</td>
<td>ext3</td>
<td>defaults</td>
<td>0 2</td>
</tr>
</tbody>
</table>

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

The system saves the configurations and exits the vi editor.

----End
3 ECS Instances

3.1 Viewing ECS Information

3.1.1 Viewing ECS Creation Statuses

Scenarios

After clicking Submit to apply for creating an ECS, you can view the task status in the Task Status area. A task involves several sub-tasks, such as creating ECS resources, binding an EIP, and attaching an EVS disk.

**Creating:** A task is being processed.

**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. For instructions about how to handle the failure, see section 14.11 How Do I Handle Error Messages Displayed on the Management Console?

This section describes how to view an ECS creation status and the information displayed in the Task Status area.

Procedure

1. Log in to the management console.
2. Click 🏛️ in the upper left corner and select the desired region and project.
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, Restart, and More.
5. Click the number displayed in the Task Status area and view details about the tasks.

**NOTE**
If you find that the Task Status area shows an ECS creation failure but the ECS list displays the created ECS, see section 15.1.7 Why Does the Task Status Area Show an ECS Creation Failure But the ECS List Displays the Created ECS?
3.1.2 Viewing Failures

Scenarios

The **Failures** area shows the tasks that failed to process due to an error, including the task name and status. Such information is displayed on the management console in one of the following scenarios:

- **Operation failed**
  - Modifying ECS specifications
    
    If an ECS specifications modification failed, this operation is recorded in **Failures**.
  - Automatic recovery enabled during ECS creation
    
    Automatic recovery is enabled during ECS creation. After the ECS is created, if the system fails to enable automatic recovery, this operation is recorded in **Failures**.

This section describes how to view 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, such as **Start, Stop, Restart**, and **More**.

**NOTE**

If **Failures** is not displayed on the management console, the following tasks have been successfully executed:

- The ECS specifications are modified.
- Automatic recovery is enabled during ECS creation.

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 to rapidly locate faults.

3.1.3 Viewing ECS Details

Scenarios

After creating 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 upper right corner of the ECS list, enter the ECS name, IP address, or ID, and click . Alternatively, click Search by Tag above the upper right corner of the ECS list and search for an ECS by tag key and value.

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 or tag to it, or bind an EIP to it, by clicking corresponding links or buttons.

### 3.1.4 Exporting ECSs

#### 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.
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.

### 3.2 Managing OSs

#### 3.2.1 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 password for logging in to the ECS is reset. To retrieve the password, perform the following operations:
- For a Linux ECS, log in to it using the key and set a new password. For instructions about how to log in to an ECS using a key pair, see section 4.2.2 Login Using an SSH Key.
- For a Windows ECS, retrieve the password by following the instructions provided in section 5.4 Obtaining the Password for Logging In to a Windows ECS.

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.

Prerequisites
- The target ECS is in the Stopped or Reinstallation failed state.
- The target ECS has a system disk attached.
- Necessary data has been backed up. (Reinstalling the OS clears the data in all partitions of the EVS system disk, including the system partition.)

Procedure
1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. Locate the row containing the target ECS. Click More in the Operation column and select Reinstall OS.
   If the ECS is not in the Stopped or Reinstallation failed state, stop the ECS before proceeding with reinstallation.
5. (Optional) Select a License Type (Use license from the system or Bring your own license (BYOL)) if the reinstalled OS running on your ECS is charged. For more details, see section 1.4.4 License Type.
   The following OSs are charged:
   - SUSE Linux Enterprise Server
   - Oracle Enterprise Linux
   - Red Hat Enterprise Linux
6. Configure the login mode.
   If the target ECS uses key authentication, you can replace the original key pair.
7. Configure user data injection.
   - If you select User Data Injection and enter data in the text box, the user data imported to the ECS will be updated to the data entered in the text box.
   - If you select User Data Injection but leave the text box blank, the user data imported to the ECS will be cleared.
   - If you do not select User Data Injection, the user data imported to the ECS will not be updated.
8. Click OK.
9. 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 automatically be 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 9 again to retry reinstalling the OS again.

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

3.2.2 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.

Notes

- After the OS is changed, the original OS is not retained, and the original system disk is deleted.
- Necessary data has been backed up using either of the following methods. (Changing the OS clears the data in all partitions of the system disk, including the system partition.)
  - Use VBS to create a backup for your EVS disk. After the OS is changed, the backup can be used to restore the EVS disk, maximizing your data correctness and security.
  - Use CSBS to back up your full ECS. After the OS is changed, the backup can be used to restore the ECS service data, maximizing your data correctness and security and ensuring service continuity.
- 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.
- After the OS is changed, the password for logging in to the ECS will be reset. To retrieve the password, perform the following operations:
  - For a Linux ECS, log in to it using the key and set a new password. For instructions about how to log in to an ECS using a key pair, see section 4.2.2 Login Using an SSH Key.
- For a Windows ECS, retrieve the password by following the instructions provided in section 5.4 Obtaining the Password for Logging In to a Windows ECS.

- The system disk capacity of an ECS with OS changed may change because the system disk capacity specified by the image of the changed OS may be changed.

Constraints

- The EVS disk quota must be greater than 0.

Notes on Cross-OS Changing

Cross-OS changing indicates that the OS is changed between Windows and Linux.

- To change Windows to Linux, install an NTFS partition tool, such as NTFS-3G for data reading and writing on the Windows ECS.

- To change Linux to Windows, install software, such as Ext2Read or Ext2Fsd to identify ext3 or ext4.

**NOTE**

You are not advised to change Linux to Window on the cloud platform. The reason is as follows: If there are LVM partitions on the Linux ECS, these partitions may fail after the OS is changed to Windows.

Prerequisites

- The target ECS is stopped, or changing/reinstalling OS on the ECS failed.

- 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 you 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.

Procedure

1. Log in to the management console.

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


4. Select the target ECS and click Stop in the upper left corner of the ECS list.

5. Locate the row containing the target ECS. Click More in the Operation column and select Change OS.

  The Change OS page is displayed.
6. Modify related ECS parameters, such as Image Type and Image, based on service requirements.
   For more details, see section 2.1 Creating and Logging In to a Windows ECS.

7. (Optional) Select a License Type (Use license from the system or Bring your own license (BYOL)) if the changed OS running on your ECS is billed. For more details, see section 1.4.4 License Type.
   The following OSs are billed:
   - SUSE Linux Enterprise Server
   - Oracle Enterprise Linux
   - Red Hat Enterprise Linux

8. Configure the login mode.
   If the target ECS uses key authentication, you can replace the original key pair.

9. Configure user data injection.
   - If you select User Data Injection and enter data in the text box, the user data imported to the ECS will be updated to the data entered in the text box.
   - If you select User Data Injection but leave the text box blank, the user data imported to the ECS will be cleared.
   - If you do not select User Data Injection, the user data imported to the ECS will not be updated.

10. Click OK.

11. On the Change ECS 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 automatically be deleted.

Follow-up Procedure
If the OS change is unsuccessful, perform steps 3 to 11 again to retry changing the OS again.
If the second OS change attempt is unsuccessful, contact customer service for manual recovery at the backend.

3.3 Managing ECS Groups

Scenarios
ECSs in an ECS group comply with the same policy. Only the anti-affinity policy is available now, which enables the ECSs in the same ECS group to be deployed on different hosts to improve service reliability.
When creating an ECS, you can add it to an ECS group. After creating the ECS, you can add it to or remove it from 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 Groups**.
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 host different from the hosts accommodating other ECSs in the same ECS group.

Make sure that the ECS to be added has been stopped.

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 Groups**.
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 any more.

Make sure that the ECS to be removed has been stopped.

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 Groups**.
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 any more.

Before deleting an ECS group, remove all ECSs from the ECS group.

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. In the navigation pane on the left, choose ECS Groups.
5. Click Delete in the Operation column of the target ECS group.
6. Click OK.

3.4 Managing User Data and Metadata

3.4.1 Managing ECS Metadata

ECS metadata is used to configure or manage running ECSs. Table 3-1 lists the two sets of APIs that ECS metadata supports.

<table>
<thead>
<tr>
<th>API Type</th>
<th>Metadata Type</th>
<th>Description</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack metadata API</td>
<td>Metadata</td>
<td>Displays ECS metadata.</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>GET Password</td>
<td>Displays the password for logging in to an ECS.</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>User Data</td>
<td>Displays ECS user data.</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>POST Password</td>
<td>Stores the password for logging in to an ECS.</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Security Key</td>
<td>Obtains temporary AKs and SKs.</td>
<td>Supported</td>
</tr>
<tr>
<td>EC2 compatible API</td>
<td>ami-id</td>
<td>Displays the image ID of an ECS.</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>ami-launch-index</td>
<td>Displays an ECS launching sequence.</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>ami-manifest-path</td>
<td>Displays the path where an image list is stored.</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>block-device-mapping</td>
<td>Displays the block device of an ECS.</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>hostname</td>
<td>Displays the name of the host accommodating an ECS.</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>instance-id</td>
<td>Displays an ECS ID.</td>
<td>Supported</td>
</tr>
</tbody>
</table>
### API Type | Metadata Type | Description | Compatibility
---|---|---|---
instance-type | Displays an ECS flavor. | Supported |
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. | Supported |
availability-zone | Displays the AZ accommodating an ECS. | Supported |
public-ipv4 | Displays the floating IP address of an ECS. If there are multiple NICs, only the floating IP address of the primary NIC is displayed. | Supported |
public-keys | Displays the public key of an ECS. | Supported |
reservation-id | Displays an ECS reservation ID. | Supported |
user-data | Displays ECS user data. | Supported |
instant-action | Displays ECS actions. | Not supported |
kernel-id | Displays an ECS kernel image ID. | Not supported |
local-hostname | Displays the local name of an ECS. | Not supported |
public-hostname | Displays the external name of an ECS. | Not supported |
ramdisk-id | Displays an ECS ramdisk image ID. | Not supported |
security-groups | Displays the security group to which an ECS belongs. | Not supported |

The following describes the URI and methods of using the supported ECS metadata.

### Prerequisites

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:** 0.0.0.0/16

### Metadata (OpenStack Metadata API)
Displays ECS metadata.

- **URI**
  
  `/169.254.169.254/openstack/{version}/meta_data.json`

- **Usage method**
  Supports GET requests.

- **Example**
The following section describes how to use the tool cURL to view ECS metadata.

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

```json
{
    "admin_pass": "sWs9YVAiytTs",
    "availability_zone": "manage-az",
    "files": [
        {
            "content_path": "/content/0000",
            "path": "/etc/litao.ini"
        }
    ],
    "hostname": "lt-test-01.novalocal",
    "launch_index": 0,
    "meta": {
        "test_key": "test_vaule"
    },
    "name": "lt-test-01",
    "public_keys": {
        "novakey": "ssh-rsa AAAAB3NzaC1yc2EAAAADQABAAAABAQCr4M6fRqbFRXE31q9NiYVrzsZD/DgAWCGqC461u+x3aLR
RtUwpSoX4W7FlRegHAp7Epih40v0M+9HrKE2bQsaifye0VP/chEFKJLU9cnDNJMiB0WofjLWDOOnUn
sFLZLlPaTAd116TuB02jzq4B8xrYcn3nSsFSYHszvHic0kys7AC+e11L4WNIyeGDSkmsHS0vNI
P0mpRqBzQSMhs/ZEIQQ+YsMoL8z+A+4+v/+/R8K7aJK31bQ8Yu8vky9M1OLG176s9pNtd1rKWN
C4ydYCS8NRxaFyvu009F7105Ekm3WkkhYNmy1Viw49d0OIr63ck8M1j
root@6B1AA2D2-3B57-11DA-8567-00000821800"]
},
"random_seed": "ptvKzBu5SNFrWKAiar6Z2VT7KOGZ83T3VdpEjRdMBoWF0RGKvjNGXasAX2o8KfzBPCq+MupA4Ig9mU
yfWXJiAc171vOVQ7WvubJ4pxQz2tNzrXR7vD5R8WJUqeqZV1Fjxx6xjJKqtWnmrT57J+SEAqRP64ONy
dikPBnI0pnsj+gNMXzEmFL3tQ0j1CzV6Ze2djc8QkT84/dnshpJx/Daak1LVVtmLghP72j/0WNHz
AnvS5ECSS5z51h2YFrnx30J0FJScwn150uFRjo827ThuJXAVhDrcqQ1srV5WXrrWc+e+yeljgy
vaGAd5PCjleaGAEEn60e5B9j4EFZLlkUv7naYGslLoGLjoOq2jvFMgcaKzrv92/YsZDbwHFVVOx/u
NA9Jx7FFIXelNdOFcP8nS4Flp5w6KOVq11EhEBAo1QVKENJ6fbYCoYe4JGK/UEGCAvhJ2PpeeS9L
vnJyQFy6e6/pTtxk1MFe6lgrpQXR8SfEJ+X6j+pRvP8U1WIMB8esq2+qbbjjpR9Tm/aT7M
WqA7oloXzssdQQBBAEH7j/86u8P12ebs6vF4ORM+RUC2FFACONSEQ2AdU1hX9FRqoK9p1o17x9m8aQAj0
SdBr9IMlCDTgVb8DSZ4A2q5ynxZyQAv9WHTcLkeM+05P7748==",
"uuid": "32274de3-6efe-45b3-86a8-46c4335f0e7"
}
```
Password (OpenStack Metadata API)

Configures and displays the password for logging in to an ECS.

- **URI**
  
  `/169.254.169.254/openstack/{version}/password`

- **Usage method**
  
  Supports both GET and POST requests, where
  - The GET request is used to obtain the password.
  - The POST request is used to store the password. Exercise caution when sending a POST request.

- **Examples**
  
  - Example 1: View the password for logging in to an ECS.
    
    `curl http://169.254.169.254/openstack/latest/password`

  - Example 2: Store the password for logging in to an ECS.
    
    `curl -X POST http://169.254.169.254/openstack/latest/password -d "v59nTqCebJKtNnDu"`

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/{version}/user_data`

- **Usage method**
  
  Supports GET requests.

- **Example**
  
  `curl http://169.254.169.254/openstack/latest/user_data`

Security Key (OpenStack Metadata API)

Obtains temporary AKs and SKs.

**NOTE**

- If you need to obtain temporary AKs and SKs on ECSs, authorize the `op_svc_ecs` account in the IAM service.
- Temporary AKs and SKs expire an hour later.
- When using temporary AKs and SKs, add `X-Security-Token:securitytoken` in the message header. `securitytoken` is the value returned when a call is made to the API.

- **URI**
  
  `/openstack/{version}/securitykey`
• Usage method
  Supports GET requests.
• Examples
  
curl http://169.254.169.254/openstack/{version}/securitykey

User Data (EC2 Compatible 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/{version}/user-data
• Usage method
  Supports GET requests.
• Example
  
curl http://169.254.169.254/latest/user-data

Ami ID (EC2 Compatible API)

Displays an ECS image ID.

• URI
  /169.254.169.254/{version}/meta-data/ami-id
• Usage method
  Supports GET requests.
• Example
  

  ami-00000003

Ami Launch Index (EC2 Compatible API)

Displays an ECS launching sequence. The value of the first launched ECS is 0.

• URI
  /169.254.169.254/{version}/meta-data/ami-launch-index
• Usage method
  Supports GET requests.
• Example
  

Ami Manifest Path (EC2 Compatible API)

Displays the path where an image list is stored.
Block Device Mapping (EC2 Compatible API)
Displays the block device of an ECS.

- **URI**
  
  `/169.254.169.254/{version}/meta-data/block-device-mapping/ami`

- **Usage method**
  Supports GET requests.

- **Example**
  ```
  ```

Hostname (EC2 Compatible API)
Displays the name of the host accommodating an ECS. The .novalocal suffix will be added later.

- **URI**
  
  `/169.254.169.254/{version}/meta-data/hostname`

- **Usage method**
  Supports GET requests.

- **Example**
  ```
  ```
  ```
  vm-test.novalocal
  ```

Instance ID (EC2 Compatible API)
Displays an ECS ID.

- **URI**
  
  `/169.254.169.254/{version}/meta-data/instance-id`

- **Usage method**
  Supports GET requests.

- **Example**
  ```
  ```
  ```
i-00000001
  ```
Instance Type (EC2 Compatible API)

Displays an ECS flavor.

- **URI**
  `/169.254.169.254/{version}/meta-data/instance-type`
- **Usage method**
  Supports GET requests.
- **Example**
  `flavor_test`

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/{version}/meta-data/local-ipv4`
- **Usage method**
  Supports GET requests.
- **Example**
  `192.1.1.2`

Availability Zone (EC2 Compatible API)

Displays the AZ accommodating an ECS.

- **URI**
  `/169.254.169.254/{version}/meta-data/placement/availability-zone`
- **Usage method**
  Supports GET requests.
- **Example**
  `az1.dc1`

Public IPv4 (EC2 Compatible API)

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

- **URI**
  `/169.254.169.254/{version}/meta-data/public-ipv4`
- **Usage method**
  Supports GET requests.
- **Example**
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**
  ```
```

Reservation ID (EC2 Compatible API)

Displays an ECS reservation ID.

- **URI**
  `/169.254.169.254/^[version]*/meta-data/reservation-id`

- **Usage method**
  Supports GET requests.

- **Example**
  ```
```

3.4.2 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.

You can also implement these functions using file injection, but user data injection is preferred.

**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 comply with user data script specifications.
- DHCP must be enabled on the VPC network, and port 80 must be enabled for the security group in the outbound direction.

- 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.
  - 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 section Related Links.
2. When creating an ECS, set Advanced Settings 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.
3. 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>
<thead>
<tr>
<th>Table 3-2 Linux ECS script types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>
How can I view the customized user data injected into a Linux ECS?

- Log in to the ECS.
- 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 Text and enter the customized user data script.

```bash
#!/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.

```bash
[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 Text and enter the customized user data script.

```bash
#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.
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 3-3 Windows ECS script types

<table>
<thead>
<tr>
<th>Format</th>
<th>Batch-Processing Program Script</th>
<th>PowerShell Script</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The script must be started with <code>rem cmd</code>, which is the first line of the script. No space is allowed at the beginning of the first line.</td>
<td>The script must be started with <code>#ps1</code>, which is the first line of the script. No space is allowed at the beginning of the first line.</td>
</tr>
<tr>
<td>Constraint</td>
<td>Before Base64 encoding, the size of the script, including the first line, cannot exceed 32 KB.</td>
<td>Before Base64 encoding, the size of the script, including the first line, cannot exceed 32 KB.</td>
</tr>
</tbody>
</table>

- 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 **Text** and enter the customized user data script.

```cmd
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:\.
To view the user data injected into the Windows ECS, log in at http://169.254.169.254/openstack/latest/user_data.

**Example 2: Inject a PowerShell script.**

When creating an ECS, set User Data Injection to 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:\.

