

Image Management Service

User Guide

Issue 01
Date 2023-08-10



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

| | |
|---|----------|
| 1 Managing Public Images..... | 1 |
| 1.1 Overview..... | 1 |
| 1.2 Known Issues..... | 3 |
| 2 Creating a Private Image..... | 7 |
| 2.1 Introduction..... | 7 |
| 2.2 Creating a System Disk Image from a Windows ECS..... | 7 |
| 2.3 Creating a System Disk Image from a Linux ECS..... | 11 |
| 2.4 Creating a Windows System Disk Image from an External Image File..... | 14 |
| 2.4.1 Overview..... | 14 |
| 2.4.2 Preparing an Image File..... | 15 |
| 2.4.3 Uploading an External Image File..... | 18 |
| 2.4.4 Registering an External Image File as a Private Image..... | 18 |
| 2.4.5 Creating a Windows ECS from an Image..... | 21 |
| 2.5 Creating a Linux System Disk Image from an External Image File..... | 22 |
| 2.5.1 Overview..... | 22 |
| 2.5.2 Preparing an Image File..... | 22 |
| 2.5.3 Uploading an External Image File..... | 25 |
| 2.5.4 Registering an External Image File as a Private Image..... | 26 |
| 2.5.5 Creating a Linux ECS from an Image..... | 29 |
| 2.6 Creating a BMS System Disk Image..... | 29 |
| 2.7 Creating a Data Disk Image from an ECS..... | 30 |
| 2.8 Creating a Data Disk Image from an External Image File..... | 32 |
| 2.9 Creating a Full-ECS Image from an ECS..... | 34 |
| 2.10 Creating a Full-ECS Image from a CSBS Backup..... | 38 |
| 2.11 Creating a Full-ECS Image from a CBR Backup..... | 40 |
| 2.12 Creating a Windows System Disk Image from an ISO File..... | 42 |
| 2.12.1 Overview..... | 42 |
| 2.12.2 Integrating VirtIO Drivers into an ISO File..... | 44 |
| 2.12.3 Registering an ISO File as an ISO Image..... | 46 |
| 2.12.4 Creating a Windows ECS from an ISO Image..... | 48 |
| 2.12.5 Installing a Windows OS and VirtIO Drivers..... | 49 |
| 2.12.6 Configuring the ECS and Creating a Windows System Disk Image..... | 59 |
| 2.13 Creating a Linux System Disk Image from an ISO File..... | 60 |

| | |
|--|-----------|
| 2.13.1 Overview..... | 60 |
| 2.13.2 Registering an ISO File as an ISO Image..... | 62 |
| 2.13.3 Creating a Linux ECS from an ISO Image..... | 63 |
| 2.13.4 Installing a Linux OS..... | 64 |
| 2.13.5 Configuring the ECS and Creating a Linux System Disk Image..... | 69 |
| 2.14 Importing an Image..... | 70 |
| 2.15 Fast Import of an Image File..... | 71 |
| 2.15.1 Overview..... | 71 |
| 2.15.2 Fast Import in Linux..... | 74 |
| 2.15.3 Fast Import in Windows..... | 79 |
| 3 Managing Private Images..... | 82 |
| 3.1 Modifying an Image..... | 82 |
| 3.2 Exporting Image List..... | 84 |
| 3.3 Checking the Disk Capacity of an Image..... | 84 |
| 3.4 Creating an ECS from an Image..... | 86 |
| 3.5 Deleting Images..... | 86 |
| 3.6 Sharing Images..... | 87 |
| 3.6.1 Overview..... | 87 |
| 3.6.2 Obtaining the Project ID..... | 88 |
| 3.6.3 Sharing Specified Images..... | 88 |
| 3.6.4 Accepting or Rejecting Shared Images..... | 90 |
| 3.6.5 Rejecting Accepted Images..... | 92 |
| 3.6.6 Accepting Rejected Images..... | 93 |
| 3.6.7 Stopping Sharing Images..... | 93 |
| 3.6.8 Adding Tenants Who Can Use Shared Images..... | 94 |
| 3.6.9 Deleting Image Recipients Who Can Use Shared Images..... | 95 |
| 3.6.10 Replicating a Shared Image..... | 95 |
| 3.7 Exporting an Image..... | 96 |
| 3.8 Optimizing a Windows Private Image..... | 98 |
| 3.8.1 Optimization Process..... | 98 |
| 3.8.2 Viewing the Virtualization Type of a Windows ECS..... | 99 |
| 3.8.3 Obtaining Required Software Packages..... | 99 |
| 3.8.4 Installing PV Drivers..... | 100 |
| 3.8.5 Installing VirtIO Drivers..... | 103 |
| 3.8.6 Clearing System Logs..... | 108 |
| 3.9 Optimizing a Linux Private Image..... | 109 |
| 3.9.1 Optimization Process..... | 109 |
| 3.9.2 Checking Whether a Private Image Needs to be Optimized..... | 110 |
| 3.9.3 Uninstalling PV Drivers from a Linux ECS..... | 111 |
| 3.9.4 Changing the Disk Identifier in the GRUB Configuration File to UUID..... | 112 |
| 3.9.5 Changing the Disk Identifier in the fstab File to UUID..... | 116 |
| 3.9.6 Installing Native Xen and KVM Drivers..... | 117 |

| | |
|---|------------|
| 3.9.7 Installing Native KVM Drivers..... | 125 |
| 3.9.8 Clearing System Logs..... | 131 |
| 3.10 Encrypting Images..... | 132 |
| 3.10.1 Overview..... | 132 |
| 3.10.2 Creating Encrypted Images..... | 132 |
| 3.11 Replicating Images Within a Region..... | 133 |
| 3.12 Replicating Images Across Regions..... | 134 |
| 3.13 Tagging an Image..... | 138 |
| 3.14 Auditing Key Operations..... | 140 |
| 3.14.1 IMS Operations Recorded by CTS..... | 140 |
| 3.14.2 Viewing Traces..... | 141 |
| 4 Windows Operations..... | 144 |
| 4.1 Setting the NIC to DHCP..... | 144 |
| 4.2 Enabling Remote Desktop Connection..... | 146 |
| 4.3 Installing and Configuring Cloudbase-Init..... | 147 |
| 4.4 Running Sysprep..... | 153 |
| 4.5 Installing Special Windows Drivers..... | 155 |
| 5 Linux Operations..... | 157 |
| 5.1 Setting the NIC to DHCP..... | 157 |
| 5.2 Deleting Files from the Network Rule Directory..... | 159 |
| 5.3 Installing Cloud-Init..... | 161 |
| 5.4 Configuring Cloud-Init..... | 171 |
| 5.5 Detaching Data Disks from an ECS..... | 175 |
| 6 Permissions Management..... | 177 |
| 6.1 Creating a User and Granting Permissions..... | 177 |
| 6.2 Creating a Custom Policy..... | 179 |

1 Managing Public Images

1.1 Overview

Public images provided by Huawei Cloud can be used with ECSs or BMSs and come with a set of basic plug-ins preinstalled. These images are available to all users and cover most mainstream OSs. This section describes the types and characteristics of public images.

Public Image Types

Public images include Huawei-developed Huawei Cloud EulerOS and EulerOS images and third-party commercial images. Choose whichever public image best meeting your needs. If you have any OS issues, you can contact the OS vendor or go to the open-source community for technical support, but Huawei Cloud also provides technical assistance.

For more information, see [Differences Between openEuler, EulerOS, and Huawei Cloud EulerOS](#).

Table 1-1 Public image types

| Image Type | Description |
|----------------------|---|
| Huawei Cloud EulerOS | is an openEuler-based cloud operating system. offers cloud native, high-performing, secure, and easy-to-migrate capabilities. This accelerates service migration to the cloud and promotes application innovation. You can use to replace operating systems such as CentOS and EulerOS. |
| EulerOS | EulerOS is an enterprise-class commercial Linux distribution. It features high security, scalability, and performance, meeting customers' requirements for IT infrastructure and cloud computing services. NOTE EulerOS is internally used by Huawei and is not open source. |

| Image Type | Description |
|------------------------------|---|
| Third-party commercial image | Huawei Cloud rigorously tests, creates, and releases licensed third-party images that are highly secure and stable. Third-party public images include: Ubuntu and CentOS |

 NOTE

The available image OSs vary depending on server flavors:

- [OSs Supported by Different Types of ECSs](#)
- [OSs Supported by Different Types of BMSs](#)

Public Image Characteristics

- OS types: Linux OSs that are updated and maintained periodically
- Supported software: Public images contain some plug-ins on which server networks and basic functions depend.

 NOTE

The plug-ins that come with public images are necessary for ECSs or BMSs to run properly. Do not delete or modify any of them. Otherwise, basic functions of your ECSs or BMSs will be affected.