To view the user data injected into the Windows ECS, log in at http://169.254.169.254/openstack/latest/user_data.
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:

```bash
#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 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. Table 3-4 lists the password rules.

Table 3-4 Password complexity requirements

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
<th>Example Value</th>
</tr>
</thead>
</table>
| Password  | • Consists of 8 characters to 26 characters.  
|           | • Contains at least three of the following character types:  
|           |   - Uppercase letters  
|           |   - Lowercase letters  
|           |   - Numerals  
|           |   - Special characters:  
|           |     $!@%_-+={}[]\/:^?"'  
|           | • Cannot contain the username or the username in Test12!@ |
### Case 3

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. Table 3-4 lists the password rules.

The content of the script file to be injected is as follows:

```bash
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 4

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:

```bash
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```
Case 5

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 authentication.

The content of the script file to be injected is as follows:

```bash
#cloud-config
disable_root: false
runmd:
- sed -i 's/^PermitRootLogin.*$/PermitRootLogin without-password/'
  /etc/ssh/sshd_config
- sed -i '/^KexAlgorithms.*$/d' /etc/ssh/sshd_config
- service sshd restart
```

Related Links

For more information about user data injection cases, visit the official Cloud-init/Cloudbase-init website:


3.4.3 Injecting Files into ECSs

Scenarios

Use the file injection function to inject files 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

- KVM ECSs do not support file injection. You are advised to use user data injection for such ECSs. For details, see section 3.4.2 Injecting User Data into ECSs.
- Linux
  - Only user `root` can execute injected files.
  - You can inject files into any directory of a Linux EVS system disk. The names of the files to be injected and directories in which they are stored can contain only letters, digits, underscores (_), and periods (.), for example, `/etc/foo.txt`.
  - The file systems supported by Linux EVS system disks are ext3 and ext4.
  - The default permission of the injected files is read and write.
  - To change file permissions, log in to the ECS as user `root`, switch to the directory containing the injected files, and run `chmod 755 Name of the injected file`.
  - Injected files can be manually or automatically executed.
  - To enable the automatic execution of injected files, the files must be stored in the `/etc/init.d` directory and you must have changed the permission of the files.
  - The file size must be less than or equal to 1 KB.
- Windows
  - Only user administrator can execute injected files.
  - You can inject files only into the root directory of drive C. You cannot change the directory for storing the injected files during the file injection process.
  - The file system supported by Windows EVS system disks is NTFS.
  - Injected files can only be manually executed.
  - The file size must be less than or equal to 1 KB.

How to Use File Injection

1. Create a script file that meets your requirements and is compatible with the OS.
2. During ECS creation, select the created script file and set the directory for storing the file.
3. The system automatically creates the ECS and injects the file into the ECS.
4. (Linux) Change the permission of the script file.
5. Execute the script.

Case 1

This case illustrates how to use the file injection function to simplify 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:

```bash
syntax on
set tabstop=4
set number
```

Case 2

This case illustrates how to use the file injection function to initialize ECS configuration.

In this example, the firewall configuration is automatically initialized upon ECS startup. The firewall configuration is written to script file initial.sh, and the file is injected into the /etc/init.d directory.

The content of the script file to be injected is as follows:

```bash
#!/bin/sh
iptables -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -p tcp --dport 49152:65534 -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
```

By default, the injected script file permission is read and write. When you use the ECS for the first time after injecting the script file, you must change the permissions of the injected file and add a file link. To do so, log in to the ECS as user root and run the following commands (This example uses CentOS 6.5, script file initial.sh, and runlevel 3):

```
cd /etc/init.d
```
chmod 775 initial.sh

ln -s /etc/init.d/initial.sh /etc/rc.d/rc3.d/S98initial

**NOTE**
In the preceding commands:
- `/etc/rc.d/rc3.d` indicates the directory for automatically executed script files when the OS runlevel is 3. If the OS runlevel is different, you must change the directory accordingly. For example, if the OS runlevel is 2, change the directory to `/etc/rc.d/rc2.d`.
- The `S` parameter in `S98initial` indicates that the script is executed during OS startup. The `98` parameter in `S98initial` indicates the script startup sequence, meaning that the script is executed in the ninety-eighth place. You can change this value as required. The OS executes scripts one by one in ascending order based on their startup sequence.

After these commands are executed, each time you start the ECS, the `initial.sh` script is automatically executed to initialize the firewall configuration.

**Case 3**

This case illustrates how to use the file injection function to activate user root permission to log in to an ECS. After injecting the file, you can log in to the ECS as user root using SSH key authentication.

The content of the script file to be injected is as follows:

```bash
#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
```

### 3.5 Creating an Image

You can create a private image using an existing ECS. This image contains an OS, preinstalled public applications, and the user's private applications and is available only to the user who created it.

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. Stop the ECS.
   - If the target ECS is running, click **More** in the **Operation** column and select **Stop**.
5. Locate the row that contains the ECS, click **More** in the **Operation** column, and select **Create Image**.
6. Configure image information as prompted.
   - **Source**: ECS
   - ECS: Retain default settings.
   - **Name**: Customize your image name.
7. Click **Submit**.
3.6 Automatically Recovering ECSs

ECSs run on physical hosts. Although there are 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 the ECSs cannot recover through live migration.

The public platform provides automatic recovery to restart ECSs through cold migration, ensuring high availability and top-performing dynamic migration capability of ECSs. You can enable automatic recovery during or after ECS creation. Once a physical host accommodating ECSs breaks down, the ECSs with automatic recovery enabled automatically migrate to a functional host. This minimizes user service interruption. These ECSs will restart in this process.

Notes

- Automatic recovery does not ensure user data consistency.
- An ECS can be automatically recovered only if the host on which it is deployed becomes faulty. This function does not take effect if the fault is caused by the ECS itself.
- Automatic recovery is not a DR or HA mechanism for your applications. You are suggested to follow best practices and take necessary operations to prevent data inconsistency or data loss due to any unexpected activities that may cause application downtime.
- 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

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. Click the name of the target ECS.
   The page providing details about the ECS is displayed.
5. Set Auto Recovery to Enable or Disable.
   Automatic recovery is enabled by default.
   - Once a physical host accommodating ECSs breaks down, the ECSs with automatic recovery enabled automatically migrate to a functional host. This minimizes user service interruption. These ECSs will restart in this process.
   - If Auto Recovery is disabled, you must wait for the system administrator to recover ECSs when hardware becomes faulty.
3.7 Obtaining ECS Console Logs

Scenarios

When an ECS cannot start or run properly, you can download and view ECS console logs for troubleshooting, for example, checking whether the kernel and service configuration are correct.

The ECS console logs record ECS operations, such as ECS starting, stopping, restarting, or forcibly restarting. Through the management console, you can obtain the ECS logs within one hour.

Notes

- The system does not record the logs for forcible ECS stopping.
- The system supports viewing console logs for the ECSs running the following OSs:
  - Red Hat Enterprise Linux 6.x series
  - Red Hat Enterprise Linux 7.x series
  - CentOS 6.x series
  - CentOS 7.x series
  - Ubuntu 14.x series
  - Ubuntu 16.x series
  -! SUSE 11.x series
  - SUSE 12.x series
  - OpenSUSE 13.x series
  - OpenSUSE 42.x series
  -! Debine 16.x series
  -! Fedora series
  -! Freebsd series
  -! CoreOS series
- The ECSs running Windows do not support console logs.
- The system can save up to 100 KB log files.

Procedure

**Step 1** Log in to the ECS.

**Step 2** Check and modify the grub file.

Configuration methods for different OSs vary.

- For CentOS 6 and Red Hat 6, perform the following steps:
  a. Run the following command to open the configuration file:
     ```
     vi /boot/grub/menu.lst
     ```
  b. Locate the row that contains `linux`, `linux16`, or `kernel` (depending on the system), add `console=ttyS0` to its end, and delete parameter `rhgb quiet`. If `console=ttyS0` already exists, you do not need to add it. Save the change and exit.

- For CentOS 7, Red Hat 7, and Ubuntu 14, perform the following steps:
a. Run the following command to open the configuration file:
   ```bash
   vi /boot/grub2/grub.cfg
   ```
b. Locate the row that contains `linux`, `linux16`, or `kernel` (depending on the system), add `console=ttys0` to its end, and delete parameter `rhgb quiet`. If `console=ttys0` already exists, you do not need to add it. Save the change and exit.

- For SUSE Linux 11, perform the following steps:
  a. Run the following command to open the configuration file:
     ```bash
     vi /boot/grub/menu.lst
     ```
b. Locate the row that contains `linux`, `linux16`, or `kernel` (depending on the system) and add `console=ttys0` to its end. If `console=ttys0` already exists, you do not need to add it. Save the change and exit.

- For SUSE Linux 12, openSUSE 13, and openSUSE 42, perform the following steps:
  a. Run the following command to open the configuration file:
     ```bash
     vi /boot/grub2/grub.cfg
     ```
b. Locate the row that contains `linux`, `linux16`, or `kernel` (depending on the system) and add `console=ttys0` to its end. If `console=ttys0` already exists, you do not need to add it. Save the change and exit.

- For Debian and Ubuntu 16, perform the following steps:
  a. Run the following command to open the configuration file:
     ```bash
     vi /boot/grub/grub.cfg
     ```
b. Locate the row that contains `linux`, `linux16`, or `kernel` (depending on the system) and add `console=ttys0` to its end. If `console=ttys0` already exists, you do not need to add it. Save the change and exit.

- For Fedora, perform the following steps:
  a. Run the following command to open the configuration file:
     ```bash
     vi /boot/grub2/grub.cfg
     ```
b. Locate the row that contains `linux`, `linux16`, or `kernel` (depending on the system) and add `console=ttys0` to its end. If `console=ttys0` already exists, you do not need to add it. Save the change and exit.

- For FreeBSD, perform the following steps:
  a. Run the following command to open the configuration file:
     ```bash
     vi /boot/loader.conf
     ```
b. Add `console="comconsole"`. If `console="comconsole"` already exists, you do not need to add it. Save the change and exit.

- For CoreOS, perform the following steps:
  a. Run the following command to check whether `ttyS0` has been configured:
     ```bash
     cat /proc/cmdline | grep ttyS0
     ```
    - If yes, `ttyS0` has been configured.
    - If no, `ttyS0` has not been configured. Go to step 2.
  b. Run the following command to open the configuration file to be edited:
     ```bash
     vi /usr/share/oem/grub.cfg
     ```

**NOTE**

If the `/usr/share/oem/grub.cfg` configuration file does not exist, manually create the file.

- Add `set linux_append="console=ttys0"`. If `set linux_append="console=ttys0"` already exists, you do not need to add it. Save the change and exit.
**NOTE**
To prevent impact on the start of the recovery mode, you are advised to modify only the item used for the default start.

**Step 3** Click **Restart** to restart the ECS.

**Step 4** Obtain ECS console logs.
1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Elastic Cloud Server**.
4. On the **Elastic Cloud Server** page, click the name of the target ECS.
5. On the page providing details about the ECS, click the **Console Logs** tab.
6. Choose the number of lines to be displayed for a log from the **Displayed Lines** drop-down list.
7. Click **Query**.
   View details of the displayed log.

**NOTE**
After you click **Query**, the system will not automatically update the displayed log. To view the latest log, click **Query** again.
8. (Optional) Click **Download** to download the information of the displayed log.
Downloaded log files are in .txt format.

---End

### 3.8 Backing Up ECS Data

**Scenarios**

ECS data can be backed up using Cloud Server Backup Service or Volume Backup Service.

- **CSBS** (recommended): Use this backup method if you want to back up the data of all EVS disks on an ECS, including the system disk and data disks. This prevents data inconsistency caused by time difference in creating a backup.
- **VBS**: Use this backup method if you want to back up the data of one or more EVS disks (system disk or data disk) on an ECS. This minimizes backup costs on the basis of data security.

For Windows ECSs, you can install the Windows Server Backup tool provided by the Windows OS to back up full ECS data. You are advised to use VBS and CSBS provided by the public cloud.

**CSBS Backup 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.
4. In the navigation pane one the left, choose **Cloud Server Backup Service**.
5. Click Create CSBS Backup.
6. Back up the ECS data as prompted.
   For more information, see Cloud Server Backup Service User Guide.

VBS Backup Procedure
1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
   The Elastic Cloud Server page is displayed.
4. In the navigation pane on the left, choose Volume Backup Service.
5. Click Create VBS Backup.
6. Back up data as prompted.
   For more information, see Volume Backup Service User Guide.

3.9 (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.
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 the ECS.
2. Run the following command to view the ECS hostname:
   sudo hostname
   For example, the obtained hostnames are as follows:
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:
   ```bash
   sudo su -
   ```
3. Run the following command to edit the hosts configuration file:
   ```bash
   vi /etc/hosts
   ```
4. Press i to enter editing mode.
5. Add the statement in the following format to set up the mapping:
   ```plaintext
   Private IP address hostname
   ```
   For example, add the following statement:
   ```plaintext
   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:
   ```bash
   :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:

```bash
ping hostname
```

---End

3.10 Quotas

Scenarios

Resource quotas are defined on the platform for each service to prevent resource exhaustion. The maximum number of ECSs that can be created varies depending on the flavor. You can apply for increasing quotas if necessary.

This section describes how to view the usage of each type of ECS resource and the total quotas in a specified region.

Procedure

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 ECS resource.
   If a quota cannot meet service requirements, click Increase Quota to adjust it.
4 ECS Logins

4.1 Logging In to a Windows ECS

4.1.1 Login Overview

Only a running ECS can be logged in.

A Windows ECS can be logged in using either VNC or MSTSC.

- Login using VNC
  If no EIP is bound to an ECS, you can remotely log in to the ECS on the management console.

- Login using MSTSC
  This option applies only to ECSs running Windows. You can run the `mstsc` command on a local computer to log in to an ECS. Ensure that the ECS has an EIP bound.

4.1.2 Login Using VNC

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

Restrictions and Limitations

- The remote login function is implemented using customized ports. Therefore, before attempting to log in remotely, ensure that the port to be used is not blocked by the firewall. For example, if the remote login link is `xxx:8002`, ensure that port 8002 is not blocked by the firewall.

- If the client OS uses a local proxy and the firewall port cannot be configured on the local proxy, disable the proxy mode and then try logging in remotely.

Procedure

1. Log in to the management console.
3. Obtain the password for logging in to the ECS.

Before logging in to the ECS, you must have the login password.

For instructions about how to obtain the password for logging in to a Windows ECS, see section 5.4 Obtaining the Password for Logging In to a Windows ECS.
4. In the search box above the upper right corner of the ECS list, enter the ECS name, IP address, or ID, and click .

5. Locate the row containing the ECS and click Remote Login in the Operation column.

6. (Optional) If the system displays "Press CTRL+ALT+DELETE to log on", click Send CtrlAltDel in the upper right corner of the remote login page to log in to the ECS.

**Figure 4-1** Click Send CtrlAltDel.

![Send CtrlAltDel](image.png)

7. Enter the ECS password as prompted.

**4.1.3 Login Using an MSTSC Password**

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

**Prerequisites**

- You have obtained the password for logging in to the Windows ECS. For details, see section 5.4 Obtaining the Password for Logging In to a Windows ECS.
- You have bound an EIP to the ECS. For details, see section 3.1.3 Viewing ECS Details.
- You have configured the inbound rules of the security group. For details, see section 9.2 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.

**Procedure**

Remote Desktop Protocol (RDP) is disabled on Windows ECSs by default. Before using MSTSC to log in to a Windows ECS for the first time, use VNC to log in to it and enable RDP.

**Step 1** Check whether RDP is enabled on the Windows ECS.

1. Log in to the Windows ECS using VNC.
   For details, see section 4.1.2 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.
3. Click the **Remote** tab and select **Allow connections from computers running any version of Remote Desktop (less secure)**.

4. Click **OK**.

**Step 2** On your local computer, use MSTSC to log in to the Windows ECS.

1. Click **Start** in the task bar.
2. In the **Search programs and files** box, enter **mstsc**.
3. Log in to the ECS according to the prompts.
   To ensure system security, change the login password after you log in to the ECS for the first time.

**Step 3** (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.

Perform this step only when you need to use RDP clipboard. This issue occurs due to Windows OS limitations. For details about the handling method, see https://support.microsoft.com/en-us/help/2258090/copying-files-larger-than-2-gb-over-a-remote-desktop-services-or-terminal-services-session-by-using-clipboard-redirection-copy-and-paste-fails-silently.

----End
4.2 Logging In to a Linux ECS

4.2.1 Login Overview

Only a running ECS can be logged in.

A Linux ECS can be logged in using either VNC or SSH.

- Logging in to an ECS using VNC
  If no EIP is bound to an ECS, you can remotely log in to the ECS on the management console.

- Logging in to an ECS using SSH
  This method applies only to Linux ECSs. You can use a remote login tool, such as PuTTY, to log in to the ECS. Ensure that the ECS has an EIP bound.

NOTE
Both an SSH key and an SSH password can be used for logins.

4.2.2 Login Using an SSH Key

Prerequisites

- You have obtained the private key file used during ECS creation.
- You have bound an EIP to the ECS. For details, see section 3.1.3 Viewing ECS Details.
- You have configured the inbound rules of the security group. For details, see section 9.2 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 a Windows Computer

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

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

The following procedure uses 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:
   http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

NOTE
PuTTYgen is a private 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 area, 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**
- If a public image is used, the username of the image is **root** in the Mexico region and **linux** in other regions.
- If you have activated user **root** permission using user data injection or file injection during ECS creation, you can log in to the ECS as user **root**. In such a case, enter **root** in **Auto-login username**.

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 4-3** 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:

```bash
ssh root@192.168.0.1
```

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

**Figure 4-4 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 a Linux Computer**

To log in to the Linux ECS from a Linux computer, perform the operations described in this section. The following procedure uses 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:
   ```bash
   chmod 400 /path/kp-123
   ```
   
   **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:
   ```bash
   ssh -i /path/kp-123 Default username@EIP
   ```
   For example, if the default username is `linux`, run the following command:
   ```bash
   ssh -i /path/kp-123 linux@EIP
   ```
   
   **NOTE**
   In the preceding command:
   
   - `path` is the path where the key file is saved.
   - `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 or the password through SSH.
- After logging in to an ECS as a common user, you can run the following command to switch to user root without entering a password:
  ```bash
  sudo su -
  ```
- After switching to user root, you can run the following command to change user root password:
  ```bash
  sudo passwd root
  ```

4.2.3 Login Using an SSH Password

Logging in to a Linux ECS using SSH password authentication is disabled by default. If you require password authentication, configure it after logging in to the ECS. To ensure system security, reset the common user password for logging in to the Linux ECS after configuring SSH password authentication.

Prerequisites

- You have bound an EIP to the ECS. For details, see section 3.1.3 Viewing ECS Details.
- You have configured the inbound rules of the security group. For details, see section 9.2 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.
- You have obtained the SSH login permission and reset the common user password for logging in to the Linux ECS. For details, see section Configuring the Login Permission Using SSH Password Authentication.

Configuring the Login Permission Using SSH Password Authentication

Assigning the remote login permission using SSH key authentication

1. Use the SSH key to log in to the Linux ECS. For details, see section 4.2.2 Login Using an SSH Key.
2. Run the following command to change the value of PasswordAuthentication in /etc/ssh/sshd_config to yes:
   ```bash
   sudo vi /etc/ssh/sshd_config
   ```
   **NOTE**
   For the ECSs running the SUSE or openSUSE OSs, ensure that the values of PasswordAuthentication, ChallengeResponseAuthentication, and UsePAM in /etc/ssh/sshd_config are all yes.
3. Run the following command to change the ssh_pwauth value to 1 or true in /etc/cloud/cloud.cfg:
   ```bash
   sudo vi /etc/cloud/cloud.cfg
   ```
4. Run the following command to reload the sshd service:
   ```bash
   sudo service sshd reload
   ```

To ensure system security, reset the common user password for logging in to the Linux ECS.

1. Run the following command to reset the ECS password:
   If the ECS username is linux, run the following command:
Elastic Cloud Server
User Guide

4 ECS Logins

To remotely log in to an ECS as user root, perform the following operations:

1. Run the following command to change the disable_root value to 0 or false and the ssh_pauth value to 1 or true in /etc/cloud/cloud.cfg:
   
   ```
   sudo vi /etc/cloud/cloud.cfg
   ```

2. Run the following command to set the user root password:
   
   ```
   sudo passwd root
   ```

3. Enter the new password as prompted and press Enter.

4. Confirm the password and press Enter.

5. Verify that the information displayed is similar to the following, indicating that the password has been reset:

   ```
   passwd: all authentication tokens updated successfully.
   ```

**Login Operations**

- **Windows**
  
  To log in to the Linux ECS from a Windows computer, perform the operations described in this section.

  The following procedure uses PuTTY as an example to log in to the ECS.

  a. Run PuTTY.

  b. Choose Session and enter the EIP of the ECS under Host Name (or IP address).

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

  d. Click Open.

  e. Enter username and the password you set during ECS creation.

- **Linux**

  To log in to the Linux ECS from a Linux computer, run the following command:

  ```
  ssh EIP bound to the ECS
  ```

**4.2.4 Login Using VNC**

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

For details about how to copy and paste data on VNC pages after the ECS login, see section Follow-up Procedure.

**Restrictions and Limitations**

- The remote login function is implemented using customized ports. Therefore, before attempting to log in remotely, ensure that the port to be used is not blocked by the firewall. For example, if the remote login link is xxx:8002, ensure that port 8002 is not blocked by the firewall.

- If the client OS uses a local proxy and the firewall port cannot be configured on the local proxy, disable the proxy mode and then try logging in remotely.

**Logging in to the ECS**

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, and click .
4. Locate the row containing the ECS and click **Remote Login** in the **Operation** column.
5. (Optional) If the system displays "Press CTRL+ALT+DELETE to log on", click **Send CtrlAltDel** in the upper right corner of the remote login page to log in to the ECS.

**Figure 4-5 Click Send CtrlAltDel.**

![Send CtrlAltDel](image)

6. Enter the ECS password as prompted.

**Follow-up Procedure**

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

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

**Figure 4-6 Input Commands**

![Input Commands](image)
3. Press **Ctrl+C** to copy data from the local computer.
4. Press **Ctrl+V** to paste the local data to the Copy Commands window.
5. 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.
5 Passwords and Key Pairs

5.1 Changing the Initial Password for Logging In to an ECS

Scenarios

After logging in an ECS for the first time, you are suggested to change the initial password. This section describes how to change the password for logging in to an ECS.

Prerequisites

The ECS can be logged in. If not, see section 5.2.1 Application Scenarios for troubleshooting.

Background

Table 5-1 shows the ECS password complexity requirements.

Table 5-1 Password complexity requirements

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>• Consists of 8 characters to 26 characters.&lt;br&gt;• Contains at least three of the following character types:&lt;br&gt;  - Uppercase letters&lt;br&gt;  - Lowercase letters&lt;br&gt;  - Numerals&lt;br&gt;  - Special characters: $!@%^_=-+[]:;^{}?&lt;br&gt;• Cannot contain the username or the username in reverse.&lt;br&gt;• Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)</td>
<td>Test12!@</td>
</tr>
</tbody>
</table>
Windows

1. Log in to the Windows ECS remotely. For details, see section 4.1.1 Login Overview.
2. Press Win+R to start the Open dialog box.
3. Enter cmd to open the command-line interface (CLI) window.
4. Run the following command to change the password (the new password must meet the requirements described in Table 5-2):
   ```
   net user Administrator New password
   ```

Linux

1. Use the existing key file to log in to the Linux ECS as user root through SSH. For more details, see section 4.2.2 Login Using an SSH Key.
2. Run the following command to reset the password of user root:
   ```
   passwd
   ```
   To reset the passwords of other users, replace passwd with passwd username.
3. Enter the new password as prompted. Ensure that the new password meets the requirements described in Table 5-2.
   ```
   New password:
   Retype new password:
   ```
   If the following information is displayed, the password has been changed:
   ```
   passwd: password updated successfully
   ```

5.2 Resetting the Password for Logging In to an ECS

5.2.1 Application Scenarios

Reset the password for logging in to an ECS if:

- The password is lost.
- The password has expired.

Background

Table 5-2 shows the ECS password complexity requirements.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
<th>Example Value</th>
</tr>
</thead>
</table>
| Password  | - Consists of 8 characters to 26 characters.  
            - Contains at least three of the following character types:  
              - Uppercase letters  
              - Lowercase letters  | Test12!@ |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Numerals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Special characters:</td>
<td>$!@%-_=+[^./^,{}?</td>
</tr>
<tr>
<td></td>
<td>• Cannot contain the username or the username in reverse.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)</td>
<td></td>
</tr>
</tbody>
</table>

### 5.2.2 Resetting the Password for Logging In to a Windows ECS

#### 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:
    ```bash
    sudo apt-get install ntfs-3g chntpw
    ```
  - **Method 2:**
    Download the desired **ntfs-3g** and **chntpw** software packages according to the temporary ECS OS. For detailed installation and use guide, see the [NTFS official website](https://www.tuxera.com/community/open-source-ntfs-3g/) and [chntpw official website](https://pkgs.org/download/chntpw).
    
    Log in at **www.tuxera.com/community/open-source-ntfs-3g/** to obtain the **ntfs-3g** software package.
    
    Log in at **https://pkgs.org/download/chntpw** to obtain the **chntpw** software package.

#### Procedure

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

   **NOTE**
   Do not forcibly stop the Windows ECS. Otherwise, password reset may fail.
   
   e. Locate the row containing the system disk and click **Detach** to detach the system disk from the ECS.
f. On the page providing details about the temporary ECS, click the Disks tab.

g. Click Attach Disk. In the displayed dialog box, select the system disk detached in step 1.e and attach it to the temporary ECS.

2. Log in to the temporary ECS remotely and attach the system disk.
   a. Run the following command to view the directory of the system disk detached from the original Windows ECS now attached to the temporary ECS:
      ```
      fdisk -l
      ```
   b. Run the following command to mount the file system of the detached system disk to the temporary ECS:
      ```
      mount -t ntfs-3g /dev/Result obtained in step 2.a /mnt/
      ```
      For example, if the query result obtained in step 2.a is xvde2, run the following command:
      ```
      mount -t ntfs-3g /dev/xvde2 /mnt/
      ```

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!

      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 5-2):
      ```
      net user Administrator New password
      ```
5.2.3 Resetting the Password for Logging In to a Linux ECS

Prerequisites

- A temporary Linux ECS which locates in the same AZ as the target ECS is available.
- You have bound an EIP to the temporary ECS.

Procedure

1. Download the script for resetting the password and upload the script to the temporary ECS.
   a. Log in to the management console and click Elastic Cloud Server under Computing.
   b. Click in the upper left corner and select the desired region and project.
   c. Locate the row containing the target ECS, click More in the Operation column, and select Reset Password. Then, download the password reset script as prompted.
   d. Use a connection tool, such as WinSCP, to upload the obtained changepasswd.sh script to the temporary ECS.

   To download WinSCP, log in at http://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.

   b. Locate the row containing the system disk to be detached and click Detach to detach the system disk from the ECS.
   c. On the page providing details about the temporary ECS, click the Disks tab.
   d. Click Attach Disk. In the displayed dialog box, select the system disk detached in step 2.b and attach it to the temporary ECS.

3. Log in to the temporary ECS remotely and reset the password.
   a. Locate the row containing the temporary ECS and click Remote Login in the Operation column.
   b. Run the following command to view the directory of the system disk detached from the original Linux ECS now attached to the temporary ECS:

   fdisk -l

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

   chmod +x changepasswd.sh

   ./changepasswd.sh

   When you run the password reset script, if the system displays a message indicating that there is no command related to logical volume manager (LVM), such as the message "no lvs command", install an LVM tool on the temporary ECS. The LVM2 tool is recommended, which can be installed by running the **yum install lvm2** command.
If the original ECS and the temporary ECS both run CentOS 7, a mount failure may occur during script execution. To resolve this issue, replace `mount $dev $mountPath` with `mount -o nouuid $dev $mountPath` in the script.

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:

```bash
set password success.
```

4. Stop the temporary ECS, detach the system disk, attach the system disk to the original Linux ECS, and restart the original Linux ECS.

a. Stop the temporary ECS, switch to the page providing details about the ECS, and click the **Disks** tab.

b. Click **Detach** to detach the data disk attached in step 2.

c. On the page providing details about the original Linux ECS, click the **Disks** tab.

d. Click **Attach Disk**. In the displayed dialog box, select the data disk detached in step 4.b and device name `/dev/sda`.

e. Restart the original Linux ECS.

---

### 5.3 Creating a Key Pair

#### Overview

A key pair that consists of a public key and a private key is required for authentication when you log in to an ECS. Both the public and private keys are used for authentication. 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. You can use either of the following methods:
  
  - Create a key pair using 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 section Creating a Key Pair Using 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 section Creating a Key Pair Using puttygen.exe.

- **Using an existing key pair**

  If a key pair is available locally, choose **Key Pair** in the navigation pane and click Import Key Pair and Select File on the right side of the page to import the key pair to the system. For details, see section Importing a Key Pair.

#### Constraints

- ECSs support the following encryption algorithms:
Passwords and Key Pairs

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 Using the Management Console

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
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.
7. Click OK.
8. In the displayed dialog box, click OK.

You can view and save the private key according to the prompts. To ensure ECS security, you are limited to downloading the private key only once.

Creating a Key Pair Using puttygen.exe

Step 1 Obtain the public and private keys.

1. Double-click puttygen.exe. The PuTTY Key Generator page is displayed.
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 5-2.
Figure 5-2 Obtaining the public and private keys

Step 2  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 3  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.
  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.
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.

b. Save the private key, for example, kp-123.pem, in a local directory.

Step 4 Import the public key to the system. For details, see section "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. To resolve this issue, obtain the public key content in correct format and import the content to the management console. For details, see section 14.10 What Should I Do If a Key Pair Created Using puttygen.exe 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.
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, click Select File and select the locally stored public key.
   - 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.

When importing a key pair, ensure that the public key is imported. Otherwise, importing the key pair will fail.

   i. 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.

**Related Links**

- 14.5 What Should I Do If a Key Pair Cannot Be Imported?
- 14.10 What Should I Do If a Key Pair Created Using puttygen.exe Cannot Be Imported to the Management Console?
5.4 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 using the management console or APIs. For details, see this section.

Obtaining the Password Using 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.
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 Using 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 section "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 section "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 private key file
to edit the code decryption ciphertext.

5.5 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.
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.
6 Configuration Modifications

6.1 Modifying ECS vCPU and Memory Specifications

6.1.1 General Operations for Modifying Specifications

Scenarios

If the 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.

- Before changing a XEN ECS to a KVM ECS, manually install the required driver on the ECS. Otherwise, the ECS will be unavailable after the modification is performed. For example, starting the OS will fail.
  
  For details, see sections 6.1.2 Changing a XEN ECS to a KVM ECS (Windows) and 6.1.3 Changing a XEN ECS to a KVM ECS (Linux).

- For instructions about how to modify the specifications of other ECSs, see this section.

- To obtain the virtualization type of an ECS, perform the following operations:
  1. Check the specifications tables in section 1.7 Instance Family for the virtualization type.

- Before changing XEN to KVM, make sure that the ECS has been correctly configured. Otherwise, the ECS will be unavailable after the modification is performed.

Notes

- 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 section "Notes" in 1.7.1 ECS Types.

Step 1: Modify Specifications

The following section provides only general operations for modifying specifications. For instructions about how to change a XEN ECS to a KVM ECS, see section 6.1.2 Changing a XEN ECS to a KVM ECS (Windows) or 6.1.3 Changing a XEN ECS to a KVM ECS (Linux).

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. On the Elastic Cloud Server page, 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. (Optional) Set DeH.
   If the ECS is created on a DeH, the system allows you to change the DeH.
   To do so, select the target DeH from the drop-down list. If no DeH is available in the drop-down list, remaining DeH resources are insufficient and cannot be used to create the ECS with specifications modified.
8. (Optional) Select the check box to confirm the ECS configuration.
   If a XEN ECS is changed to a KVM ECS, manually configure the ECS based on the instructions provided in section 6.1.2 Changing a XEN ECS to a KVM ECS (Windows) or 6.1.3 Changing a XEN ECS to a KVM ECS (Linux).
9. Click OK.
10. On the Modify ECS Specifications page, confirm the modified vCPU and memory specifications, select I have read and agreed to the agreement, and click Submit.
11. 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 section 3.1.2 Viewing Failures.
      ■ If yes, go to step 11.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 section 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
  a. Check whether the number of disks displayed on the Computer page after specifications modification is the same as that before specifications modifications.
     ■ 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 b.

An example is provided as follows:
An ECS running Windows Server 2008 has one system disk and two data disks attached before specifications modifications.
After the specifications are modified, check disk attachment.

**Figure 6-2** Disk attachment after specifications modification

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

b. Set the affected disks to be online.
   
i. 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.
ii. In the navigation pane on the left, choose Storage > Disk Management. The Disk Management page is displayed.

iii. 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 6-3 Making the disk online

c. On the Computer page, check whether the number of disks is the same as that before the specifications modification.

- If yes, no further action is required.
- If no, contact customer service.
Figure 6-4 Disk attachment after disk online

Figure 6-5 Viewing disks attached before specifications modification

As shown in Figure 6-5, the ECS has three disks attached: /dev/vda, /dev/vdb, and /dev/vdc.

c. Run the following command to view disks attached after specifications modification:
   \texttt{df -h | grep '/dev/'}

Figure 6-6 Viewing disks attached after specifications modification

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

d. Check whether the number of disks obtained in \textit{b} is the same as that obtained in \textit{c}.
   \begin{itemize}
   \item If yes, the specifications have been modified. No further action is required.
   \end{itemize}
If no, the disk attachment failed. In such a case, go to e.

e. Run the **mount** command to attach the affected disks.

An example is provided as follows:

```
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.

f. 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 yes, no further action is required.
- If no, contact customer service.

---

**Figure 6-7 Checking the number of disks attached**

As shown in **Figure 6-7**, the numbers of disks before and after specifications modification are the same. The disks are `/dev/vda`, `/dev/vdb`, and `/dev/vdc`.

---

**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 technical support.
6.1.2 Changing a XEN ECS to a KVM ECS (Windows)

Scenarios

A Windows ECS can be switched from XEN to KVM only if XEN guest OS driver (PV driver) and KVM guest OS driver (UVP VMTools) run on the ECS. Before changing a XEN ECS to a KVM ECS, ensure that PV driver and UVP VMTools have been installed on the ECS.

This section describes how to configure a Windows ECS for changing XEN to KVM.

NOTE
After configuring the ECS, contact customer service to modify the ECS specifications.

Constraints

- A XEN ECS with more than 24 VBD disks attached cannot be changed to a KVM ECS.
- A XEN ECS can be changed to a KVM ECS, but a KVM ECS cannot be changed to a XEN ECS.
- General-purpose ECSs and memory-optimized ECSs can be exchanged (only from XEN to KVM if the virtualization type is changed), as shown in Table 6-1.

Table 6-1 ECS types supporting change from XEN to KVM

<table>
<thead>
<tr>
<th></th>
<th>S2</th>
<th>S3</th>
<th>C3</th>
<th>M2</th>
<th>M3</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>C1</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>C2</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>M1</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>H1</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

For example, an S1 ECS can be changed to an S2, S3, C3, M2, or M3 ECS.

Procedure

Figure 6-8 shows the flowchart for changing a XEN ECS to a KVM ECS.
Table 6-2 describes the operations.

**Table 6-2 Procedure for changing a XEN ECS to a KVM ECS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(Optional) Backing Up the System Disk</td>
</tr>
<tr>
<td>2</td>
<td>Configuring the ECS</td>
</tr>
<tr>
<td>3</td>
<td>Verifying the ECS Configuration</td>
</tr>
<tr>
<td>4</td>
<td>Modifying Specifications</td>
</tr>
<tr>
<td>5</td>
<td>Checking Disk Attachment</td>
</tr>
</tbody>
</table>

**(Optional) Backing Up the System Disk**

Before modifying the specifications, back up the system disk and install the driver on the ECS. Otherwise, the ECS will be unavailable after the modification is performed. If the ECS becomes unavailable, the fault can be rectified by reinstalling the OS, which may cause data loss in your system disk.
For instructions about how to back up the system disk, see section “Getting Started > Creating a VBS Backup” in Volume Backup Service User Guide.

Configuring the ECS

1. Log in to the ECS as the administrator.
2. Download the PV driver and UVP VMTools installation packages.
   - To download the installation package for the PV driver, log in at https://ecs-instance-driver.obs.myhwclouds.com/pvdriver-windows.zip.
   - To download the installation package for the UVP VMTools, log in at https://ecs-instance-driver.obs.myhwclouds.com/vmtools-windows.zip.
3. Install the latest PV driver.
   Run Setup.exe and install the PV driver as prompted.
4. Install UVP VMTools.
   Run Setup.exe and install the UVP VMTools as prompted.

Verifying the ECS Configuration

Perform the following operations to check whether the drivers have been installed on the ECS:

1. Log in to the ECS.
2. Check whether the PV driver of 2.3 or a later version has been installed.
   Switch to the C:\Program Files (x86)\Xen PV Drivers\bin directory, open the version.ini file, and view the PV driver version.

```
 pvdriverVersion=5.0.104.010
```
   - If the directory is available and the driver version is 2.3 or later, the PV driver has been installed.
   - If the directory is unavailable or the driver version is earlier than 2.3, installing the PV driver failed. In such a case, reinstall the PV driver by following the operations provided in Configuring the ECS.
3. Check whether the UVP VMTools of 2.3 or a later version has been installed.
   Switch to the C:\Program Files (x86)\virtio\bin directory, open the version.ini file, and view the UVP VMTools version.

```
cur_vmtools_ver=2.5.0.105org_vmtools_ver=0cur_daemon_ver=2.5.0.105-010cur_drivers_ver=2.5.0.105-010
```
   - If the directory is available and the driver version is 2.3 or later, the UVP VMTools has been installed.
   - If the directory is unavailable or the driver version is earlier than 2.3, installing the UVP VMTools failed. In such a case, reinstall the UVP VMTools by following the operations provided in Configuring the ECS.

**NOTICE**

Ensure that the ECS is configured successfully. Otherwise, the ECS will be unavailable after the modification is performed.
Modifying Specifications
After configuring the ECS, contact customer service to modify the ECS specifications.

Checking Disk Attachment

After a XEN ECS is changed to a KVM ECS, disk attachment may fail. Therefore, check disk attachment after specifications modification. If disks are properly attached, the specifications modification is successful.

1. Check whether the number of disks displayed on the Computer page after specifications modification is the same as that before specifications modifications.
   - 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 2.

An example is provided as follows:
An ECS running Windows Server 2008 has one system disk and two data disks attached before specifications modifications.

Figure 6-9 Disk attachment before specifications modification

![Disk attachment before specifications modification](image)

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

2. Set the affected disks to be online.
   a. Click Start in the task bar. In the displayed Start menu, right-click Computer and choose Manage from the shortcut menu. The Server Manager page is displayed.
   b. In the navigation pane on the left, choose Storage > Disk Management. The Disk Management page is displayed.
   c. In the left pane, the disk list is displayed. Right-click the affected disk and choose Online from the shortcut menu to make it online.
3. On the **Computer** page, check whether the number of disks is the same as that before the specifications modification.
   - If yes, no further action is required.
   - If no, contact customer service.

**Figure 6-12** Disk attachment after disk online
Follow-up Procedure

If the ECS with specifications modified is displayed in the ECS list but its OS cannot be started after the ECS is remotely logged in, reinstall the ECS OS to rectify this fault. For details, see section 3.2.1 Reinstalling the OS.

6.1.3 Changing a XEN ECS to a KVM ECS (Linux)

Scenarios

A Linux ECS can be switched from XEN to KVM if xen-pv and virtio drivers run on the ECS. Before changing a XEN ECS to a KVM ECS, ensure that the required drivers have been installed and the UUID has been configured on the ECS.

This section describes how to manually configure a Linux ECS for changing XEN to KVM.

**NOTE**

After configuring the ECS, contact customer service to modify the ECS specifications.

Constraints

- A XEN ECS with more than 24 VBD disks attached cannot be changed to a KVM ECS.
- A XEN ECS can be changed to a KVM ECS, but a KVM ECS cannot be changed to a XEN ECS.
- General-purpose ECSs and memory-optimized ECSs can be exchanged (only from XEN to KVM if the virtualization type is changed), as shown in Table 6-3.

Table 6-3 ECS types supporting change from XEN to KVM

<table>
<thead>
<tr>
<th></th>
<th>S2</th>
<th>S3</th>
<th>C3</th>
<th>M2</th>
<th>M3</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>C1</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>C2</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>M1</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>H1</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

For example, an S1 ECS can be changed to an S2, S3, C3, M2, or M3 ECS.

Procedure

Figure 6-13 shows the flowchart for changing a XEN ECS to a KVM ECS.
In the preceding figure:

1: indicates that the ECS is automatically configured using a script. The OSs supporting automatic script operations are as follows:

- Ubuntu 14.04
- Ubuntu 16.04
- CentOS 6.7
- CentOS 6.8
- CentOS 7.1
- CentOS 7.2
- CentOS 7.3
- CentOS 7.4

Table 6-4 describes the operations for these OSs.

**Table 6-4** Procedure for changing a XEN ECS to a KVM ECS using a script

<table>
<thead>
<tr>
<th>Step</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(Optional) Backing Up the System Disk</td>
</tr>
<tr>
<td>2</td>
<td>Automatically Configuring the ECS Using a Script</td>
</tr>
<tr>
<td>3</td>
<td>Modifying Specifications</td>
</tr>
<tr>
<td>4</td>
<td>Checking Disk Attachment</td>
</tr>
</tbody>
</table>

2: indicates that the ECS is manually configured. If your ECS does not support the configuration using a script, manually configure the ECS. Table 6-5 describes the operations.

**Table 6-5** Procedure for manually changing a XEN ECS to a KVM ECS

<table>
<thead>
<tr>
<th>Step</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(Optional) Backing Up the System Disk</td>
</tr>
<tr>
<td>2</td>
<td>Manually Configuring the ECS</td>
</tr>
<tr>
<td>3</td>
<td>(Optional) Verifying the ECS Configuration</td>
</tr>
<tr>
<td>4</td>
<td>Modifying Specifications</td>
</tr>
<tr>
<td>5</td>
<td>Checking Disk Attachment</td>
</tr>
</tbody>
</table>
(Optional) Backing Up the System Disk

Before modifying the specifications, back up the system disk and install the driver on the ECS. Otherwise, the ECS will be unavailable after the modification is performed. If the ECS becomes unavailable, the fault can be rectified by reinstalling the OS, which may cause data loss in your system disk.

For instructions about how to back up the system disk, see section "Getting Started > Creating a VBS Backup" in Volume Backup Service User Guide.

Automatically Configuring the ECS Using a Script

Perform the operations described in this section if your ECS supports the configuration using a script. If your ECS does not support this mode, manually configure it. For details, see Manually Configuring the ECS.

![NOTE]
For details about the ECSs supporting the configuration using a script, see Procedure.

1. Log in to the ECS.
2. Run the following command to download the driver installation script to the /home directory:

   ```bash
curl URL > /home/resize_ecs_modify_linux.sh
   ```

   In the preceding command, URL is the address for downloading the specifications modification script.

   URL: https://obs.telefonicaopencloud.com/drivers/resize_ecs_modify_linux.sh

3. Run the following command to execute the script which automatically checks and installs the native XEN PV driver and virtio driver:

   ```bash
   bash resize_ecs_modify_linux.sh
   ```

   ![Figure 6-14 Executing the script]

4. Wait until the script execution is complete. If the message "{Image name} already contain xen and virtio driver" is displayed, the driver has been installed.

   Contact customer service to modify specifications. For details, see section Modifying Specifications.
Ensure that the ECS is configured successfully. Otherwise, the ECS will be unavailable after the modification is performed.

**Manually Configuring the ECS**

Perform the operations described in this section if your ECS does not support the configuration using a script.