Table 1-2 Supported software

| Software | Description |
|---------------------------------|---|
| Cloud-Init or Cloudbase-Init | Cloud-Init is an open-source cloud initialization tool. It is essentially a series of Python scripts and components. When creating a cloud server using an image that has Cloud-Init installed, you can inject custom details (such as the login password for the cloud server). You can also query and use metadata to configure and manage cloud servers. By default, Cloud-Init is installed for Linux public images. |
| One-click password reset plugin | ECS and BMS provide a one-click password reset function. If you forget the password of your ECS or BMS, or the password expires, you can set a new password from the management console using the one-click password reset plug-in. This plug-in is installed for public images by default. |
| NIC multi-queue plug-in | NIC multi-queue enables multiple vCPUs to process NIC interrupts, thereby improving network PPS and I/O performance. For details about the public images that support NIC multi-queue, see How Do I Set NIC Multi-Queue for an Image? |

- Compatibility: Public images are compatible with different server hardware.
- Security: Public images are stable and licensed.

Differences Between openEuler, EulerOS, and Huawei Cloud EulerOS

- openEuler was initially developed by Huawei, but it was donated to the OpenAtom Foundation on November 9, 2021. Now, it is an open-source, free OS.
- EulerOS is a free enterprise-class Linux OS developed by Huawei. It will be replaced by Huawei Cloud EulerOS.
- Huawei Cloud EulerOS is developed based on openEuler. It was commercially released in 2022 and will replace CentOS and EulerOS. Currently, Huawei Cloud EulerOS images are free of charge.

1.2 Known Issues

This section describes known issues of public images. Private images also have these issues.

Network Disconnection Caused by a Windows Server DHCP Lease Longer Than 99 Days

Symptom:

If the DHCP lease is longer than 99 days, instance IP addresses cannot be automatically renewed. As a result, the instance network will be disconnected when the lease comes to an end.

Involved images:

Public and private images of Windows Server 2008, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019

Solutions:

1. Change the DHCP lease of the subnet where the instance is located to one day or unlimited.
2. Run the following command to make the change take effect:

NOTE

The following command will temporarily disconnect you from the network. Do it during off-peak hours.

```
ipconfig /renew
```

Occasional System Errors Triggered By Adding or Deleting NICs

Symptom:

After an ECS is started, adding or deleting a NIC or other equivalent actions may:

- Trigger a kernel panic, and the OS automatically restarts.

- Trigger frequent software interrupts, and the network may fail to receive or send packets.

Patch link: <https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=f00e35e259948b995aa1f3ee7fddb05f34a50157>

Involved images:

CentOS 7 public and private images

Solutions:

Upgrade the kernel to a version matching the 3.10.0-1160.25.1.e17.x86_64 kernel of CentOS 7.

Kernels Are Occasionally Disconnected from the TCP Network

Symptom:

This issue is caused by the kernel vulnerability CVE-2019-11477 (TCP SACK). When the socket buffer is low, the network may be disconnected.

The involved images are listed in the following table.

| Image Type | Kernel Version |
|---|---|
| CentOS 7 public images from 2019-06-26 to 2019-09-29 | 3.10.0-957.21.3.e17.x86_64 |
| Ubuntu 16 and Ubuntu 18 public images from 2019-06-26 to 2019-10-15 | Ubuntu 16.04: 4.4.0-151-generic Ubuntu 18.04: 4.15.0-52-generic |
| Debian 9.0 public images from 2019-06-26 to 2019-10-15 | 4.9.0-9-amd64 |
| Fedora 29 and openSUSE 15.0 public images from 2019-06-27 to 2019-10-15 | Fedora 29: 5.1.11-200.fc29.x86_64 openSUSE 15.0: 4.12.14-1p150.12.64-default |

Solutions:

Upgrade the kernel to the latest version. Run the following commands to upgrade the kernel of each image type:

- CentOS/Fedora: **yum update kernel**
- Ubuntu: **apt-get update && apt-get install linux-image-generic**
- openSUSE: **zypper refresh && zypper install kernel-default**
- Debian: **apt-get update && apt search linux-image && apt-get install linux-image-xxx**

NOTE

You can run the **apt search linux-image** command to query for the latest kernel version. The **apt-get install linux-image-xxx** command is used to upgrade a kernel to the latest version.

OS Parameter Settings Do Not Take Effect

Symptom:

After `net.ipv4.tcp_max_tw_buckets` is configured in the `/etc/sysctl.conf` file, the check result of `sysctl -a` indicates that the configuration does not take effect. The configurations in `/etc/sysctl.d/huawei.conf` and `/etc/security/limits.d/huawei-nofile.conf` have been built in public images and these configurations have higher priorities than those in `/etc/sysctl.conf`. As a result, the configurations in `/etc/sysctl.conf` do not take effect.

The involved parameters are listed in the following table.

| Parameter | Configuration File |
|--|--|
| <code>vm.swappiness</code> <code>net.core.somaxconn</code> <code>net.ipv4.tcp_max_tw_buckets</code> <code>net.ipv4.tcp_max_syn_backlog</code> | <code>/etc/sysctl.d/huawei.conf</code> |
| <code>* soft nofile 65535</code> <code>* hard nofile 65535</code> | <code>/etc/security/limits.d/huawei-nofile.conf</code> |

Involved images:

- CentOS 7 public images from 2018-09-25 to 2019-09-29
- CentOS 6 public images from 2018-09-25 to 2019-10-10
- Ubuntu, openSUSE 15.0, Debian, and Fedora 29 public images from 2018-09-28 to 2019-10-15

Solutions:

1. Delete the built-in configuration files.

```
rm -rf /etc/sysctl.d/huawei.conf
rm -rf /etc/security/limits.d/huawei-nofile.conf
```
2. Modify the kernel parameter configuration files (`limits.conf` and `sysctl.conf`).

```
cat >>/etc/security/limits.conf <<EOF
root soft nofile 65535
root hard nofile 65535
* soft nofile 65535
* hard nofile 65535
EOF

cat >>/etc/sysctl.conf <<EOF
vm.swappiness=0
net.core.somaxconn=1024
net.ipv4.tcp_max_tw_buckets=5000
net.ipv4.tcp_max_syn_backlog=1024
```

EOF

1822 NIC-based Offloading Instance Is Incompatible with the Linux 3.16.x Kernel

Symptom:

ECSs that use the hardware offloading function provided by Huawei-developed 25GE intelligent high-speed NIC may be incompatible with Linux 3.16.47–3.16.x OSs, which may cause occasional network disconnections of ECSs. ECSs that have this issue include but are not limited to C3ne, M3ne, C6, M6, G5, P2v, G5r, P2vs, P2s, Pi2, FP1cn1, Ai1, e3.26xlarge.14, e3.52xlarge.14, e3.52xlarge.20, KC1, and KM1.

Involved images:

Debian 8.2.0 64bit and Debian 8.8.0 public images

Solutions:

Remove Debian 8 public images from flavors. Migrate services of ECSs using this offloading function to S3 and C3 ECSs as soon as possible.

Data Is Lost During Disk Reset Due to the Incompatibility Between Server Manager of Windows Server 2012 R2 and VMTools

Symptom:

A Windows Server 2012 R2 ECS is configured with two data disks. When Windows Server Manager resets the second data disk, the first data disk is reset. As a result, the data of the first data disk is lost.

Involved images:

Windows Server 2012 R2 public image before 2019-02-19

Solutions:

Upgrade VMTools of involved ECSs to 2.5.0.156 or later.

Service Interruptions Caused By Lingering CLOSE_WAIT Connections

Symptom:

Some services are interrupted because a socket in a TCP connection created by the one-click password reset plug-in process stays in the **CLOSE_WAIT** state.

Involved images:

- CentOS and EulerOS public images issued before June 5, 2019
- Ubuntu and Debian public images issued before June 3, 2019

Solutions:

Update the one-click password reset plug-ins for the ECSs.

2 Creating a Private Image

2.1 Introduction

A private image is an image available only to the user who created it. It contains an OS, preinstalled public applications, and a user's personal applications. A private image can be a system disk image, data disk image, or full-ECS image. It can be created from a cloud server or an external image file.

Creating a private image does not affect the running of services on the cloud server or cause data loss.

This section describes how to create a private image using any of the following methods:

- [Creating a System Disk Image from a Linux ECS](#)
- [Creating a Linux System Disk Image from an External Image File](#)
- [Creating a BMS System Disk Image](#)
- [Creating a Data Disk Image from an ECS](#)
- [Creating a Data Disk Image from an External Image File](#)
- [Creating a Full-ECS Image from an ECS](#)
- [Creating a Full-ECS Image from a CSBS Backup](#)
- [Creating a Full-ECS Image from a CBR Backup](#)
- [Creating a Linux System Disk Image from an ISO File](#)

After a system disk image is created, you can use it to [create an ECS](#) or [change the OS](#) of an ECS.

2.2 Creating a System Disk Image from a Windows ECS

Scenarios

If you have created and configured a Windows ECS based on your service requirements (for example, by installing software and setting up an application environment), you can create a system disk image based on this configured ECS.

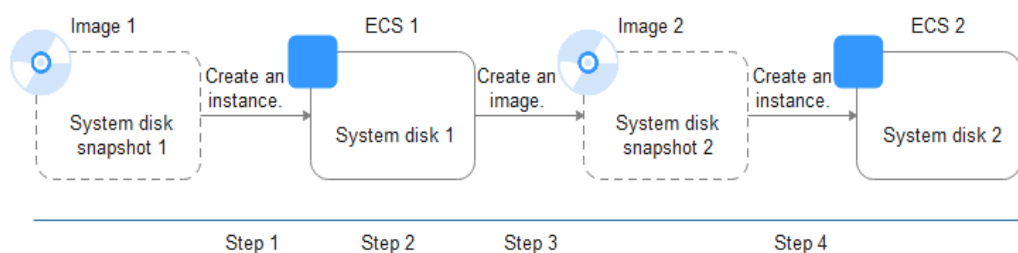
Then, all new ECSs created from this image will have the same software and environment preinstalled.