1. Log in to the ECS.
2. Uninstall Tools from the ECS.
   For details, see section [Uninstalling Tools from a Linux ECS](#).
3. Change the GRUB disk ID to UUID.
   For details, see section [Changing the Disk Identifier of the GRUB Configuration File to UUID](#).
4. Change the fstab disk ID to UUID.
   For details, see section [Changing the Disk Identifier of the fstab File to UUID](#).
5. Install native XEN and KVM drivers.
   For details, see section [Installing Native XEN and KVM Drivers](#).

**(Optional) Verifying the ECS Configuration**

Perform the following operations to check whether the configuration files have been modified and the drivers have been installed:

1. Log in to the ECS.
2. Run the following command to check whether the root partition is in UUID format:
   ```
cat /boot/grub/grub.cfg
   ```
   - If yes, the disk ID in the GRUB configuration file has been changed to UUID.
   - If no, the modification failed. In such a case, change the GRUB disk ID to UUID again.
NOTE
The path in which the GRUB configuration file is stored varies depending on the OS. For example, the path can be /boot/grub/menu.lst, /boot/grub/grub.cfg, /boot/gurb2/grub.cfg, or /boot/grub/grub.conf.

3. Run the following command to check whether the disk ID in the fstab configuration file is UUID:
   ```
cat /etc/fstab
```
- If yes, the disk ID has been changed to UUID.
- If no, the modification failed. In such a case, change the fstab disk ID to UUID again.

4. Check whether the native XEN and KVM drivers have been installed.
- If the boot virtual file system is initramfs, run the following commands:
  ```
  lsinitrd /boot/initramfs-`uname -r`.img | grep xen
  lsinitrd /boot/initramfs-`uname -r`.img | grep virtio
  ```
- If the boot virtual file system is initrd, run the following commands:
  ```
  lsinitrd /boot/initrd-`uname -r` | grep xen
  lsinitrd /boot/initrd-`uname -r` | grep virtio
  ```
If the names of the native XEN and KVM drivers are displayed in the command output, the drivers have been installed.

```
Modifying Specifications

After configuring the ECS, contact customer service to modify the ECS specifications.

Checking Disk Attachment

After a XEN ECS is changed to a KVM ECS, disk attachment may fail. Therefore, check disk attachment after specifications modification. If disks are properly attached, the specifications modification is successful.

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

   **Figure 6-16 Viewing disks attached before specifications modification**

   As shown in **Figure 6-16**, 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:
   
   ```bash
   df -h | grep '/dev/
   ```

   **Figure 6-17 Viewing disks attached after specifications modification**

   As shown in **Figure 6-17**, only one disk /dev/vda is attached to the ECS.

4. Check whether the number of disks obtained in 2 is the same as that obtained in 3.
   - If yes, the specifications have been modified. No further action is required.
   - If no, the disk attachment failed. In such a case, go to 5.

5. Run the `mount` command to attach the affected disks.
An example is provided as follows:

```
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 yes, no further action is required.
   - If no, contact customer service.

![Figure 6-18 Checking the number of disks attached](image)

As shown in Figure 6-18, the numbers of disks before and after specifications modification are the same. The disks are `/dev/vda`, `/dev/vdb`, and `/dev/vdc`.

**Follow-up Procedure**

If the ECS with specifications modified is displayed in the ECS list but its OS cannot be started after the ECS is remotely logged in, reinstall the ECS OS to rectify this fault. For details, see section 3.2.1 Reinstalling the OS.

6.2 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:
   ```bash
   su - root
   ```
3. Run the following command to obtain the time zones supported by the ECS:
   ```bash
   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 shown in **Figure 6-19** to obtain your desired time zone file.

   **Figure 6-19** Time zones supported by the ECS
   
   ![Time zones supported by the ECS](image)

   The directory structure shown in **Figure 6-19** 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 Hong Kong, the directory in which the time zone file is stored is `/usr/share/zoneinfo/Hongkong`.
   - 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:
      ```bash
      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 Hong Kong, change the `ZONE` entry value to `Hongkong`:
        ```bash
        ZONE="Hongkong"
        ```
      - If the target time zone is for Paris, change the `ZONE` entry value to `Paris`:
        ```bash
        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/Hongkong /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`

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** is displayed.
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**.
7 Disks

7.1 Attaching a Disk to an ECS

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 section "Creating an EVS Disk" in Elastic Volume Service User Guide.

Procedure

1. Log in to the management console.
3. In the search box above the upper right corner of the ECS list, enter the ECS name, IP address, or ID for searching.
4. Click the name of the target ECS. The page providing details about the ECS is displayed.
5. Click the Disks tab. Then, click Attach Disk. The Attach Disk dialog box is displayed.
6. Select the target disk and set the device name as prompted.

**NOTE**

- If no EVS disks are available, click Create Disk in the lower part of the list.
- For details about restrictions for attaching a disk, see section 15.8.3 What Are the Restrictions for Attaching an EVS Disk to an ECS?

7. 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 section 2.3.1 Scenarios and Disk Partitions.

7.2 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 section External Image File.
- Table 7-1 lists the second part of supported OSs.

**Table 7-1 OSs supporting EVS disk detachment from a running ECS**

<table>
<thead>
<tr>
<th>OS</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS</td>
<td>7.3 64bit</td>
</tr>
<tr>
<td></td>
<td>7.2 64bit</td>
</tr>
<tr>
<td></td>
<td>6.8 64bit</td>
</tr>
<tr>
<td></td>
<td>6.7 64bit</td>
</tr>
<tr>
<td>Debian</td>
<td>8.6.0 64bit</td>
</tr>
<tr>
<td></td>
<td>8.5.0 64bit</td>
</tr>
<tr>
<td>Fedora</td>
<td>25 64bit</td>
</tr>
<tr>
<td></td>
<td>24 64bit</td>
</tr>
<tr>
<td>SUSE</td>
<td>SUSE Linux Enterprise Server 12 SP2 64bit</td>
</tr>
<tr>
<td></td>
<td>SUSE Linux Enterprise Server 12 SP1 64bit</td>
</tr>
<tr>
<td></td>
<td>SUSE Linux Enterprise Server 11 SP4 64bit</td>
</tr>
<tr>
<td></td>
<td>SUSE Linux Enterprise Server 12 64bit</td>
</tr>
<tr>
<td>OpenSUSE</td>
<td>42.2 64bit</td>
</tr>
<tr>
<td></td>
<td>42.1 64bit</td>
</tr>
<tr>
<td>Oracle Linux Server release</td>
<td>7.3 64bit</td>
</tr>
<tr>
<td></td>
<td>7.2 64bit</td>
</tr>
<tr>
<td></td>
<td>6.8 64bit</td>
</tr>
<tr>
<td></td>
<td>6.7 64bit</td>
</tr>
</tbody>
</table>
### 7.3 Expanding the Capacity of an EVS Disk

When the storage space of an EVS disk is insufficient, you can handle the insufficiency in either of the following ways:

- Create 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.

You can expand the disk capacities when the EVS disks are in the **In-use** or **Available** state.

- Expanding an **In-use** EVS disk means that the to-be-expanded EVS disk has been attached to an ECS. Only certain ECS OSs support the expansion of **In-use** EVS disks. For details, see section "Expanding an **In-use** EVS Disk" in *Elastic Volume Service User Guide*.
- Expanding an **Available** EVS disk means that the to-be-expanded EVS disk has not been attached to an ECS. For details, see section "Expanding an Available EVS Disk" in *Elastic Volume Service User Guide*.
8.1 Adding a NIC

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:

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. In the search box above the upper right corner of the ECS list, enter the ECS name, IP address, or ID for searching.
5. Click the name of the target ECS.
   The page providing details about the ECS is displayed.
6. Click the NICs tab. Then, click Add NIC.
7. 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.
8. 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. Find 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 `ifconfig` 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. Find the target ECS, click More in the Operation column, and then click Restart.

10. Run the `ifconfig` command to check whether the NIC name obtained in step 2 is displayed in the command output.

    - If the password can be obtained, no further action is required.
    - If no, contact technical support.

### 8.2 Deleting a NIC

An ECS can have up to 12 NICs, including one primary NIC that cannot be deleted. To delete a non-primary NIC, perform the following 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. On the **Elastic Cloud Server** page, click the name of the target ECS. The page providing details about the ECS is displayed.

5. Click the **NICs** 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.

6. 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.
8.3 Managing Virtual IP Addresses

A virtual IP address provides the second IP address for one or more ECS NICs, improving high availability between the ECSs.

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. On the Elastic Cloud Server page, click the name of the target ECS.
   The page providing details about the ECS is displayed.
5. Click the NICs tab. Then, click Manage Virtual IP Address.
6. In the Manage Virtual IP Address dialog box, select Bind virtual IP address.
7. Set the IP address.
   This IP address is a virtual one. Multiple ECSs deployed to work in active/standby mode can be bound with the same virtual IP address for disaster recovery.
8. (Optional) Select Enable external access.
   After this option is selected, the ECSs with a virtual IP address bound can be accessed through VPN, Direct Connect, VPC peering, or Internet for flexible network functions.

NOTE
If you are required to access the target ECS through the Internet, you must bind an EIP to the virtual IP address of the ECS.
9. Click OK.

8.4 Enabling NIC Multi-Queue

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.

Support of NIC Multi-Queue

XEN ECSs do not support NIC multi-queue.
KVM ECSs created using the images listed in Table 8-1 support NIC multi-queue.

<table>
<thead>
<tr>
<th>OS</th>
<th>Image</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Windows Server 2008 WEB R2 64bit</td>
<td>Supported using private images</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 Standard/Datacenter/Enterprise 64bit</td>
<td>Supported using private images</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 Standard/Datacenter 64bit</td>
<td>Supported using private images</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016 Standard/Datacenter 64bit</td>
<td>Supported using private images</td>
</tr>
</tbody>
</table>
### OS | Image | Status
--- | --- | ---
Linux | Ubuntu 14.04 server 32bit | Supported
Linux | Ubuntu 14.04/16.04 server 64bit | Supported
Linux | OpenSUSE 42.2 64bit | Supported
Linux | SUSE Enterprise 12 SP1/SP2 64bit | Supported
Linux | CentOS 6.8/6.9/7.0/7.1/7.2/7.3/7.4 64bit | Supported
Linux | Red Hat 7.2/7.3/7.4 64bit | Supported
Linux | Debian 8.0.0/9.0.0 64bit | Supported
Linux | Fedora 24 64bit | Supported
Linux | Fedora 25 64bit | Supported
Linux | EulerOS 2.2 64bit | Supported

#### NOTE
- To obtain the virtualization type and number of NIC queues of an ECS, see section 1.7 Instance Family.
- Windows ECSs use private images to support NIC multi-queue. For details, see section "How Do I Set NIC Multi-queue Feature of an Image?" in Image Management Service User Guide.

### Procedure

KVM Windows ECSs use private images to support NIC multi-queue. For details, see section "How Do I Set NIC Multi-queue Feature of an Image?" in Image Management Service User Guide.

This section uses a Linux ECS running CentOS 7.4 as an example to describe how to enable NIC multi-queue.

**Step 1** Enable NIC multi-queue.

1. Log in to the ECS.
2. Run the following command to obtain the number of queues supported by the NIC and the number of queues with NIC multi-queue enabled:
   ```bash
ethtool -l NIC
```
3. Run the following command to configure the number of queues used by the NIC:
   ```bash
ehtool -L NIC combined Number of queues
```

An example is provided as follows:
```
[root@localhost ~]# ethtool -1 eth0  #View the number of queues used by NIC eth0.
Channel parameters for eth0:
Pre-set maximums:
  RX: 0
  TX: 0
Other: 0
Combined: 4  #Indicates that a maximum of four queues can be enabled for the NIC.
```
Current hardware settings:
RX: 0
TX: 0
Other: 0
Combined: 1 # Indicates that one queue has been enabled.

[root@localhost ~]# ethtool -L eth0 combined 4 # Enable four queues on NIC eth0.

**Step 2** (Optional) Enable irqbalance so that the system automatically allocates NIC interrupts on multiple vCPUs.

1. Run the following command to enable irqbalance:
   ```
   service irqbalance start
   ```
2. Run the following command to view the irqbalance status:
   ```
   service irqbalance status
   ```
   If the **Active** value in the command output contains **active(running)**, irqbalance has been enabled.

**Figure 8-1** Enabled irqbalance

**Step 3** (Optional) Enable interrupt binding.

Enabling irqbalance allows the system to automatically allocate NIC interrupts, improving network performance. If the improved network performance still fails to meet your requirements, manually configure interrupt affinity on the ECS.

To do so, perform the following operations:

Configure the following script so that one ECS vCPU serves the interrupt requests initialized by one queue. One queue corresponds to one interrupt, and one interrupt binds to one vCPU.

```bash
#!/bin/bash
service irqbalance stop

eth_dirs=$(ls -d /sys/class/net/eth*)
if [ $? -ne 0 ];then
   echo "Failed to find eth* , sleep 30" >> $ecs_network_log
   sleep 30
   eth_dirs=$(ls -d /sys/class/net/eth*)
fi

for eth in $eth_dirs
do
   cur_eth=$(basename $eth)
   cpu_count=`cat /proc/cpuinfo| grep "processor"| wc -l`
   virtio_name=$(ls -l /sys/class/net/$cur_eth/device/driver/ | grep pci | awk '{print $9}')
   affinity_cpu=0
```
Step 4  (Optional) Enable XPS and RPS.

XPS allows the system with NIC multi-queue enabled to select a queue by vCPU when sending a data packet.

```bash
#!/bin/bash
# enable XPS feature
cpu_count=$(grep -c processor /proc/cpuinfo)
dec2hex(){
    echo $(printf "%x" $1)
}
eth_dirs=$(ls -d /sys/class/net/eth*)
if [ $# -ne 0 ];then
    echo "Failed to find eth*, sleep 30" >> $ecs_network_log
    sleep 30
    eth_dirs=$(ls -d /sys/class/net/eth*)
fi
for eth in $eth_dirs
do
cpu_id=1
cur_eth=$(basename $eth)
cur_q_num=$(ethtool -l $cur_eth | grep -iA5 current | grep -i combined | awk {'print $2'})
for((i=0;i<cur_q_num;i++))
do
    if [ $i -eq $cpu_count ];then
        cpu_id=1
    fi
    xps_file="/sys/class/net/$cur_eth/queues/tx-$i/xps_cpus"
    rps_file="/sys/class/net/$cur_eth/queues/rx-$i/rps_cpus"
    cpuset=$(dec2hex "$cpu_id")
    echo $cpuset > $xps_file
    echo $cpuset > $rps_file
    let cpu_id=cpu_id*2
    done
done
```
9 Security Groups

9.1 Security Group Configuration Examples

9.1.1 Security Group Configuration Examples

Common security group configuration examples are as follows:

- Enable ECSs in different security groups to communicate with each other through an internal network.
  In this scenario, resources on an ECS associated with a security group need to be copied to another ECS associated with another security group. The two ECSs are in the same VPC. We recommend that you enable internal network communication between the ECSs and then copy resources.
  For details about security group configuration, see 9.1.2 Enabling ECSs in Different Security Groups to Communicate with Each Other Through an Internal Network.

- Enable specified IP addresses to remotely access ECSs in a security group.
  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.
  For details about security group configuration, see 9.1.3 Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group.

- Remotely connect to Linux ECSs using SSH.
  After creating Linux ECSs, you can add a security group rule to enable remote SSH access to the Linux ECSs.
  For details about security group configuration, see 9.1.4 Remotely Connecting to Linux ECSs Using SSH.

- Remotely connect to Windows ECSs using RDP.
  After creating Windows ECSs, you can add a security group rule to enable remote RDP access to the Windows ECSs.
  For details about security group configuration, see 9.1.5 Remotely Connecting to Windows ECSs Using RDP.

- Enable communication between ECSs.
  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.
For details about security group configuration, see 9.1.6 Enabling Communication Between ECSs.

- **Host a website on ECSs.**
  
  If you deploy a website on your ECSs and require that your website be accessed over HTTP or HTTPS, you can add the following rules to the security group used by the ECSs functions as the web servers.
  
  For details about security group configuration, see 9.1.7 Hosting a Website on ECSs.

- **Enable an ECS to function as a DNS server.**
  
  If you need to use an ECS as the 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.
  
  For details about security group configuration, see 9.1.8 Enabling an ECS to Function as a DNS Server.

- **Upload or download files using FTP.**
  
  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.
  
  For details about security group configuration, see 9.1.9 Uploading or Downloading Files using FTP.

### 9.1.2 Enabling ECSs in Different Security Groups to Communicate with Each Other Through an Internal Network

- **Example scenario:**
  
  In this scenario, resources on an ECS associated with a security group need to be copied to another ECS associated with another security group. The two ECSs are in the same VPC. We recommend that you enable internal network communication between the ECSs and then copy resources.

- **Security group configuration:**
  
  In the same VPC, ECSs associated with the same security group can communicate with one another by default, and no additional configuration is required. However, ECSs in different security groups cannot communicate with each other by default. You must add security group rules to enable the ECSs to communicate with one another through an internal network.
  
  You can add an inbound rule to each security group associated with the ECSs to allow access from ECSs associated with the other security group. The security group rule is as follows.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Direction</th>
<th>Port/Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol to be used for internal network communication. Supported values are TCP, UDP, ICMP, All, and GRE.</td>
<td>Inbound</td>
<td>Port or port range</td>
<td>IPv4 address, IPv4 CIDR block, or ID of another security group</td>
</tr>
</tbody>
</table>
9.1.3 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 associated with a security group over the SSH protocol and port 22, you can configure the following security group rule.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Direction</th>
<th>Port/Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH (22)</td>
<td>Inbound</td>
<td>22</td>
<td>IPv4 address, IPv4 CIDR block, or ID of another security group For example, 192.168.20.2</td>
</tr>
</tbody>
</table>

9.1.4 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 Linux ECSs.

- Security group configuration:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Direction</th>
<th>Port/Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH (22)</td>
<td>Inbound</td>
<td>22</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

9.1.5 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 Windows ECSs.

- Security group configuration:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Direction</th>
<th>Port/Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDP (3389)</td>
<td>Inbound</td>
<td>3389</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

9.1.6 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 configuration:
### 9.1.7 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 the following rules to the security group used by the ECSs functions as the web servers.

- **Security group configuration:**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Direction</th>
<th>Port/Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>Inbound</td>
<td>All</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>80 (HTTP)</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>443 (HTTPS)</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

### 9.1.8 Enabling an ECS to Function as a DNS Server

- **Example scenario:**
  
  If you need to use an ECS as the 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 configuration:**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Direction</th>
<th>Port/Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>Inbound</td>
<td>53</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>UDP</td>
<td>Inbound</td>
<td>53</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

### 9.1.9 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 configuration:**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Direction</th>
<th>Port/Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>Inbound</td>
<td>20-21</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>
9.2 Configuring Security Group Rules

Scenarios

If you do not have a VPC configured when creating your first ECS, the system automatically creates a default VPC. The security group policy of a default VPC allows data exchange only within the security group. As a result, ECSs in a default security group cannot be accessed from an external network. To remotely access an ECS in such a security group, you must configure the inbound rules of the security group.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. On the Elastic Cloud Server page, click the name of the target ECS. The page providing details about the ECS is displayed.
5. Click the Security Groups tab and view security group rules.
6. Click the security group ID. The system automatically switches to the Security Group page.
7. On the Inbound tab, click Delete in the Description column to delete the inbound rule.
8. Click Add Rule to add an inbound rule for the security group.
   - To remotely access a Windows ECS, set Protocol/Application to TCP and Port to 3389.
   - To remotely access a Linux ECS, set Protocol/Application to TCP and Port to 22.
   - Set Source IP Address to the IP address segment containing the IP addresses that you want to allow to access the ECS over the Internet.

   **NOTE**
   The default source IP address 0.0.0.0/0 indicates that all IP addresses can access ECSs in the security group.
9. Click OK to complete the security rule configuration.

9.3 Changing a Security Group

To change the security group of an ECS NIC, perform the following operations:

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. Locate the row containing the target ECS, click More in the Operation column, and select Change Security Group. The Change Security Group dialog box is displayed.
5. 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.

6. Click **OK**.
10.1 Changing an EIP Bandwidth

If an EIP has been bound to the ECS, the ECS can access the Internet in a specified bandwidth. To adjust the ECS bandwidth, perform the following operations:

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. On the Elastic Cloud Server page, click the name of the target ECS.
   The page providing details about the ECS is displayed.
5. Click the EIPS tab. Expand the information of the EIP to be modified and click the ID hyperlink.
   The Elastic IP page is displayed.
6. Switch to the page providing details about the EIP and click Modify behind Bandwidth Size.
7. Change the bandwidth name or size as prompted.

10.2 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 (to perform a software upgrade or install a patch, for example), you can select an ECS with a public IP address bound to function as an agent ECS, providing an access channel for these ECS.

Prerequisites

- An agent ECS with a public IP address bound is available.
  In this example, the agent ECS runs CentOS 6.5.
The IP address of the agent 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.
4. In the search box above the upper right corner of the ECS list, enter the agent ECS name for searching.
5. Click the name of the agent ECS. The page providing details about the ECS is displayed.
6. Click the NICs 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 agent ECS.
   For more details, see section 4.2.1 Login Overview.
8. Run the following command to check whether the agent ECS can access the Internet:
   ```
   ping www.google.com
   ```
   The agent ECS can access the Internet if information similar to the following is displayed:
   ```
   64 bytes from 220.181.111.148: icmp_seq=1 ttl=51 time=9.34 ms
   64 bytes from 220.181.111.148: icmp_seq=2 ttl=51 time=9.11 ms
   64 bytes from 220.181.111.148: icmp_seq=3 ttl=51 time=8.99 ms
   ```
9. Run the following command to check whether IP forwarding is enabled on the agent 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.
    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 agent ECS:
   ```
   iptables -t nat -A POSTROUTING -o eth0 -s subnet/netmask-bits -j SNAT --to nat-instance-ip
   ```
   For example, if the agent 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
   ```