Creating a system disk image does not affect the running of services on the ECS or cause data loss.

Background

The following figure shows the process of creating a system disk image from an ECS.

Figure 2-1 Creating a system disk image and using it to create ECSs



- System disk images are often used for application scale-out. They can also be used for hybrid cloud deployment. You can create system disk images for resource synchronization on and off cloud. The procedure is as follows:

- a. Create a system disk image from an ECS.

NOTE

The ECS must be created from a private image. If it is created from a public image, the system disk image cannot be exported.

- b. Export the image to an OBS bucket. For details, see [Exporting an Image](#).
 - c. Download the image file from the OBS bucket.
- You can create an image from a running ECS.

The image creation does not affect service running on the ECS.

In this process, do not stop, start, or restart the ECS, or the image creation may fail.

- The time required for creating an image depends on the ECS system disk size, network quality, and the number of concurrent tasks.
- A system disk image will be created in the same region as the ECS that was used to create it.
- If an ECS has expired or been released, you can use the system disk image created from the ECS to restore it.

Prerequisites

Before creating a private image from an ECS:

- Delete any sensitive data the ECS may contain.
- Ensure that the ECS is in the **Running** or **Stopped** state.

- Check network configuration of the ECS and ensure that DHCP is configured for the NICs. Enable remote desktop connection if needed. For details, see [Setting the NIC to DHCP](#) and [Enabling Remote Desktop Connection](#).
- Check whether the one-click password reset plug-in has been installed on the ECS. The password reset function on the management console is only available for new ECSs that have this plug-in installed.
- Check whether Cloudbase-Init has been installed on the ECS. The user data injection function on the management console is only available for new ECSs that have this tool installed. You can use data injection, for example, to set the login password for a new ECS. For details, see [Installing and Configuring Cloudbase-Init](#).
- Check and install VirtIO drivers to ensure that new ECSs created from the image support KVM virtualization and to improve network performance. For details, see steps 2 to 4 in [Optimization Process](#).
- Run Sysprep to ensure that the SIDs of the new ECSs created from the image are unique within their domain. In a cluster deployment scenario, the SIDs must be unique. For details, see [Running Sysprep](#).
- Ensure that the system disk capacity of the ECS used to create a system disk image must be no greater than 1 TB.

If the capacity is greater than 1 TB, you can only use it to create a full-ECS image.

NOTE

If an ECS is created from a public image, the one-click password reset plug-in and Cloudbase-Init have been installed by default. You can follow the guide in the prerequisites to verify the installation.

Procedure

Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Create a system disk image.

1. Click **Create Image** in the upper right corner.
2. Set image parameters.

[Table 2-1](#) and [Table 2-2](#) list the parameters in the **Image Type and Source** and **Image Information** areas, respectively.

Table 2-1 Image type and source

| Parameter | Description |
|-----------|---|
| Type | Select System disk image . |
| Source | Select ECS and select an ECS with required configurations. |

Table 2-2 Image information

| Parameter | Description |
|--------------------|--|
| Encryption | This parameter specifies whether the image will be encrypted. The value is provided by the system and cannot be changed. <ul style="list-style-type: none">- Only an unencrypted private image can be created from an unencrypted ECS.- Only an encrypted private image can be created from an encrypted ECS. |
| Name | Set a name for the image. |
| Enterprise Project | Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. To enable this function, contact your customer manager. An enterprise project provides central management of cloud resources on a project. |
| Tag | (Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. |
| Description | (Optional) Enter a description of the image. |

3. Read and agree to the disclaimer, and click **Next**.
4. Confirm the settings and click **Submit**.

Step 3 Go back to the **Private Images** page and view the new system disk image.

The time required for creating an image depends on the ECS system disk size, network quality, and the number of concurrent tasks. When the image status changes to **Normal**, the image creation is complete.

 **NOTE**

- Do not perform any operations on the selected ECS or its associated resources during image creation.
- An ECS created from an encrypted image is also encrypted. The key used for encrypting the ECS is the same as that used for encrypting the image.
- An image created from an encrypted ECS is also encrypted. The key used for encrypting the image is the same as that used for encrypting the ECS.

----End

Follow-up Procedure

After a system disk image is created, you can:

- Use the image to create new ECSs. For details, see [Creating an ECS from an Image](#).

- Use the image to change the OSs of existing ECSs. For details, see [Changing the OS](#).