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 10-1 is displayed.

```plaintext
Figure 10-1 Successful SNAT configuration
```

18. Add a route.
   a. Log in to 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 agent 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
```
11 Monitoring

11.1 ECS Monitoring

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.

This section covers the following content:

- Viewing ECS metrics
- Customizing ECS alarm rules
- Viewing ECS running statuses for routine monitoring

11.2 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>
<thead>
<tr>
<th>Metric</th>
<th>Windows ECS</th>
<th>Linux ECS</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>XEN</td>
<td>KVM</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>
## Monitoring

---

<table>
<thead>
<tr>
<th>Metric</th>
<th>Windows ECS</th>
<th>Linux ECS</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Read Bandwidth</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Disk Write Bandwidth</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Disk Read IOPS</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Disk Write IOPS</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Inband Incoming Rate</td>
<td>√</td>
<td>√</td>
<td>√ (vmtools must be installed on the image. Otherwise, this metric is unavailable.)</td>
</tr>
<tr>
<td>Inband Outgoing Rate</td>
<td>√</td>
<td>√</td>
<td>√ (vmtools must be installed on the image. Otherwise, this metric is unavailable.)</td>
</tr>
<tr>
<td>Outband Incoming Rate</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Outband Outgoing Rate</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>System Status Check Failed</td>
<td>√</td>
<td>x</td>
<td>√</td>
</tr>
</tbody>
</table>

**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/UVP-Tools/UVP-Tools/](https://github.com/UVP-Tools/UVP-Tools/).

Table 11-2 describes these ECS metrics.

### Table 11-2 ECS metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Formula</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Usage</td>
<td>Indicates the vCPU usage (%) of an ECS.</td>
<td>vCPU usage of an ECS/Number of vCPUs in the ECS</td>
<td>N/A</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Formula</td>
<td>Remarks</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>Indicates the memory usage (%) of an ECS.</td>
<td>Used memory of an ECS/Total memory of the ECS</td>
<td>This metric is unavailable if the image has no vmtools installed.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>Indicates the disk usage (%) of an ECS.</td>
<td>Used capacity of an ECS disk/Total capacity of the ECS disk</td>
<td>This metric is unavailable if the image has no vmtools installed.</td>
</tr>
<tr>
<td>Disk Read Bandwidth</td>
<td>Indicates the number of bytes read from an ECS per second.</td>
<td>Total number of bytes read from an ECS disk/Monitoring period</td>
<td>byte_out = (rd_bytes - last_rd_bytes)/Time difference</td>
</tr>
<tr>
<td>Disk Write Bandwidth</td>
<td>Indicates the number of bytes written to an ECS per second.</td>
<td>Total number of bytes written to an ECS disk/Monitoring period</td>
<td>N/A</td>
</tr>
<tr>
<td>Disk Read IOPS</td>
<td>Indicates the number of read requests sent to an ECS per second.</td>
<td>Total number of read requests sent to an ECS disk/Monitoring period</td>
<td>req_out = (rd_req - last_rd_req)/Time difference</td>
</tr>
<tr>
<td>Disk Write IOPS</td>
<td>Indicates the number of write requests sent to an ECS per second.</td>
<td>Total number of write requests sent to an ECS disk/Monitoring period</td>
<td>req_in = (wr_req - last_wr_req)/Time difference</td>
</tr>
<tr>
<td>Inband Incoming Rate</td>
<td>Indicates the number of incoming bytes on an ECS per second.</td>
<td>Total number of inband incoming bytes on an ECS/Monitoring period</td>
<td>N/A</td>
</tr>
<tr>
<td>Inband Outgoing Rate</td>
<td>Indicates the number of outgoing bytes on an ECS per second.</td>
<td>Total number of inband outgoing bytes on an ECS/Monitoring period</td>
<td>N/A</td>
</tr>
<tr>
<td>Outband Incoming Rate</td>
<td>Indicates the number of incoming bytes on an ECS per second on the hypervisor.</td>
<td>Total number of outband incoming bytes on an ECS/Monitoring period</td>
<td>This metric is unavailable if SR-IOV is enabled.</td>
</tr>
<tr>
<td>Outband Outgoing Rate</td>
<td>Indicates the number of outgoing bytes on an ECS per second on the hypervisor.</td>
<td>Total number of outband outgoing bytes on an ECS/Monitoring period</td>
<td>This metric is unavailable if SR-IOV is enabled.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Formula</td>
<td>Remarks</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System Status Check Failed</td>
<td>Check the status of the cloud platform for running ECSs. The check result is 0 or 1.</td>
<td>ECS/Monitoring period</td>
<td>When the power source of the physical host fails or the hardware/software becomes faulty, the check result is 1.</td>
</tr>
<tr>
<td></td>
<td>• 0: The system is running properly. All check items are normal.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1: The system is not running properly. At least one check item failed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The system periodically checks the status and returns check results using value 0 or 1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the detected fault does not affect ECS functions, certain management operations performed on the ECS, such as starting, stopping, or specifications modifications, may be affected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the detected fault affects ECS functions, such as a host power supply failure, the system will recover the ECS as soon as possible.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 11.3 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 periods, and notifications.

**Procedure**

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Management & Deployment**, click **Cloud Eye**.
4. In the navigation pane on the left, choose **Alarm Management > Alarm Rules**.
5. 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 complies with the alarm rule is generated.

   **NOTE**
   For more information about ECS alarm rules, see *Cloud Eye User Guide*.

### 11.4 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 section 11.3 **Setting Alarm Rules**.

- The target 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. 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 searching.
5. Click the name of the target ECS. The page providing details about the ECS is displayed.
6. Click the **Monitoring** tab to view the monitoring data.
7. 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.
A tag identifies an ECS. Adding tags to an ECS facilitates ECS identification and management.

You can add a tag to an ECS during the ECS creation or after the ECS creation (Tags tab on the page providing details about the ECS). Up to 10 tags can be added to an ECS.

**NOTE**
Tags added during ECS creation will also be added to the created EIP and EVS disks (including the system disk and data disks) of the ECS. If the ECS uses an existing EIP, the tags will not be added to the EIP.

After creating the ECS, you can view the tags on the pages providing details about the ECS, EIP, and EVS disks.

A tag consists of a tag key and a tag value. Table 12-1 lists the tag key and value requirements.

**Table 12-1 Tag key and value requirements**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
<th>Example Value</th>
</tr>
</thead>
</table>
| Key       | • Cannot be left blank.  
           | • The key value must be unique for an ECS.  
           | • Can contain a maximum of 36 characters.  
           | • Cannot contain the following characters: =<>\|  
           | • Cannot be started or ended with a space. | Organization |
| Value     | • Can contain a maximum of 43 characters.  
           | • Cannot contain the following characters: =<>\|  
           | • Cannot be started or ended with a space. | Apache |

Based on tags, you can perform the following operations:

- On the Elastic Cloud Server page, search for ECSs by tag key and value.
  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. Click **Search by Tag** above the upper right corner of the ECS list to expand the search area.
e. Enter the tag of the ECS to be searched for.
   Neither the tag key nor value can be empty. When the tag key or value is matched, the system automatically shows the target ECSs.
f. Click **Add Tag**.
   The system supports multiple tags and uses the intersection set of all tags to search for ECSs.
g. Click **Search**.
   The system searches for ECSs based on tag keys and values.

- On the **Tags** tab of an ECS, add, delete, modify, or view tags.
  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. On the **Elastic Cloud Server** page, click the name of the target ECS.
     The page providing details about the ECS is displayed.
  e. Click the **Tags** tab and perform desired operations.
    - **View tags.**
      You can view details of ECS tags, including the number of tags and the key and value of each tag.
    - **Add a tag.**
      Click **Add Tag** in the upper left corner. In the displayed dialog box, enter the key and value of the tag to be added, and click **OK**.
    - **Modify a tag.**
      Locate the row containing the tag to be edited and click **Edit** in the **Operation** column. In the **Edit Tag** dialog box, change the key and value of the tag and click **OK**.
    - **Delete a tag.**
      Locate the row containing the tag to be deleted and click **Delete** in the **Operation** column. In the **Delete Tag** dialog box, click **OK**.
13 Operation Trace Management

13.1 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>
<thead>
<tr>
<th>Operation</th>
<th>Resource Type</th>
<th>Trace Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating an ECS</td>
<td>ecs</td>
<td>createServer</td>
</tr>
<tr>
<td>Deleting an ECS</td>
<td>ecs</td>
<td>deleteServer</td>
</tr>
<tr>
<td>Starting an ECS</td>
<td>ecs</td>
<td>startServer</td>
</tr>
<tr>
<td>Restarting an ECS</td>
<td>ecs</td>
<td>rebootServer</td>
</tr>
<tr>
<td>Stopping an ECS</td>
<td>ecs</td>
<td>stopServer</td>
</tr>
<tr>
<td>Adding a NIC to an ECS</td>
<td>ecs</td>
<td>addNic</td>
</tr>
<tr>
<td>Removing a NIC to an ECS</td>
<td>ecs</td>
<td>deleteNic</td>
</tr>
<tr>
<td>Attaching a disk to an ECS</td>
<td>ecs</td>
<td>attachVolume</td>
</tr>
<tr>
<td>Attaching a disk to an ECS (on the ECS console)</td>
<td>ecs</td>
<td>attachVolume2</td>
</tr>
<tr>
<td>Detaching a disk from an ECS</td>
<td>ecs</td>
<td>detachVolume</td>
</tr>
<tr>
<td>Reinstalling the OS</td>
<td>ecs</td>
<td>reinstallOs</td>
</tr>
<tr>
<td>Changing the OS</td>
<td>ecs</td>
<td>changeOs</td>
</tr>
</tbody>
</table>
### 13.2 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 ![location_icon](image) in the upper left corner and select the desired region and project.
3. Click **Service List**. Under **Management & Deployment**, click **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. 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.
6. Click ![expand_icon](image) on the left of the required trace to expand its details.
7. 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.*
14 Troubleshooting

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

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

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

14.2 What Should I Do If a NIC Fails to Work?

Symptom

The NIC equipped on a large-memory ECS fails to work.

Possible Causes

The NIC driver has not been correctly installed.

Solution

Large-memory ECSs use passthrough NICs to improve network performance. You must install the passthrough NIC driver on the ECS or the image that is used for creating the ECS.

NOTE

If you mount the CD/DVD-ROM driver over a VPN, ensure that the VPN bandwidth is greater than 8 Mbit/s.

You can do so by performing the following operations:
Step 1  Obtain the passthrough NIC driver.

Passthrough NIC driver versions vary depending on the OS. For details, see Table 14-1.

Table 14-1 NIC driver versions and OSs

<table>
<thead>
<tr>
<th>NIC Driver Version</th>
<th>OS</th>
<th>How to Obtain</th>
</tr>
</thead>
<tbody>
<tr>
<td>ixgbevf 2.16.4</td>
<td>CentOS 7.2 64bit</td>
<td><a href="https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/2.16.4/">https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/2.16.4/</a></td>
</tr>
</tbody>
</table>

Step 2  Log in to the ECS.

For more details, see section 4.1.2 Login Using VNC.

Step 3  Install the passthrough NIC driver on the ECS. In this procedure, CentOS 7.2 64bit is used as an example.

1. Configure the passthrough NIC.

Not all ECS OSs identify passthrough NICs using the standard NIC naming rule of ethx, where x is a number. If this is the case, you must configure the ECS so that it can identify the passthrough NIC. The procedure is as follows:

a. Run the following command to view all NICs on the ECS and identify the passthrough NIC:
   
   `ifconfig -a`

b. Run the following command to switch to the directory where configuration files are stored:
   
   `cd /etc/sysconfig/network-scripts/`

c. Run the following command to create a configuration file for the passthrough NIC:
   
   `cp ifcfg-eth0 ifcfg-NIC_name`

In the preceding command, NIC_name specifies the name of the passthrough NIC.

d. Use the vi editor to edit this configuration file:
   
   `vi ifcfg-NIC_name`

e. Set the DEVICE parameter in the configuration file to the name of the passthrough NIC. The following is an example configuration:

```
DEVICE="NIC_name"
BOOTPROTO="dhcp"
ONBOOT="yes"
STARTMODE="onboot"
```

f. Run the following command to restart the network service and allow the configuration to take effect:

   `service network restart`

2. Upload the obtained passthrough NIC driver to a directory on the ECS, for example, /home.

3. Switch to user root on the ECS CLI and open the target directory.

In this example, the passthrough NIC driver is stored in the /home directory. Run the cd /home command to switch to the target directory.
4. Run the following command to decompress the software package. (In this procedure, ixgbevf version 2.16.4 is used as an example.)
   
   ```
   tar -zxvf ixgbevf-2.16.4.tar.gz
   ```

5. Run the following command to switch to the generated src directory:
   
   ```
   cd ixgbevf-2.16.4/src
   ```

6. Run the following commands to install the driver:
   
   ```
   make
   make install
   ```

7. Run the following command to restart the ECS to make the drive take effect:
   
   ```
   reboot
   ```

8. Switch to user root on the ECS CLI and open the src directory, for example, by running the `cd /home/ixgbevf-2.16.4/src` command. Then, run the following commands to check whether the driver has been installed:
   
   ```
   rmmod ixgbevf
   insmod ./ixgbevf.ko
   ethtool -i NIC_name
   ```

   **NOTE**
   
   - After you run the `rmmod ixgbevf` command, the system may display an error message. This message does not affect the installation of the passthrough NIC driver and can be ignored.
   - `NIC_name` specifies the passthrough NIC name, for example, `ens5`.

9. Check the driver status based on the displayed information.
   
   In this example, the driver is installed if `driver` is `ixgbevf` and `version` is `2.16.4`.

---End

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

**Symptom**

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

**Figure 14-1** Connection timeout

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

**Solution**

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

5. Press Esc to exit editing mode.
6. Run the following command to save the configuration and exit:
   
   :wq

**NOTE**

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

---

### 14.4 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.
2. Run the following command to switch to user root:
   
   `sudo su`

3. 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`
4. Change the drive letter (for example, /dev/sdb) of the SCSI disk to the corresponding SCSI ID in the /etc/fstab file.

```
CNA64_22:/opt/galax/eucalyptus/ecs_scripts # ll /dev/disk/by-id/|grep sdb
lrwxrwxrwx 1 root root  9 Dec  6 11:26 scsi-368860300001436b005014f890338280 -> ../../sdb
lrwxrwxrwx 1 root root  9 Dec  6 11:26 wwn-0x688860300001436b005014f890338280 -> ../../sdb
```

/dev/disk/by-id/SCSI ID
For example, if the SCSI ID obtained in step 3 is scsi-368860300001436b005014f890338280, use the following data to replace /dev/sdb:

```
/dev/disk/by-id/scsi-368860300001436b005014f890338280
```

### 14.5 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.

### 14.6 Why Was My Login to a Linux ECS with a Key File Unsuccessful?

**Symptom**

When the key file for creating a Linux ECS was used to log in to the ECS, the login failed.

**Possible Causes**

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

- **Cause 1:** The image used to create the Linux ECS is a private image, on which Cloud-Init is not installed.
- **Cause 2:** Cloud-Init is installed on the image, but the key pair was not obtained during ECS creation.
Solution

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

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

- If the issue is a result of cause 2, proceed as follows:
  
  a. Locate the row containing the target ECS, click More in the Operation column, and select Restart.
  
  b. Use the key file to log in to the ECS again and check whether the login is successful.
     - If the login is successful, no further action is required.
     - If the login fails, contact technical support.

14.7 What Should I Do If Error "command `gcc` failed with exit status 1" Occurs During PIP-based Software Installation

Symptom

When installing the Python library software, you need to configure the PIP source. Take the official image source as an example:

```
[root@test home]# cat /root/.pip/pip.conf
[global]
index-url = https://pypi.python.org/simple
trusted-host = pypi.python.org
```

During the installation, the system displays the message "command `gcc` failed with exit status 1". However, GCC has been installed by running the yum command before the Python library software is installed using the PIP.

Figure 14-2 Installation error
Possible Causes

openssl-devel is not supported.

Solution

The following operations use psutil as an example:

1. Run the following command to install openssl-devel:
   
   ```
   yum install gcc libffi-devel python-devel openssl-devel -y
   ```

2. Use PIP to install the Python library software again. The error message is cleared.

![Figure 14-3 Successful installation](image)

14.8 What Should I Do If Packages Are Downloaded Using PIP or wget at a Low Rate?

Symptom

When a user runs the wget command to download software packages, the download rate is far less than the bandwidth.

![Figure 14-4 wget-based package downloading](image)

Possible Causes

The official PIP website is accessed using HTTPS. Each time PIP is used to install a third-party Python module, the source code package must be downloaded at the official PIP website. Therefore, openssl packages are required.
Solution

Run the following command to install openssl packages:

```
yum install openssl openssl-devel
```

14.9 What Should I Do When a Disk Goes 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."

![Offline disk](image)

Possible Causes

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

<table>
<thead>
<tr>
<th>SAN Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnlineAll</td>
<td>Indicates that all newly detected disks are automatically brought online.</td>
</tr>
<tr>
<td>OfflineShared</td>
<td>Indicates that all newly detected disks on sharable buses, such as FC or iSCSI, are left offline by default, while disks on non-sharable buses are kept online.</td>
</tr>
<tr>
<td>OfflineInternal</td>
<td>Indicates that all newly detected disks are left offline.</td>
</tr>
</tbody>
</table>

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

Solution

Use the disk partition management tool DiskPart to obtain and set the SAN policy on the ECS to **OnlineAll**.
1. Log in to the Windows ECS.
2. Press **Win+R** to run **cmd.exe**.
3. Run the following command to access DiskPart:
   ```
   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 to make
   the configuration take effect permanently. After an ECS is created using this private
   image, the disks attached to the ECS are online by default. You only need to initialize
   them.

14.10 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**. The **PuTTY Key Generator** page is displayed.
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 14-7 is the public key with the format meeting system requirements.
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.
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.

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

Symptom

- An error message was displayed on the management console after you performed ECS-related operations.
- An error code was displayed after you used an ECS-related API.
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 14-3.

Table 14-3 Error codes and solution suggestions

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Message Displayed on the Management Console</th>
<th>Solution Suggestion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ecs.0000</td>
<td>Request error. Try again later or contact customer service.</td>
<td>Adjust the request structure as directed in Elastic Cloud Server API Reference.</td>
</tr>
<tr>
<td>Ecs.0001</td>
<td>The maximum number of ECSs or EVS disks has been reached. Contact customer service and request a quota increase.</td>
<td>Contact customer service to apply for an increased ECS quota. \n<strong>NOTE</strong> When applying for increasing your ECS quota, first determine the number of target ECSs, CPU cores (vCPUs), and memory capacity (RAM) required.</td>
</tr>
<tr>
<td>Ecs.0003</td>
<td>You do not have the permission or your balance is insufficient.</td>
<td>Contact customer service to check your account information.</td>
</tr>
<tr>
<td>Ecs.0005</td>
<td>System error. Try again later or contact customer service.</td>
<td>Adjust the request structure as directed in Elastic Cloud Server API Reference.</td>
</tr>
<tr>
<td>Ecs.0010</td>
<td>The private IP address is in use. Select an available IP address and create the ECS again.</td>
<td>Use an idle IP address to create your ECS.</td>
</tr>
<tr>
<td>Ecs.0011</td>
<td>Invalid password. Change the password to make it meet the password complexity requirements, and perform the required operation again.</td>
<td>Input a password that meets password complexity requirements. Then, initial the request again.</td>
</tr>
<tr>
<td>Ecs.0012</td>
<td>The number of IP addresses in the subnet is insufficient. Release IP addresses in the subnet or select another subnet, and</td>
<td>Obtain more idle IP addresses on the target subnet or use a new subnet for creating ECSs.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Message Displayed on the Management Console</td>
<td>Solution Suggestion</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Ecs.0013</td>
<td>Insufficient EIP quota. Contact customer service and request a quota increase.</td>
<td>Contact customer service to apply for an increased EIP quota.</td>
</tr>
<tr>
<td>Ecs.0015</td>
<td>The disk of this type is not applicable to the ECS.</td>
<td>Select a supported EVS disk and attach it to the ECS.</td>
</tr>
<tr>
<td>Ecs.0100</td>
<td>The ECS status does not meet requirements. Make the ECS in the required status and try again.</td>
<td>Change the ECS status to the required status and try again.</td>
</tr>
<tr>
<td>Ecs.0103</td>
<td>The disk is unavailable.</td>
<td>Change the ECS status to the required status and try again. If the EVS disk is faulty, contact customer service for troubleshooting.</td>
</tr>
<tr>
<td>Ecs.0104</td>
<td>Insufficient number of ECS slots for attaching disks.</td>
<td>Detach an EVS disk from the ECS before attaching a new EVS disk.</td>
</tr>
<tr>
<td>Ecs.0105</td>
<td>No system disk found.</td>
<td>Reattach the EVS system disk to the ECS and perform the desired operation again.</td>
</tr>
<tr>
<td>Ecs.0107</td>
<td>The number of shared disks that can be attached to an ECS exceeds the maximum limit.</td>
<td>Detach an EVS disk from the ECS before attaching a new EVS disk.</td>
</tr>
<tr>
<td>Other error codes</td>
<td>Other error messages</td>
<td>Initiate the request again. If the error persists, record the returned error code and contact customer service for troubleshooting.</td>
</tr>
</tbody>
</table>

### 14.12 How Can I Handle Slow ECS Startup?

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

1. Log in to the ECS.
2. Run the following command to switch to user `root`:

   ```sh
sudo su
   ```

3. Run the following command to obtain the grub version:

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

**Figure 14-9 Changing timeout duration**

### 14.13 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 14-10.

**Figure 14-10 Errors in Cloud-Init**
Possible Causes

The Python version used by Cloud-Init was incorrect.