2.3 Creating a System Disk Image from a Linux ECS

Scenarios

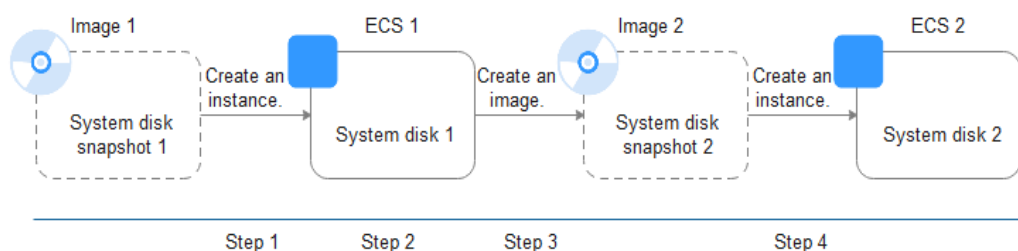
If you have created and configured a Linux ECS based on your service requirements (for example, by installing software and setting up an application environment), you can create a system disk image based on this configured ECS. Then, all new ECSs created from this image will have the same software and environment preinstalled.

Creating a system disk image does not affect the running of services on the ECS or cause data loss.

Background

The following figure shows the process of creating a system disk image from an ECS.

Figure 2-2 Creating a system disk image and using it to create ECSs



- System disk images are often used for application scale-out. They can also be used for hybrid cloud deployment. You can create system disk images for resource synchronization on and off cloud. The procedure is as follows:
 - a. Create a system disk image from an ECS.

NOTE

If the ECS is created from any of the following images, the system disk image cannot be exported:

- ISO image
 - Private image created from an Ubuntu public image
- b. Export the image to an OBS bucket. For details, see [Exporting an Image](#).
 - c. Download the image file from the OBS bucket.
- You can create an image from a running ECS.

The image creation does not affect service running on the ECS.

In this process, do not stop, start, or restart the ECS, or the image creation may fail.
 - The time required for creating an image depends on the ECS system disk size, network quality, and the number of concurrent tasks.

- A system disk image will be created in the same region as the ECS that was used to create it.
- If an ECS has expired or been released, you can use the system disk image created from the ECS to restore it.

Prerequisites

Before creating a private image from an ECS:

- Delete any sensitive data the ECS may contain.
- Ensure that the ECS is in the **Running** or **Stopped** state.
- Check network configuration of the ECS and ensure that DHCP is configured for the NICs. For details, see [Setting the NIC to DHCP](#).
- Check whether the one-click password reset plug-in has been installed on the ECS. The password reset function on the management console is only available for new ECSs that have this plug-in installed.
- Check whether Cloud-Init has been installed on the ECS. The user data injection function on the management console is only available for new ECSs that have this tool installed. You can use data injection, for example, to set the login password for a new ECS. For details, see [Installing Cloud-Init](#) and [Configuring Cloud-Init](#).
- Delete any network rules to prevent NIC name drift on the ECSs created from the image. For details, see [Deleting Files from the Network Rule Directory](#).
- To ensure that the ECSs created from the image support both Xen and KVM virtualization, the Linux ECS used to create the image has to be modified. For instance, the disk IDs in the GRUB and fstab files need to be UUID and native Xen and KVM drivers need to be installed.

For details, see steps [2](#) to [6](#) in [Optimization Process](#).

- If multiple data disks are attached to an ECS used to create a private image, the ECSs created from the image may be unavailable. You need to detach all data disks from the ECS before using it to create an image. For details, see [Detaching Data Disks from an ECS](#).
- If data disks have been attached to the ECS and automatic partition mounting has been configured in the fstab file for the ECS, delete these configurations from the file before using the ECS to create a system disk image.
- Ensure that the system disk capacity of the ECS used to create a system disk image must be no greater than 1 TB.

If the capacity is greater than 1 TB, you can only use it to create a full-ECS image.

NOTE

If an ECS is created from a public image, the one-click password reset plug-in and Cloud-Init have been installed by default. You can follow the guide to verify the installation.

Procedure

Step 1 Access the IMS console.

1. Log in to the management console.

2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Create a system disk image.

1. Click **Create Image** in the upper right corner.
2. Set image parameters.

Table 2-3 and **Table 2-4** list the parameters in the **Image Type and Source** and **Image Information** areas, respectively.

Table 2-3 Image type and source

| Parameter | Description |
|-----------|---|
| Type | Select System disk image . |
| Source | Select ECS and select an ECS with required configurations. |

Table 2-4 Image information

| Parameter | Description |
|--------------------|--|
| Encryption | This parameter specifies whether the image will be encrypted. The value is provided by the system and cannot be changed. <ul style="list-style-type: none">- Only an unencrypted private image can be created from an unencrypted ECS.- Only an encrypted private image can be created from an encrypted ECS. |
| Name | Set a name for the image. |
| Enterprise Project | Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. To enable this function, contact your customer manager. An enterprise project provides central management of cloud resources on a project. |
| Tag | (Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. |
| Description | (Optional) Enter a description of the image. |

3. Read and agree to the disclaimer, and click **Next**.
4. Confirm the settings and click **Submit**.

Step 3 Go back to the **Private Images** page and view the new system disk image.

The time required for creating an image depends on the ECS system disk size, network quality, and the number of concurrent tasks. When the image status changes to **Normal**, the image creation is complete.

 **NOTE**

- Do not perform any operations on the selected ECS or its associated resources during image creation.
- An ECS created from an encrypted image is also encrypted. The key used for encrypting the ECS is the same as that used for encrypting the image.
- An image created from an encrypted ECS is also encrypted. The key used for encrypting the image is the same as that used for encrypting the ECS.

----End

Follow-up Procedure

After a system disk image is created, you can:

- Use the image to create new ECSs. For details, see [Creating an ECS from an Image](#).
- Use the image to change the OSs of existing ECSs. For details, see [Changing the OS](#).

2.4 Creating a Windows System Disk Image from an External Image File

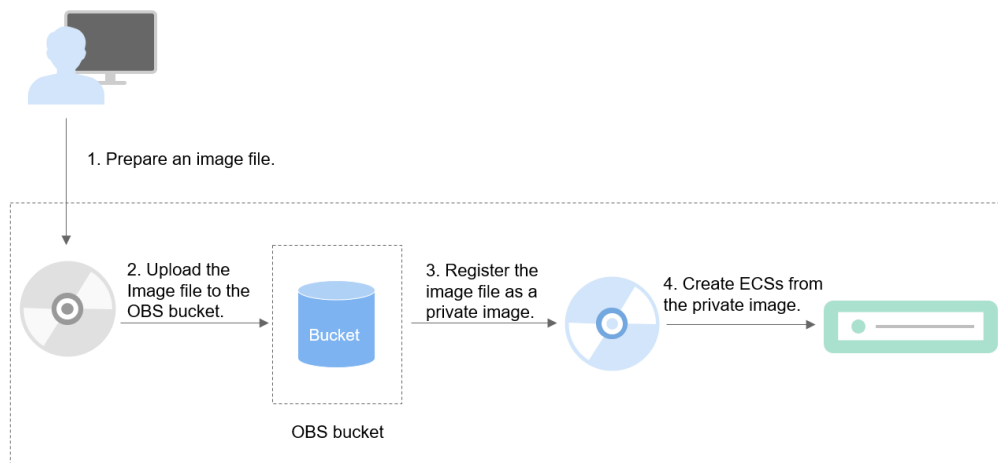
2.4.1 Overview

You can import a local image or a system disk image from another cloud platform to the current cloud. After an image is imported, you can use it to create ECSs or reinstall the OSs of existing ECSs.

Creation Process

[Figure 2-3](#) shows the process of creating a private image.

Figure 2-3 Creating a Windows system disk image



As shown in the figure, the following steps are required to register an external image file as a private image:

1. Prepare an external image file that meets platform requirements. For details, see [Preparing an Image File](#).
2. Upload the external image file to your OBS bucket. For details, see [Uploading an External Image File](#).
3. On the management console, select the uploaded image file and register it as a private image. For details, see [Registering an External Image File as a Private Image](#).
4. After the private image is registered, you can use it to create ECSs. For details, see [Creating a Windows ECS from an Image](#).

2.4.2 Preparing an Image File

You need to prepare an image file that can be used to create a private image.

NOTE

Currently, a large image file (maximum: 1 TB) can be imported only in RAW or ZVHD2 format. In addition to the requirements described in [Table 2-6](#), a bitmap file needs to be generated alongside each RAW image file. The bitmap file is uploaded together with the image file. For details, see [Fast Import of an Image File](#).