Solution

Change the Python version used by Cloud-Init to the source version. To do so, change the environment variable value of `/usr/bin/cloud-init` from the default value `#!/usr/bin/python` to `#!/usr/bin/python2.6`.

Figure 14-11 Changing the Python version
15 FAQs

15.1 General FAQs

15.1.1 What Restrictions Apply to ECSs?

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

15.1.2 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.

15.1.3 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.

15.1.4 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**.

### 15.1.5 What Is a Deleted ECS?

**Deleted** is an intermediate state of the ECS. **Deleted** indicates that the ECS has been deleted. ECSs in this state can no longer provide services and are soon removed from the system.

### 15.1.6 Can a Deleted ECS Be Provisioned Again?

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

### 15.1.7 Why Does the Task Status 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 **Task Status** 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 details about created ECSs.
- The **Task Status** 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.

### 15.2 Management FAQs

#### 15.2.1 Can I Transfer ECS Ownership Between Accounts?

No. This function is not supported.

#### 15.2.2 What Is the cloudbase-init Account in Windows ECSs?

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.

Do not modify or delete this account or uninstall the Cloudbase-Init agent program. Otherwise, injecting the customized data for initializing the ECS generated using the Windows private image created based on this ECS will fail.

**NOTE**

This account is unavailable on Linux ECSs.
15.2.3 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.

Solution

To make the changed hostname take effect even after the ECS is stopped or restarted, save the changed name 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
   ```
   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:
```bash
sudo reboot
```

**Step 5** Run the following command to check whether the hostname has been changed:
```bash
sudo hostname
```
If the changed hostname is displayed in the command output, the hostname has been changed and the new name permanently takes effect.

---

**15.2.4 Is the 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 15-1 lists the hostnames (obtained by running the `hostname` command) of ECSs created using different images and those displayed after the ECSs are restarted.

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

Hostnames of ECSs created from 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 host names, change the host names. For details, see section 15.2.3 How Can a Changed Static Hostname Take Effect Permanently?
15.2.5 Why Does the System Display a Question Mark When I Attempt to Obtain Console Logs?

Symptom

The system displays a question mark (?) when users attempt to obtain the console logs of an ECS.

Possible Causes

The image based on which the ECS was created supports viewing console logs. However, this function is not enabled on the ECS.

Solution

Enable management console log obtaining on the ECS.

For details, see step 1 in section 3.7 Obtaining ECS Console Logs.

15.3 VNC FAQs

15.3.1 Why Cannot I Use the Spanish Keyboard to Enter Characters After I Log In to an ECS Using VNC?

Symptom

Characters ☄, ☾, and ☣ cannot be entered properly when the Spanish keyboard is used for input.

Solution

Use the keyboard on the VNC page to replace the physical keyboard. To do so, perform the following operations:

1. Click AltGr on the VNC page so that AltGr enters the hold-down state (AltGr turns red).
2. Click the desired character in the upper-right corner of the VNC page.

An example is provided as follows:

To enter character ☄, perform the following operations:

1. Click AltGr on the VNC page.
   This operation is successful if AltGr turns red.
2. Click ☄ in the upper-right corner of the VNC page.
15.3.2 Why Cannot I Use the Portuguese Keyboard to Enter Characters After I Log In to an ECS Using VNC?

Characters ☛, ☞, and ☜ cannot be entered properly when the Portuguese keyboard is used for input.

Solution

Use the keyboard on the VNC page to replace the physical keyboard. To do so, perform the following operations:

1. Click AltGr on the VNC page so that AltGr enters the hold-down state (AltGr turns red).
2. Click the desired character in the upper-right corner of the VNC page.

An example is provided as follows:

To enter character ☛, perform the following operations:

1. Click AltGr on the VNC page.
   This operation is successful if AltGr turns red.
2. Click ☛ in the upper-right corner of the VNC page.
3. Click AltGr on the VNC page again to cancel the hold-down state.

15.3.3 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.

15.3.4 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 perform a data viewing operation, such as running the cat command to view large files or playing videos, VNC may become unavailable due to the high memory usage of the browser. In this case, use another browser to log in to the ECS again.
15.3.5 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.

15.4 Login FAQs

15.4.1 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 15-2.

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

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

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

1. Ensure that the key pair for logging in to the ECS is correct.
2. Ensure that DHCP is enabled in the VPC to which the ECS belongs.
3. Ensure that the ECS has an EIP bound.
4. View security group rules in the outbound direction and ensure that port 80 port is open.
15.4.3 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 set up a remote desktop connection to a Windows ECS using RDP, such as MSTSC, an error occurs. The system displays the possible cause "This could be due to CredSSP encryption oracle remediation."

**Figure 15-1** Failed to set up a remote desktop connection

Possible Causes

Microsoft released a security patch in March 2018, which may affect RDP-based CredSSP connections. As a result, setting up RDP-based connections to ECSs failed. For details, visit [Unable to RDP to Virtual Machine: CredSSP Encryption Oracle Remediation](https://go.microsoft.com/fwlink/?linkid=866660).

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 15-2 Modifying remote desktop connection settings

5. Click OK.

15.4.4 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 15-3 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 section 6.1.1 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 section 15.9.10 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.

If neither of the preceding methods take effect, contact customer service for technical support.

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

Symptom

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

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

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

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

Windows

For example, there are two Windows ECSs with parameters configured in Table 15-3.

<table>
<thead>
<tr>
<th>ECS</th>
<th>System Disk</th>
<th>Key Pair</th>
</tr>
</thead>
<tbody>
<tr>
<td>ecs_01</td>
<td>vol_01</td>
<td>Keypair_01</td>
</tr>
<tr>
<td>ecs_02</td>
<td>vol_02</td>
<td>Keypair_02</td>
</tr>
</tbody>
</table>
System disk vol_01 is detached from ecs_01 offline and then attached to ecs_02 as the system disk. How can I log in to ecs_02?

The random password for logging in to ecs_02 must be resolved again. The procedure is as follows:

1. Delete the initial password for logging in to ecs_02.
   Locate the row containing ecs_02, click More in the Operation column, and select Delete Password from the drop-down list. Then, click Delete.

   NOTE
   ecs_02 must be in Stopped state.

2. Start ecs_02.
   Locate the row containing ecs_02, click More in the Operation column, and select Start from the drop-down list. Then, in the Start ECS dialog box, click OK.

3. Obtain the password for logging in to ecs_02.
   a. Locate the row containing ecs_02, click More in the Operation column, and select Get Password from the drop-down list.
   b. Click Select File and upload private key file Keypair_02 of ecs_02.
   c. Click Get Password to obtain a new random password.

4. Use the random password obtained in step 3 to log in to ecs_02 with the system disk replaced.

### Linux

For example, there are two Linux ECSs with parameters configured in Table 15-4.

<table>
<thead>
<tr>
<th>ECS</th>
<th>System Disk</th>
<th>Key Pair</th>
</tr>
</thead>
<tbody>
<tr>
<td>ecs_01</td>
<td>vol_01</td>
<td>Keypair_01</td>
</tr>
<tr>
<td>ecs_02</td>
<td>vol_02</td>
<td>Keypair_02</td>
</tr>
</tbody>
</table>

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

Use either of the following methods to log in to ecs_02:

- Use private key file Keypair_01 of ecs_01.
- Use private key file Keypair_02 of ecs_02.

### 15.4.6 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** (see section 5.4 Obtaining the Password for Logging In to a Windows ECS) is clicked, the system displays a message indicating that the password could not be viewed. ECS login was therefore unsuccessful.

### Possible Causes

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

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

### Solution

- **If the issue is a result of cause 1,** proceed as follows:
  
  If a private image is created without Cloudbase-Init installed, the ECS configuration cannot be customized. As a result, you can log in to the ECS only using the original image password.
  
  The original image password is the OS password configured when the private image was created. If the original image password has been lost, use the password reset function available on the **Elastic Cloud Server** page to reset the password.

- **If the issue is a result of cause 2,** proceed as follows:
  
  a. Locate the row containing the target ECS, click **More** in the **Operation** column, and select **Restart**.
  
  b. 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 technical support.

### 15.5 Key Pair

#### 15.5.1 How Can I Obtain the Key Pair Used by an ECS?

**Symptom**

If a user has created multiple key pairs, the user might not know which is the required one for logging in to the target ECS. This section describes how to quickly identify the target key pair on the management console.

**Procedure**

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Elastic Cloud Server**.
4. On the **Elastic Cloud Server** page, select the target ECS.
5. Click the name of the ECS.
   
   The page providing details about the ECS is displayed.
6. Obtain the **Key Pair** value.
   The value is the key pair used by the ECS.

### 15.6 EIP FAQs

#### 15.6.1 Can Multiple EIPs Be Bound to an ECS?

Yes. However, this configuration is not recommended.

To configure multiple EIPs, you must manually configure routing policies. Exercise caution when you perform this operation.

**Configuration Example**

Table 15-5 lists ECS configurations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>ecs_test</td>
</tr>
<tr>
<td>Image</td>
<td>Red Hat Enterprise Linux 6.5 64bit</td>
</tr>
<tr>
<td>EIP</td>
<td>2</td>
</tr>
<tr>
<td>Primary NIC</td>
<td>eth0</td>
</tr>
<tr>
<td>Secondary NIC</td>
<td>eth1</td>
</tr>
</tbody>
</table>

**Example 1:**

If you are required to access public network 11.11.11.0/24 through standby NIC **eth1**, perform the following operations to configure a routing policy:

1. Log in to the ECS.
2. Run the following command to configure a routing policy:
   ```
   ip route add 11.11.11.0/24 dev eth1 via 192.168.2.1
   ```
   In the preceding command, **192.168.2.1** is the gateway IP address of standby NIC **eth1**.

**Example 2:**

Based on example 1, if you are required to enable routing for default public network traffic through standby NIC **eth1**, perform the following operations to configure a routing policy:

1. Log in to the ECS.
2. Run the following command to delete the default route:
   ```
   ip route delete default
   ```
3. Run the following command to configure a new default route:
   ```
   ip route add 0.0.0.0/0 dev eth1 via 192.168.2.1
   ```
   In the preceding command, **192.168.2.1** is the gateway IP address of standby NIC **eth1**.
15.6.2 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.

15.6.3 Can an ECS Without an EIP Access the Internet?

Yes.

- Method 1: Configure a SNAT server.
  You can configure the SNAT server so that the ECS without an EIP bound can access the Internet.
  For details, see section Configuring a SNAT Server in Virtual Private Cloud User Guide.
- Method 2: Create a NAT gateway.
  If a large number of concurrent connections are required, you are advised to use the NAT Gateway service provided by the public cloud platform.
  The NAT Gateway service offers the NAT function for ECSs in a VPC, allowing these ECSs to access the Internet using an EIP. For more information about NAT Gateway, see NAT Gateway User Guide.

15.6.4 Why Can I Remotely Access an ECS But Cannot Ping It?

To ping an ECS, enable Internet Control Message Protocol (ICMP) in the security group rules for the ECS.

1. Log in to the management console.
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.
6. Add an inbound rule for the security group and enable ICMP.
   - Protocol/Application: ICMP
   - Source: IP address 0.0.0.0/0

15.7 Network

15.7.1 Can the ECSs of Different Accounts Communicate over the Intranet?

No. The ECSs of different accounts cannot communicate with each other over the intranet.
15.7.2 How Can I Check Whether Remaining Resources Are Sufficient for Automatic Recovery?

The operation team checks the capacity report for physical hosts every day for the following information:

- Whether resource utilization has reached the upper threshold.
- Whether remaining resources are sufficient for automatic recovery.

Based on the information, the operation team determines whether to expand the resource pool.

15.7.3 How Can I Receive an Automatic ECS Recovery Event?

Create an alarm rule with Metric setting to System Status Check Failed on the Cloud Eye console.

15.7.4 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 15-6.
- Back up key ECS data before modifying kernel parameter settings.

Background

Table 15-6 Common Linux kernel parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>net.core.rmem_default</td>
<td>Specifies the default size (in bytes) of the window for receiving TCP data.</td>
</tr>
<tr>
<td>net.core.rmem_max</td>
<td>Specifies the maximum size (in bytes) of the window for receiving TCP data.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>net.core.wmem_default</td>
<td>Specifies the default size (in bytes) of the window for transmitting TCP data.</td>
</tr>
<tr>
<td>net.core.wmem_max</td>
<td>Specifies the maximum size (in bytes) of the window for transmitting TCP data.</td>
</tr>
<tr>
<td>net.core.netdev_max_backlog</td>
<td>Specifies the maximum number of packets that can be sent to a queue when the rate at which each network port receives packets is faster than the rate at which the kernel processes these packets.</td>
</tr>
<tr>
<td>net.core.somaxconn</td>
<td>Defines the maximum length of the listening queue for each port in the system. This parameter applies globally.</td>
</tr>
<tr>
<td>net.core.optmem_max</td>
<td>Specifies the maximum size of the buffer allowed by each socket.</td>
</tr>
<tr>
<td>net.ipv4.tcp_mem</td>
<td>Uses the TCP stack to show memory usage in memory pages (4 KB generally).</td>
</tr>
<tr>
<td></td>
<td>• The first value is the lower limit of memory usage.</td>
</tr>
<tr>
<td></td>
<td>• The second value is the upper limit of the load added to the buffer when the memory is overloaded.</td>
</tr>
<tr>
<td></td>
<td>• The third value is the upper limit of memory usage. When this value is reached, packets can be discarded to reduce memory usage. For a large BDP, increase the parameter value as needed. The unit of this parameter is memory page but not byte.</td>
</tr>
<tr>
<td>net.ipv4.tcp_rmem</td>
<td>Specifies the memory used by sockets for automatic optimization.</td>
</tr>
<tr>
<td></td>
<td>• The first value is the minimum number of bytes allocated to the socket buffer for receiving data.</td>
</tr>
<tr>
<td></td>
<td>• The second value is the default value, which is overwritten by rmem_default. The buffer size can increase to this value when the system load is not heavy.</td>
</tr>
<tr>
<td></td>
<td>• The third value is the maximum number of bytes allocated to the socket buffer for receiving data. This value is overwritten by rmem_max.</td>
</tr>
<tr>
<td>net.ipv4.tcp_wmem</td>
<td>Specifies the memory used by sockets for automatic optimization.</td>
</tr>
<tr>
<td></td>
<td>• The first value is the minimum number of bytes allocated to the socket buffer for transmitting data.</td>
</tr>
<tr>
<td></td>
<td>• The second value is the default value, which is overwritten by wmem_default. The buffer size can increase to this value when the system load is not heavy.</td>
</tr>
<tr>
<td></td>
<td>• The third value is the maximum number of bytes allocated to the socket buffer for transmitting data. This value is overwritten by wmem_max.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>net.ipv4.tcp_keepalive_time</td>
<td>Specifies the interval at which keepalive detection messages are sent in seconds for checking TCP connections.</td>
</tr>
<tr>
<td>net.ipv4.tcp_keepalive_intvl</td>
<td>Specifies the interval at which keepalive detection messages are resent in seconds when no response is received.</td>
</tr>
<tr>
<td>net.ipv4.tcp_keepalive_probes</td>
<td>Specifies the maximum number of keepalive detection messages that are sent to determine a TCP connection failure.</td>
</tr>
<tr>
<td>net.ipv4.tcp_sack</td>
<td>Enables selective acknowledgment (value 1 indicates enabled). This configuration allows the transmitter to resend only lost packets, thereby improving system performance. However, this configuration will increase the CPU usage. You are suggested to enable selective acknowledgment for WAN communication.</td>
</tr>
<tr>
<td>net.ipv4.tcp_fack</td>
<td>Enables forwarding acknowledgment for selective acknowledgment (SACK), thereby reducing congestion. You are suggested to enable forwarding acknowledgment.</td>
</tr>
<tr>
<td>net.ipv4.tcp_timestamps</td>
<td>Specifies a TCP timestamp, which will add 12 bytes in the TCP packet header. This configuration calculates RTT using RFC1323, a more precise retransmission method upon timeout than retransmission. You are suggested to use this configuration for higher system performance.</td>
</tr>
<tr>
<td>net.ipv4.tcp_window_scaling</td>
<td>Enables RFC1323-based window scaling by setting the parameter value to 1 if the TCP window is larger than 64 KB. The maximum TCP window is 1 GB. This parameter takes effect only when window scaling is enabled on both ends of the TCP connection.</td>
</tr>
<tr>
<td>net.ipv4.tcp_syncookies</td>
<td>Specifies whether to enable TCP synchronization (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.</td>
</tr>
<tr>
<td>net.ipv4.tcp_twReuse</td>
<td>Specifies whether a TIME-WAIT socket (TIME-WAIT port) can be used for new TCP connections.</td>
</tr>
<tr>
<td>net.ipv4.tcp_twRecycle</td>
<td>Allows fast recycle of TIME-WAIT sockets.</td>
</tr>
<tr>
<td>net.ipv4.tcp_fin_timeout</td>
<td>Specifies the time (in seconds) during which a socket TCP connection that is disconnected from the local end retains in 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.</td>
</tr>
<tr>
<td>net.ipv4.ip_local_port_range</td>
<td>Specifies local port numbers allowed by TCP/UDP.</td>
</tr>
</tbody>
</table>
| net.ipv4.tcp_max_syn_backlog     | Specifies the maximum number of connection requests that}
### Parameter | Description
--- | ---
og | 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.

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_twReuse = 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:
15.7.5 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: indicates an ECS that is tested for network performance. Such an ECS functions as the client (TX end) or server (RX end) in netperf tests.
- Load generator: indicates an ECS that is used to exchange test data with the tested ECS. The load generator functions as the client (TX end) or server (RX end) in netperf tests.
- Table 15-7 and Table 15-8 list common test tool parameters.

Table 15-7 Common netperf parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>Port number</td>
</tr>
<tr>
<td>-H</td>
<td>IP address of the RX end</td>
</tr>
<tr>
<td>-t</td>
<td>Protocol used in packet transmitting, the value of which is TCP_STREAM in bandwidth tests</td>
</tr>
<tr>
<td>-l</td>
<td>Test duration</td>
</tr>
<tr>
<td>-m</td>
<td>Data packet size, which is suggested to be 1440 in bandwidth tests</td>
</tr>
</tbody>
</table>

Table 15-8 Common iperf3 parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>Port number</td>
</tr>
<tr>
<td>-c</td>
<td>IP address of the RX end</td>
</tr>
<tr>
<td>-u</td>
<td>UDP packets</td>
</tr>
<tr>
<td>-b</td>
<td>TX bandwidth</td>
</tr>
<tr>
<td>-t</td>
<td>Test duration</td>
</tr>
<tr>
<td>-l</td>
<td>Data packet size, which is suggested to be 16 in PPS tests</td>
</tr>
<tr>
<td>-A</td>
<td>ID of the vCPU used by iperf3</td>
</tr>
</tbody>
</table>

In this section, the maximum number of 16 vCPUs is used as an example for each ECS. If an ECS has 8 vCPUs, the -A value ranges from 0 to 7.
Test Preparations

**Step 1** Prepare ECSs.

Ensure that both type and specifications of the tested ECS and load generators are the same. In addition, these ECSs are deployed in the same ECS group with anti-affinity enabled.

<table>
<thead>
<tr>
<th>Table 15-9 Preparations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td>Tested ECS</td>
</tr>
<tr>
<td>Load generator</td>
</tr>
</tbody>
</table>

**Step 2** Install the netperf, iperf3, and sar test tools on both the tested ECS and load generators.

Table 15-10 lists the procedures for installing these tools.

<table>
<thead>
<tr>
<th>Table 15-10 Installing test tools</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tool</strong></td>
</tr>
</tbody>
</table>
| netperf | 1. Run the following command to install gcc: \n  \n  `yum -y install unzip gcc gcc-c++`  
  2. Run the following command to download the netperf installation package: \n  \n  `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: \n  \n  `unzip netperf-2.7.0.zip`  
  `cd netperf-netperf-2.7.0/`  
  `/ configure & & make & & make install` |
| iperf3 | 1. Run the following command to download the iperf3 installation package: \n  \n  `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: \n  \n  `unzip iperf3.zip`  
  `cd iperf-master/`  
  `/ configure & & make & & make install` |
| sar | Run the following command to install sar: \n  \n  `yum -y install sysstat` |
Step 3 Enable NIC multi-queue on both tested ECSs and load generators.

1. Run the following command to check the number of queues supported by the ECSs:
   \texttt{ethtool -l eth0 | grep -i Pre -A 5 | grep Combined}
2. Run the following command to enable NIC multi-queue:
   \texttt{ethtool -L eth0 combined X}
   In the preceding command, \texttt{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 load generators to start the netserver process:
   \texttt{netserver -p 12001}
   \texttt{netserver -p 12002}
   In the preceding commands, \texttt{-p} specifies the listening port.
2. Start the netperf process on the tested ECS and specify a netserver port on each load generator. For details about common netperf parameters, see Table 15-7.
   ##Load generator 1
   \texttt{netperf -H 192.168.2.11 -p 12001 -t TCP_STREAM -l 300 --m 1440 &}
   \texttt{netperf -H 192.168.2.11 -p 12002 -t TCP_STREAM -l 300 --m 1440 &}
   ##Load generator 2
   \texttt{netperf -H 192.168.2.12 -p 12001 -t TCP_STREAM -l 300 --m 1440 &}
   \texttt{netperf -H 192.168.2.12 -p 12002 -t TCP_STREAM -l 300 --m 1440 &}
   ##Load generator 3
   \texttt{netperf -H 192.168.2.13 -p 12001 -t TCP_STREAM -l 300 --m 1440 &}
   \texttt{netperf -H 192.168.2.13 -p 12002 -t TCP_STREAM -l 300 --m 1440 &}
   ##Load generator 4
   \texttt{netperf -H 192.168.2.14 -p 12001 -t TCP_STREAM -l 300 --m 1440 &}
   \texttt{netperf -H 192.168.2.14 -p 12002 -t TCP_STREAM -l 300 --m 1440 &}
   ##Load generator 5
   \texttt{netperf -H 192.168.2.15 -p 12001 -t TCP_STREAM -l 300 --m 1440 &}
   \texttt{netperf -H 192.168.2.15 -p 12002 -t TCP_STREAM -l 300 --m 1440 &}
   ##Load generator 6
   \texttt{netperf -H 192.168.2.16 -p 12001 -t TCP_STREAM -l 300 --m 1440 &}
   \texttt{netperf -H 192.168.2.16 -p 12002 -t TCP_STREAM -l 300 --m 1440 &}
   ##Load generator 7
   \texttt{netperf -H 192.168.2.17 -p 12001 -t TCP_STREAM -l 300 --m 1440 &}
   \texttt{netperf -H 192.168.2.17 -p 12002 -t TCP_STREAM -l 300 --m 1440 &}
## Load generator 8
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.
   ## Load generator 1
   netserver -p 12001
   netserver -p 12002
   ## Load generator 2
   netserver -p 12003
   netserver -p 12004
   ## Load generator 3
   netserver -p 12005
   netserver -p 12006
   ## Load generator 4
   netserver -p 12007
   netserver -p 12008
   ## Load generator 5
   netserver -p 12009
   netserver -p 12010
   ## Load generator 6
   netserver -p 12011
   netserver -p 12012
   ## Load generator 7
   netserver -p 12013
   netserver -p 12014
   ## Load generator 8
   netserver -p 12015
   netserver -p 12016

2. Start the netperf process on all load generators.
   Load generator 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 &
   Load generator 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 &
   Load generator 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 &
   Load generator 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 &
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 15-4. The final result is the sum of the test results of the netperf processes on all TX ends.

**Figure 15-4** Output of the netperf process on one TX end

<table>
<thead>
<tr>
<th>recv</th>
<th>send</th>
<th>send</th>
</tr>
</thead>
<tbody>
<tr>
<td>socket</td>
<td>socket</td>
<td>message</td>
</tr>
<tr>
<td>size</td>
<td>size</td>
<td>size</td>
</tr>
<tr>
<td>bytes</td>
<td>bytes</td>
<td>bytes</td>
</tr>
</tbody>
</table>

![TX buffer][Test duration][Throughput](87380 16384 1440 120.02 956.30)

**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 load generators to start the server process:
   
   `iperf3 -s -p 12001 &`
   
   `iperf3 -s -p 12002 &`
In the preceding commands, \texttt{-p} specifies the listening port.

2. Start the client process on the tested ECS. For details about common iperf3 parameters, see Table 15-8.

\texttt{##Load generator 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 &

\texttt{##Load generator 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 &

\texttt{##Load generator 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 &

\texttt{##Load generator 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 &

\texttt{##Load generator 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 &

\texttt{##Load generator 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 &

\texttt{##Load generator 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 &

\texttt{##Load generator 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 &

\texttt{Step 2} Test the UDP RX PPS.

1. Start the server process on the tested ECS. For details about common iperf3 parameters, see Table 15-8.

\texttt{##Load generator 1}
iperf3 -s -p 12001 -A 0 -i 60 &
iperf3 -s -p 12002 -A 1 -i 60 &

\texttt{##Load generator 2}
iperf3 -s -p 12003 -A 2 -i 60 &
iperf3 -s -p 12004 -A 3 -i 60 &

\texttt{##Load generator 3}
iperf3 -s -p 12005 -A 4 -i 60 &
iperf3 -s -p 12006 -A 5 -i 60 &

\texttt{##Load generator 4}
iperf3 -s -p 12007 -A 6 -i 60 &
iperf3 -s -p 12008 -A 7 -i 60 &
Step 3  Analyze the test result.

Figure 15-5 shows an example of the UDP PPS test result.
Latency Test

**Step 1** Run the following command to start the qperf process on the tested ECS:

```
qperf &
```

**Step 2** Log in to load generator 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

15.8 Disk FAQs

15.8.1 Can Multiple Disks Be Attached to an ECS?

Yes. Up to 24 EVS disks, including the system disk, can be attached to an ECS. A large-memory ECS can be attached with up to 40 EVS disks, including the system disk.

**NOTE**

The total number of EVS disks and NICs attached to an ECS is suggested not to be greater than 25. Otherwise, disks may fail to be attached to the ECS.

15.8.2 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.

15.8.3 What Are the Restrictions for Attaching an EVS Disk to an ECS?

- The EVS disk and the target ECS must be located in the same AZ.
- For a non-shared disk, the EVS disk must be in Available state. For a shared disk, the target ECS must be in In-use or Available state.
- The target ECS must be in Running or Stopped state.
- A frozen EVS disk cannot be attached to an ECS.
- A SCSI EVS disk cannot be used as an ECS system disk.
- Certain ECSs support SCSI EVS disk attachment. For details, see section 15.8.2 Which ECSs Can Be Attached with SCSI EVS Disks?

15.8.4 How Can I Adjust System Disk Partitions?

Scenarios

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

There are two ways to expand a system disk:

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

Procedure

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

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

**Step 1** View disk partitions.

1. Log in to the ECS.
2. Run the following command to switch to user root:
   ```bash
   sudo su -
   ```
3. Run the following command to view ECS disk details:
   ```bash
   fdisk -1
   ```
   In the following command output, /dev/xvda or /dev/vda indicates the system disk.
4. Run the following command to view disk partitions:

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

![Parted output](image)

**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:

```
Number Start  End   Size Type       File system Flags
 1 1049kB 11kB  10.9GB primary  ext4        boot
 2 42.9GB 43.9GB 2000MB primary  linux–swap(v1)
```
3. Enter the new partition's start cylinder number and press **Enter**.

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

```
First sector (00000000-125029119, default 00000000): 030006000
Using default value 030006000
Last sector, +sectors or +size(K,M,G) (00000000-125029119, default 125029119):
Using default value 125029119
Partition 3 of type Linux and of size 20 GiB is set
```

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

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

```
Last sector, +sectors or +size(K,M,G) (00000000-125029119, default 125029119):
Using default value 125029119
Partition 3 of type Linux and of size 20 GiB is set
```

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

Information similar to the following is displayed.

```
Command (m for help): p

Disk /dev/xda: 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: 0x8000a45e

Device Boot Start   End     Blocks  Id  System
/dev/xda1   2048 79988543  39999246  83  Linux
/dev/xda2 79988644 83886879  1952768  82  Linux swap / Solaris
/dev/xda3 030006000 125029119 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.
7. Run the following command to view disk partitions:

   `parted -l /dev/xvda`

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

   `partprobe`

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

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

   `df -TH`

   ![Disk Flags](image)

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:
```

---

2018-10-30 227
Step 5  Mount the new partition to the target directory.

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

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

1. Run the following command to create the `/root/new` directory:
   ```bash
   mkdir /root/new
   ```
2. Run the following command to mount the new partition to the `/root/new` directory:
   ```bash
   mount /dev/xvda3 /root/new
   ```
   Information similar to the following is displayed:
   ```bash
   [root@ecs-86dc ]# mount /dev/xvda3 /root/new
   [root@ecs-86dc ]#
   ```
3. Run the following command to view the mounted file systems:
   ```bash
   df -TH
   ```
   Information similar to the following is displayed:
   ```bash
   [root@ecs-86dc ]# df -TH
   Filesystem Type  Size  Used  Avail  %Mnted on
   /dev/xvda1  ext4  41G  1.3G  37G  3% /dev
   devtmpfs  devtmpfs  943M  0  943M  0% /dev/shm
   tmpfs  tmpfs  952M  0  952M  0% /run
   tmpfs  tmpfs  952M  8.8M  944M  1% /run
   /dev/xvda3  ext4  22G  17M  20G  1% /root/new
   tmpfs  tmpfs  191M  0  191M  0% /run/user/0
   ```

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

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

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

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

---

**NOTICE**

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

```bash
blkid
```

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

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

```bash
vi /etc/fstab
```

3. Press `i` to enter editing mode.

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

```bash
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.

```bash
:wq
```

---End

### 15.8.5 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`

   ```plaintext
   [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
   ```

<table>
<thead>
<tr>
<th>Number</th>
<th>Start</th>
<th>End</th>
<th>Size</th>
<th>Type</th>
<th>File system</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1049kB</td>
<td>4296MB</td>
<td>4295MB</td>
<td>primary</td>
<td>linux-swap(v1)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4296MB</td>
<td>53.7GB</td>
<td>49.4GB</td>
<td>primary</td>
<td>ext4</td>
<td>boot</td>
</tr>
</tbody>
</table>

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

   `blkid`

   ```plaintext
   /dev/xvda1: UUID="25ec3bcb-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-utils-growpart` command to ensure it is available.

4. Run the following command to expand the root partition (the second partition) using
   `growpart`:

   ```plaintext
   growpart /dev/xvda 2
   ```

   ```plaintext
   [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`

   ```plaintext
   [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
   ```

<table>
<thead>
<tr>
<th>Number</th>
<th>Start</th>
<th>End</th>
<th>Size</th>
<th>Type</th>
<th>File system</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1049kB</td>
<td>4296MB</td>
<td>4295MB</td>
<td>primary</td>
<td>linux-swap(v1)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4296MB</td>
<td>53.7GB</td>
<td>49.4GB</td>
<td>primary</td>
<td>ext4</td>
<td>boot</td>
</tr>
</tbody>
</table>

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:

   ```plaintext
   [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
   ```
15.8.6 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:
   
   ```bash
   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:
      
      ```bash
      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.
      
      ```bash
      vi /etc/fstab
      ```
      
      ```bash
      tail -n 3 /etc/fstab
      ```
      
      ```bash
      [root@sluo-ecs-a611 ~]# vi /etc/fstab
      ```
      
      ```bash
      [root@sluo-ecs-a611 ~]# tail -n 3 /etc/fstab
      ```
      
      ```bash
      # UUID=7c4fce5d-f8f7-4ed6-8463-f2bd22d0ddea /                       ext4
      defaults        1 1
      ```

3. Run the following command to disable the swap partition:
   
   ```bash
   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
   mklable,mktabe 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:

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

   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
### FAQs

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Elastic Cloud Server User Guide</td>
</tr>
</tbody>
</table>

**Partition Table: msdos**

**Disk Flags:**

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

**System Information:**

- Run the following command to edit the fstab partition table:
  
  ```
  (parted) quit
  Information: You may need to update /etc/fstab.
  ```

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

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

Model: Xen Virtual Block Device (xvd)

Disk /dev/xvda: 107GB

Sector size (logical/physical): 512B/512B

Partition Table: msdos

**Disk Flags:**

<table>
<thead>
<tr>
<th>Number</th>
<th>Start</th>
<th>End</th>
<th>Size</th>
<th>Type</th>
<th>File system</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1049kB</td>
<td>107GB</td>
<td>107GB</td>
<td>primary</td>
<td>ext4</td>
<td>boot</td>
</tr>
</tbody>
</table>

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

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

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

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

8. Run the following command to verify that online capacity expansion is successful:

```bash
(parted) quit
```

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

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

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

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

```bash
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
```
15.8.7 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Windows ECS?

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

1. Log in to the Windows ECS.
2. Click Start in the lower left corner of the desktop.
4. In the navigation pane on the left, choose Storage > Disk Management.

Figure 15-6 Disk Management

5. Taking disk 1 marked in Figure 15-6 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 15-6.
   b. Click Properties.
      The SCSI Disk Device Properties dialog box is displayed, as shown in Figure 15-7.
c. Click the Details tab and set Property to Parent.

**Figure 15-8 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 15-11.

The disk device corresponding to 51776 is xvde. The disk device used by disk 1 is xvde.
### Table 15-11 Mapping between disk partitions and disk devices

<table>
<thead>
<tr>
<th>Master and Slave Device Number for a Disk Partition</th>
<th>Disk Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>51712</td>
<td>xvda</td>
</tr>
<tr>
<td>51728</td>
<td>xvdb</td>
</tr>
<tr>
<td>51744</td>
<td>xvdc</td>
</tr>
<tr>
<td>51760</td>
<td>xvdd</td>
</tr>
<tr>
<td>51776</td>
<td>xvde</td>
</tr>
<tr>
<td>51792</td>
<td>xvdf</td>
</tr>
<tr>
<td>51808</td>
<td>xvdg</td>
</tr>
<tr>
<td>51824</td>
<td>xvdh</td>
</tr>
<tr>
<td>51840</td>
<td>xvdI</td>
</tr>
<tr>
<td>51856</td>
<td>xvdj</td>
</tr>
<tr>
<td>51872</td>
<td>xvdk</td>
</tr>
<tr>
<td>51888</td>
<td>xvdI</td>
</tr>
<tr>
<td>51904</td>
<td>xvdm</td>
</tr>
<tr>
<td>51920</td>
<td>xvdn</td>
</tr>
<tr>
<td>51936</td>
<td>xvdo</td>
</tr>
<tr>
<td>51952</td>
<td>xvdp</td>
</tr>
<tr>
<td>268439552</td>
<td>xvdq</td>
</tr>
<tr>
<td>268439808</td>
<td>xvdr</td>
</tr>
<tr>
<td>268440064</td>
<td>xvds</td>
</tr>
<tr>
<td>268440320</td>
<td>xvdI</td>
</tr>
<tr>
<td>268440576</td>
<td>xvdu</td>
</tr>
<tr>
<td>268440832</td>
<td>xvdv</td>
</tr>
<tr>
<td>268441088</td>
<td>xvdw</td>
</tr>
<tr>
<td>268441344</td>
<td>xvdx</td>
</tr>
</tbody>
</table>

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

For a Linux ECS, its disk partitions correspond to disk devices. This section uses a Linux ECS running Red Hat Enterprise Linux 7 as an example to describe how to obtain the mapping between disk partitions and disk devices.
1. Log in to the Linux ECS as user **root**.
2. Right-click in the blank area of the desktop and choose **Open Terminal** from the shortcut menu.

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

   ```bash
   fdisk -l
   ```

   ![Applications, Places, New Folder, Paste, Select All, Keep aligned, Organize Desktop by Name, Change Background, Open Terminal]

   Table 15-12 lists the mapping between disk partitions and disk devices.

   **Table 15-12** Mapping between disk partitions and disk devices

<table>
<thead>
<tr>
<th>Disk Partition</th>
<th>Disk Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>xvda</td>
<td>xvda</td>
</tr>
<tr>
<td>xvdb</td>
<td>xvdb</td>
</tr>
<tr>
<td>xvdc</td>
<td>xvdc</td>
</tr>
<tr>
<td>xvdd</td>
<td>xvdd</td>
</tr>
<tr>
<td>xvde</td>
<td>xvde</td>
</tr>
<tr>
<td>xvdf</td>
<td>xvdf</td>
</tr>
</tbody>
</table>
15.8.9 Who Can Use the Encryption Feature?

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

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

The following section uses a user group as an example to describe how to grant KMS access rights to EVS for using the encryption feature.
For example, a user group shown in Figure 15-9 consists of four users, user 1 to user 4. User 1 has security administrator rights. Users 2, 3, and 4 are common users who do not have security administrator rights.

**Figure 15-9 User group**

![User group diagram](image)

**Scenario 1: User 1 Uses the Encryption Feature**

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

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

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

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

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

**Scenario 2: Common User Uses the Encryption Feature**

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

1. When user 3 uses the encryption feature, the system displays a message indicating that the user has no rights.
2. User 3 asks user 1 to create Xrole to grant KMS access rights to EVS.
After the rights are granted, user 3 and all other users in the user group can use the encryption feature, without requiring to contact user 1 for rights granting.

15.9 OS FAQs

15.9.1 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.

15.9.2 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 section 3.2.2 Changing the OS.

15.9.3 Is a GUI Provided for OSs?

Windows ECSs are managed through a GUI but Linux ECSs are managed through the CLI. You can configure a GUI if required.

15.9.4 Is the FTP Upload Tool Included in the OS?

No. The FTP upload tool must be installed and configured by the user.

15.9.5 Can I Select Other OSs 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 section 3.2.2 Changing the OS.

15.9.6 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 and Yes and click OK to forcibly stop the original ECS.

Manually refresh the Elastic Cloud Server page. The original ECS is stopped once the Status changes to Stopped.
NOTE
The ECSs running certain OSs support online data disk detaching. If your OS supports this feature, you can detach data disks from the running ECS.

3. Click to view information about the data disks attached to the original ECS.

NOTE
If the original ECS has multiple data disks attached, repeat steps 4 to 6 to attach each data disk to the new ECS.

4. Click a data disk.

The Elastic Volume Service page is displayed.

5. Select the data disk to be detached and click Detach in the Operation column. On the Detach Disk page, select the original ECS and click OK to detach the data disk from the original ECS.

Manually refresh the Elastic Volume Service page. The data disk is detached from the original ECS once the Status changes to Available.

6. Select the detached data disk and click Attach in the Operation column. On the Attach Disk page, click the new ECS, select a device name, and click OK to attach the data disk to the new ECS.

Manually refresh the EVS list. The data disk is attached to the new ECS once the Status value changes to In-use. You can then log in to the management console and view information about the data disk of the new ECS.

15.9.7 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:
   
   ```bash
   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`:
   
   ```bash
   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.
15.9.8 Why Is the Memory of an ECS Obtained by Running the free Command Inconsistent with the Actual Memory?

Symptom

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

An example is provided as follows:

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

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

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

Run the `dmidecode -t memory` command to check the actual memory configured for the ECS. The command output is as follows:

```
[root@localhost ~]# dmidecode -t memory
# dmidecode 3.0
Getting SMBIOS data from sysfs.
SMBIOS 2.8 present.
Handle 0x1000, DMI type 16, 23 bytes
Physical Memory Array
Location: Other
Use: System Memory
Error Correction Type: Multi-bit ECC
Maximum Capacity: 4 GB
Error Information Handle: Not Provided
Number Of Devices: 1

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

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

### Possible Causes

When the OS is started, related devices are initialized, which occupies memory. In addition, when the kernel is started, it also occupies memory. The memory occupied by the kernel 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.

---

### 15.9.9 How to configure the SUSE repository?

#### Symptom

Before installing a patch on an ECS using the SUSE image, ensure that the `/etc/resolv.conf` file of the DNS server contains the following records so that the patch server provided by the public cloud platform can be used:

```
nameserver 100.125.1.22
nameserver 8.8.8.8
```

#### Procedure

**Step 1** Client VM installs the SMT Server Certificate.

1. Configure the local DNS hosts.
   
   `vi /etc/hosts`

   `100.125.1.19 SMT.suse`

2. Download the clientSetup4SMT.sh file from SMT server.
wget http://SMT.suse/repo/tools/clientSetup4SMT.sh
chmod 755 clientSetup4SMT.sh

3. Trust and Register the SMT Server certificate.
   `./clientSetup4SMT.sh --host SMT.suse`

   **SUSE 11 SP4**

   ```
   ecs-suse114:/home/linux # ./clientSetup4SMT.sh --host SMT.suse
   Certificate:
   Data:
   
   Version: 3 (0x2)
   Signature Algorithm: sha256WithRSAEncryption
   Issuer: C=MX, ST=Local, L=Local, O=Telefonica, OU=Public Cloud,
   CN=YaST_Default_CA/emailAddress=tcsfcloud@xxx.com
   Validity
   Not Before: Nov 15 23:51:51 2017 GMT
   Not After : Nov 13 23:51:51 2027 GMT
   Subject: C=MX, ST=Local, L=Local, O=Telefonica, OU=Public Cloud,
   CN=YaST_Default_CA/emailAddress=tcsfcloud@xxx.com
   Subject Public Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (2048 bit)
   Modulus (2048 bit):
   d6:ef

   Exponent: 65537 (0x10001)
   X509v3 extensions:
   X509v3 Basic Constraints: critical
   CA:TRUE
   Netscape Comment:
   YaST Generated CA Certificate
   Netscape Cert Type:
   SSL CA, S/MIME CA
   X509v3 Key Usage:
   Certificate Sign, CRL Sign
   X509v3 Subject Key Identifier:
   X509v3 Authority Key Identifier:
   ```
DirName:/C=MX/ST=Local/L=Local/O=Telefonica/OU=Public Cloud/CN=YaST_Default_CA/emailAddress=tefcloud@xxx.com
X509v3 Subject Alternative Name:
  email:tefcloud@xxx.com
X509v3 Issuer Alternative Name:
  email:tefcloud@xxx.com
Signature Algorithm: sha256WithRSAEncryption
65:86:d9:0b
Do you accept this certificate? [y/n] y
Client setup finished.
Start the registration now? [y/n] y
/usr/bin/suse_register -i -L /root/.suse_register.log
All services have been refreshed.
Repository 'SUSE-Linux-Enterprise-Server-11-SP4 11.4.4-1.109' is up to date.
All repositories have been refreshed.
Refreshing service 'SMT-http_SMT_suse'.
Adding repository 'SLE11-SP4-Debuginfo-Updates' [done]
Adding repository 'SLE11-SP4-Debuginfo-Pool' [done]
Adding repository 'SLES11-SP4-Updates' [done]
Adding repository 'SLES11-SP4-Pool' [done]
All services have been refreshed.
Retrieving repository 'SLES11-SP4-Pool' metadata [done]
Building repository 'SLES11-SP4-Pool' cache [done]
Retrieving repository 'SLES11-SP4-Updates' metadata [done]
Building repository 'SLES11-SP4-Updates' cache [done]
Repository 'SUSE-Linux-Enterprise-Server-11-SP4 11.4.4-1.109' is up to date.
All repositories have been refreshed.
Registration finished successfully

- SUSE 12 SP1

ecs-suse121:/home/linux # ./clientSetup4SMT.sh --host SMT.suse
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 10420693902693132962 (0x9093abe4a6a6a2)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=MX, ST=Local, L=Local, O=Telefonica, OU=Public Cloud,
    CN=YaST_Default_CA/emailAddress=tefcloud@xxx.com
    Validity
Not Before: Nov 15 23:51:51 2017 GMT
Not After : Nov 13 23:51:51 2027 GMT
Subject: C=MX, ST=Local, L=Local, O=Telefonica, OU=Public Cloud, CN=YaST_Default_CA/emailAddress=tefcloud@xxx.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:c9:30:9b:ff:68:c0:ae:74:11:7c:03:c2:25:6a:
95:0e:2c:9b:1e:5e:8a:3d:2d:8f:5e:cc:13:bb:9b:
a2:00:59:dd:87:af:9d:5f:43:4e:4c:9e:2:03:a3:
57:bd:00:6e:0c:2c:92:57:07:33:86:ae:81:6b:10:
f7:ca:e5:6d:8b:e5:95:0d:8b:ff:a8:71:9a:3d:11:
67:31:75:qi:00:aa:8b:06:dd:0c:5f:10:4c:28:89:
d6:ef
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE
Netscape Comment:
YaST Generated CA Certificate
Netscape Cert Type:
SSL CA, S/MIME CA
X509v3 Key Usage:
Certificate Sign, CRL Sign
X509v3 Subject Key Identifier:
X509v3 Authority Key Identifier:
DirName:/C=MX/ST=Local/L=Local/O=Telefonica/O=Public Cloud/CN=YaST_Default_CA/emailAddress=tefcloud@xxx.com
X509v3 Subject Alternative Name:
email:tefcloud@xxx.com
X509v3 Issuer Alternative Name:
email:tefcloud@xxx.com
Signature Algorithm: sha256WithRSAEncryption
94:2e:76:9f:61:0e:26:61:0e:0f:00:06:69:ff:8e:52:ff:fc:3:4b:
Step 2  Confirm the correction of the repositories.

zypper update

If the system feedback the information like the following, that means the new repositories have worked, please CTRL+C to cancel the update.

- **SUSE 11 SP4**

- **SUSE 12 SP1**

----End
15.9.10 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.

![Performance Options](image)

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 15-12 Virtual Memory**

7. Click **Set** and then **OK** to complete the configuration.
8. Restart the ECS for the configuration to take effect.

### 15.9.11 How Can I Handle Strange Routes and IP Addresses on an ECS?

**Symptom**

Strange CentOS 7.0 installation table route
Strange Ubuntu 16.04 installation table route

Strange Debian 8.6 installation table route

Strange SUSE 11 installation table route

Root Cause

They are not errors or bugs, but are normal cases.

IP address 169.254.169.254 is used by the Cloud-Init software in OpenCloud, Amazon EC2, and others cloud computing platforms to distribute metadata to ECSs.

In a preview CloudServers version, disabling DHCP caused service failures. For example, user authentication failed.

Using IP address 169.254.169.254, OpenStack shows information, such as SSH public keys, users data, or MAC addresses.

Examples are as follows:

- Show all metadata:
  
Show an SSH public key:

```
```

Show a hostname:

```
root@linux:/home# curl http://169.254.169.254/latest/meta-data/public-hostname
```

### 15.9.12 How Can I Change the Patch Update Source of an ECS Running a Windows Server OS to an Official Microsoft Patch Server?

**Scenarios**

The patch update source of an ECS running a Windows Server OS must be changed to an official Microsoft patch server.

**Constraints**

The target ECS must be able to access the Internet, for example, by binding an EIP or using NAT mapping so that the ECS can access the official Microsoft Windows update server.

**Procedure**

1. Log in to the ECS.
2. Open the Run dialog box and enter `gpedit.msc` to start Local Group Policy Editor.
4. Modify **Configure Automatic Updates** and **Specify intranet Microsoft update service location**.
   - Modify **Configure Automatic Updates**.
     i. Double-click **Configure Automatic Updates**.
     ii. Set **Configure Automatic Updates** to **Enabled**.
     iii. Set **Configure automatic updating** to **2-Notify for download and notify for install**.

**NOTE**

You can also select other updates options as required.
Figure 15-14 Modifying Configure Automatic Updates

- Modify Specify intranet Microsoft update service location.
  - iv. Double-click Specify intranet Microsoft update service location.
  - v. Set Specify intranet Microsoft update service location to Not configured.
5. Start **cmd** or **PowerShell** as an administrator and run the following command for the modifications to take effect:

```
gpupdate /force
```

**Figure 15-16** Command to make the modifications take effect
15.10 Database FAQs

15.10.1 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.

15.10.2 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.
<table>
<thead>
<tr>
<th>Released On</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2018-10-30   | This issue is the twenty-second official release, which incorporates the following changes:  

  * Added the following content:  
    * 15.3.1 Why Cannot I Use the Spanish Keyboard to Enter Characters After I Log In to an ECS Using VNC?  
    * 15.3.2 Why Cannot I Use the Portuguese Keyboard to Enter Characters After I Log In to an ECS Using VNC?  

| 2018-09-30   | This issue is the twenty-first official release, which incorporates the following changes:  

  * Modified the following content:  
    * Modified description in section 3.3 Managing ECS Groups, allowing you to add a created ECS to an ECS group or remove it from an ECS group.  

| 2018-08-30   | This issue is the twentieth official release, which incorporates the following changes:  

  * Added the following content:  
    * 3.10 Quotas  

  * Modified the following content:  
    * Added the procedure for restarting the ECS in section 15.9.10 How Can I Enable Virtual Memory on a Windows ECS?  

| 2018-07-30   | This issue is the nineteenth official release, which incorporates the following changes:  

  * Added the following content:  
    * Added E3 ECS specifications in section 1.7.6 Large-Memory ECSs.  
    * 3.10 Quotas  
    * 5.1 Changing the Initial Password for Logging In to an ECS  
    * 6.1.2 Changing a XEN ECS to a KVM ECS (Windows)  
    * 6.1.3 Changing a XEN ECS to a KVM ECS (Linux)  
    * 14.13 What Should I Do If Cloud-Init Does Not Work After Python Is Upgraded?
## Change History

### 2018-06-30
This issue is the eighteenth official release, which incorporates the following changes:

- Added the following content:
  - 15.7.5 How Can I Test Network Performance?
  - 15.4.3 What Should I Do If an Authentication Failure Occurs After I Attempt to Remotely Log In to a Windows ECS?

- Modified the following content:
  - Allowed to export certain ECSs in section 3.1.4 Exporting ECSs.
  - Modified prerequisites in section 3.2.2 Changing the OS, allowing you to change the OS of an ECS on which reinstalling the OS failed.

### 2018-05-30
This issue is the seventeenth official release, which incorporates the following changes:

- Added the following content:
  - 14.9 What Should I Do When a Disk Goes Offline?
  - 14.12 How Can I Handle Slow ECS Startup?

- Modified the following content:
  - Modified description in sections 2.1 Creating and Logging In to a Windows ECS and 2.2 Creating and Logging In to a Linux ECS, allowing you to specify NIC IP addresses when creating multiple ECSs in a batch.
  - Modified ECS naming rules in sections 2.1 Creating and Logging In to a Windows ECS and 2.2 Creating and Logging In to a Linux ECS.
  - Changed the method of selecting ECS specifications in sections 2.1 Creating and Logging In to a Windows ECS and 2.2 Creating and
### Change History

<table>
<thead>
<tr>
<th>Released On</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Logging In to a Linux ECS.</strong></td>
</tr>
<tr>
<td></td>
<td>- Modified the description of <strong>local-ipv4</strong> and <strong>public-ipv4</strong> in section 3.4.1 Managing ECS Metadata.</td>
</tr>
<tr>
<td></td>
<td>- Added introduction to user data scripts in section 3.4.2 Injecting User Data into ECSs.</td>
</tr>
<tr>
<td>2018-04-30</td>
<td>This issue is the sixteenth official release, which incorporates the following changes:</td>
</tr>
<tr>
<td></td>
<td>Added the following content:</td>
</tr>
<tr>
<td></td>
<td>- 3.5 Creating an Image</td>
</tr>
<tr>
<td></td>
<td>- 3.1.2 Viewing Failures</td>
</tr>
<tr>
<td></td>
<td>- 14.7 What Should I Do If Error “command ‘gcc’ failed with exit status 1” Occurs During PIP-based Software Installation</td>
</tr>
<tr>
<td></td>
<td>- 14.8 What Should I Do If Packages Are Downloaded Using PIP or wget at a Low Rate?</td>
</tr>
<tr>
<td></td>
<td>- 15.7.4 How Can I View and Modify Kernel Parameters of a Linux ECS?</td>
</tr>
<tr>
<td></td>
<td>Modified the following content:</td>
</tr>
<tr>
<td></td>
<td>- Added the description that data can be copied and pasted on VNC pages in section 4.2.4 Login Using VNC.</td>
</tr>
<tr>
<td></td>
<td>- Added the method of checking whether specifications have been modified in section 6.1.1 General Operations for Modifying Specifications.</td>
</tr>
<tr>
<td></td>
<td>- Added the description that KVM ECSs can be automatically recovered in section 3.6 Automatically Recovering ECSs.</td>
</tr>
<tr>
<td>2018-03-30</td>
<td>This issue is the fifteenth official release, which incorporates the following changes:</td>
</tr>
<tr>
<td></td>
<td>Added the following content:</td>
</tr>
<tr>
<td></td>
<td>- 15.4.5 How Can I Log In to an ECS After Its System Disk Is Exchanged with That Attached to Another ECS Running the Same OS?</td>
</tr>
<tr>
<td></td>
<td>Modified the following content:</td>
</tr>
<tr>
<td></td>
<td>- 15.6.4 Why Can I Remotely Access an ECS But Cannot Ping It?</td>
</tr>
<tr>
<td>2018-01-30</td>
<td>This issue is the fourteenth official release, which incorporates the following changes:</td>
</tr>
<tr>
<td></td>
<td>Added the following content:</td>
</tr>
<tr>
<td></td>
<td>- 15.9.9 How to configure the SUSE repository?</td>
</tr>
<tr>
<td></td>
<td>- 14.3 What Can I Do If Switching from a Non-root User to User root Times Out?</td>
</tr>
<tr>
<td></td>
<td>Modified the following content:</td>
</tr>
<tr>
<td></td>
<td>- 15.8.1 Can Multiple Disks Be Attached to an ECS?</td>
</tr>
<tr>
<td></td>
<td>- Modified the method of selecting the ECS type in sections 2.1 Creating and Logging In to a Windows ECS and 2.2 Creating and Logging In to a Linux ECS.</td>
</tr>
<tr>
<td>Released On</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>• Added &quot;Follow-up Procedure&quot; in section 6.1.1 General Operations for Modifying Specifications.</td>
</tr>
<tr>
<td></td>
<td>• The system does not create built-in tags any longer in section 12 Tags.</td>
</tr>
<tr>
<td>2017-11-30</td>
<td>This issue is the thirteenth official release, which incorporates the following changes:</td>
</tr>
<tr>
<td></td>
<td>Added the following content:</td>
</tr>
<tr>
<td></td>
<td>• 14.4 What Should I Do If a Linux ECS with a SCSI Disk Attached Fails to Restart?</td>
</tr>
<tr>
<td></td>
<td>• 15.8.7 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Windows ECS?</td>
</tr>
<tr>
<td></td>
<td>• 15.8.8 How Can I Obtain the Mapping Between Disk Partitions and Disk Devices on a Linux ECS?</td>
</tr>
<tr>
<td></td>
<td>Modified the following content:</td>
</tr>
<tr>
<td></td>
<td>• Added the description that users must use BYOL when they create ECSs on DeHs.</td>
</tr>
<tr>
<td></td>
<td>• Added case 3 in section 3.4.2 Injecting User Data into ECSs.</td>
</tr>
<tr>
<td></td>
<td>• Added case 3 in section 3.4.3 Injecting Files into ECSs.</td>
</tr>
<tr>
<td></td>
<td>• Added the Xshell-based ECS login method in section 4.2.2 Login Using an SSH Key.</td>
</tr>
<tr>
<td></td>
<td>• Added the description of Ivm in section 5.2.3 Resetting the Password for Logging In to a Linux ECS.</td>
</tr>
<tr>
<td></td>
<td>• Added a list in section 11.2 ECS Metrics.</td>
</tr>
<tr>
<td></td>
<td>• 15.8.3 What Are the Restrictions for Attaching an EVS Disk to an ECS?</td>
</tr>
<tr>
<td>2017-09-30</td>
<td>This issue is the twelfth official release, which incorporates the following changes:</td>
</tr>
<tr>
<td></td>
<td>Added the following content:</td>
</tr>
<tr>
<td></td>
<td>• Added ECS groups in section 3.3 Managing ECS Groups.</td>
</tr>
<tr>
<td></td>
<td>• 3.9 (Optional) Configuring Mapping Between Hostnames and IP Addresses</td>
</tr>
<tr>
<td></td>
<td>• 3.7 Obtaining ECS Console Logs</td>
</tr>
<tr>
<td></td>
<td>• 15.9.7 How Can I Set the Validity Period of the Image Password?</td>
</tr>
<tr>
<td></td>
<td>• 15.5.1 How Can I Obtain the Key Pair Used by an ECS?</td>
</tr>
<tr>
<td></td>
<td>• 15.4.2 What Should I Do If I Cannot Log In to an ECS with Cloud-Init Enabled?</td>
</tr>
<tr>
<td></td>
<td>• 15.8.4 How Can I Adjust System Disk Partitions?</td>
</tr>
<tr>
<td></td>
<td>• 15.8.5 How Can I Add the Empty Partition of an Expanded System Disk to the End Root Partition Online?</td>
</tr>
<tr>
<td></td>
<td>• 15.8.6 How Can I Add the Empty Partition of an Expanded System Disk to the Non-end Root Partition Online?</td>
</tr>
<tr>
<td></td>
<td>• Supported encrypted images and EVS disks.</td>
</tr>
<tr>
<td></td>
<td>• Supported high I/O (performance-optimized I) and ultra-high I/O</td>
</tr>
<tr>
<td>Released On</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>(latency optimization) EVS disks. Modified the following content:</td>
</tr>
<tr>
<td></td>
<td>- Added user data injection in section 3.2.1 Reinstalling the OS.</td>
</tr>
<tr>
<td></td>
<td>- Added user data injection in section 3.2.2 Changing the OS.</td>
</tr>
<tr>
<td></td>
<td>- Added the description of managing virtual IP addresses in section 6.1.1 General Operations for Modifying Specifications.</td>
</tr>
<tr>
<td></td>
<td>- Added examples for configuring routing policies in section 15.6.1 Can Multiple EIPs Be Bound to an ECS?</td>
</tr>
<tr>
<td></td>
<td>- Added constraints in section 7.2 Detaching an EVS Disk from a Running ECS.</td>
</tr>
<tr>
<td>2017-08-30</td>
<td>This issue is the eleventh official release, which incorporates the following changes: Added the following content:</td>
</tr>
<tr>
<td></td>
<td>- Added the multi-project feature.</td>
</tr>
<tr>
<td></td>
<td>- 3.6 Automatically Recovering ECSs</td>
</tr>
<tr>
<td></td>
<td>Modified the following content:</td>
</tr>
<tr>
<td></td>
<td>- Added the ECS product architecture in section 1.1 ECS.</td>
</tr>
<tr>
<td></td>
<td>- 15.8.3 What Are the Restrictions for Attaching an EVS Disk to an ECS?</td>
</tr>
<tr>
<td>2017-07-31</td>
<td>This issue is the tenth official release, which incorporates the following changes: Added the following content:</td>
</tr>
<tr>
<td></td>
<td>- Added the ECS automatic recovery function.</td>
</tr>
<tr>
<td>2017-07-12</td>
<td>This issue is the ninth official release, which incorporates the following changes: Added the following content:</td>
</tr>
<tr>
<td></td>
<td>- Added the function of using shared EVS disks as data disks.</td>
</tr>
<tr>
<td></td>
<td>- Added SCSI data disks.</td>
</tr>
<tr>
<td>2017-05-30</td>
<td>This issue is the eighth official release, which incorporates the following changes: Added the following content:</td>
</tr>
<tr>
<td></td>
<td>- Added large-memory ECSs.</td>
</tr>
<tr>
<td></td>
<td>Modified the following content:</td>
</tr>
<tr>
<td></td>
<td>- Added the description of adding, viewing, modifying, and deleting tags in section 6.1.1 General Operations for Modifying Specifications.</td>
</tr>
<tr>
<td>2017-04-28</td>
<td>This issue is the seventh official release, which incorporates the following changes: Added the following content:</td>
</tr>
<tr>
<td></td>
<td>- Supported adding tags to an ECS.</td>
</tr>
<tr>
<td></td>
<td>- Supported BYOL.</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>This issue is the sixth official release, which incorporates the following</td>
</tr>
<tr>
<td>Released On</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>changes: Added the following content: • Added the function of configuring multiple security groups for an ECS. • 15.2.3 How Can a Changed Static Hostname Take Effect Permanently?</td>
</tr>
<tr>
<td>2016-12-30</td>
<td>This issue is the fifth official release, which incorporates the following changes: Modified the following content: • Supported replacing a key pair when you reinstall or change an ECS OS. • Supported configuring security group rules when you initialize or access an ECS.</td>
</tr>
<tr>
<td>2016-11-30</td>
<td>This issue is the fourth official release, which incorporates the following changes: Added the following content: • ECS metadata</td>
</tr>
<tr>
<td>2016-10-29</td>
<td>This issue is the third official release, which incorporates the following changes: Added the following content: • GPU-optimized ECSs • Disk-intensive ECSs • High-performance ECSs • Cloud-Init Modified the following content: • ECS login modes</td>
</tr>
<tr>
<td>2016-07-15</td>
<td>This issue is the second official release, which incorporates the following changes: Added the following content: • Forcible ECS shutdown • Forcible ECS restarting • OS changing Modified the following content: • OS reinstallation</td>
</tr>
<tr>
<td>2016-03-30</td>
<td>This issue is the first official release.</td>
</tr>
</tbody>
</table>