Initial Configuration for an Image File

The initial configuration must be completed on the source VM before an image file is exported from it. If you did not configure it, use the image file to create an ECS, configure the ECS, and use the ECS to create a private image. For details, see [What Do I Do If a Windows Image File Is Not Pre-Configured When I Use It to Register a Private Image?](#)

Table 2-5 Initial configuration for an image file

| Configuration Item | How to Configure |
|--------------------|--|
| Network | <p>The NIC must be set to DHCP. Otherwise, the ECS startup or network capability will be abnormal. For details, see: Setting the NIC to DHCP</p> <p>The following operations are optional:</p> <ul style="list-style-type: none">• Enabling NIC multi-queue NIC multi-queue enables multiple vCPUs to process NIC interrupts, thereby improving network PPS and I/O performance. For details, see How Do I Enable NIC Multi-Queue for an Image?• Configuring dynamic assignment of IPv6 addresses IPv6 addresses are used to deal with IPv4 address exhaustion. If dynamic configuration is enabled in an image file, the ECSs created from this file will be automatically assigned an IPv6 address. These ECSs will support both IPv4 and IPv6 addresses. Configure dynamic assignment of IPv6 addresses. For details, see How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses? |
| Tools | <p>You are advised to install Cloudbase-Init.</p> <p>Cloudbase-Init is an open-source tool for cloud instance initialization. When creating ECSs from an image with Cloudbase-Init, you can use user data injection to inject customized initialization details (for example, an ECS login password) to the ECSs. You can also configure and manage a running ECS by querying and using metadata. If Cloudbase-Init is not installed, you cannot apply custom configurations to the ECSs. You will have to use the original password in the image file to log in to the ECSs.</p> <p>For details, see Installing and Configuring Cloudbase-Init.</p> <p>If each of your ECSs requires a unique SID in a domain, run Sysprep after Cloudbase-Init is installed. For details, see Running Sysprep.</p> |
| Drivers | <p>An ECS can run properly only after Xen Guest OS drivers (PV drivers) and KVM Guest OS drivers (VirtIO drivers) are installed on it. To ensure that ECSs support both Xen and KVM and to improve network performance, PV and VirtIO drivers must be installed for the image.</p> <ul style="list-style-type: none">• Installing PV drivers• Installing VirtIO drivers <p>For GPU-accelerated ECSs, you need to install special drivers when creating a private image. For details, see Installing Special Windows Drivers.</p> |

Image File Properties

Table 2-6 Windows image file properties

| Image File Property | Requirement |
|---------------------|--|
| OS | <ul style="list-style-type: none">Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 1032-bit or 64-bitThe OS cannot be bound to specific hardware.The OS must support full virtualization. <p>For details about the supported OS versions, see External Image File Formats and Supported OSs. These OSs support automatic configuration. For details, see What Will the System Do to an Image File When I Use the File to Register a Private Image? For other OSs, check and install Guest OS drivers. On the image registration page, select Other Windows. After the image is imported, whether the system is started depends on the driver integrity.</p> |
| Image format | VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, and ZVHD |
| Image size | <p>If an image is no larger than 128 GB, import it directly.</p> <p>If an image is between 128 GB and 1 TB, convert the image file into RAW or ZVHD2 and import it using fast import.</p> <ul style="list-style-type: none">For details about how to convert the image file format, see Converting the Image Format Using qemu-img-hw.For details about fast import, see Fast Import of an Image File. |

Other

- Currently, images with data disks cannot be created. The image file must contain only a system disk, and the system disk size must be [40 GB, 1024 GB].
- The initial password in the image file must contain uppercase letters, lowercase letters, digits, and special characters (!@\$%^-_=+[{ } ; , / ?).
- The boot partition and system partition must be on the same disk.
- For an external image file, you need a tenant administrator account and password combination.
- If you use an external image file to create a Windows system disk image and then use the image to create an ECS, you cannot log in to the ECS using a key pair or obtain the password from the key pair.
- Supported boot modes:
Some x86 OS images support the UEFI boot mode. (For details, see [OSs Supporting UEFI Boot Mode](#).)

Arm OS images support only the UEFI boot mode.

- The image file cannot be encrypted, or ECSs created from the registered image may not work properly.
- A VMDK image file must be generated from a VM created in VMware Tools. Otherwise, the system may fail to start due to image parsing problems.

2.4.3 Uploading an External Image File

You are advised to use OBS Browser+ to upload external image files to OBS buckets.

NOTE

- Only unencrypted external image files or those encrypted using SSE-KMS can be uploaded to the OBS bucket.
- The storage class of the OBS bucket must be Standard.
- If you want to create a data disk image along with the system disk image, you also need to upload an image file containing data disks to the OBS bucket. You can create one system disk image and no more than three data disk images.

2.4.4 Registering an External Image File as a Private Image

Scenarios

Register an image file uploaded to the OBS bucket as a private image.

Procedure

Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Register an external image file as a private image.

1. Click **Create Image** in the upper right corner.
2. Set image parameters.

Table 2-7 and **Table 2-8** list the parameters in the **Image Type and Source** and **Image Information** areas, respectively.


Table 2-7 Image type and source

| Parameter | Description |
|-----------|---|
| Type | Select System disk image . |
| Source | Select Image File for Source . Select the bucket storing the image file from the list and then select the image file. |

| Parameter | Description |
|--------------------|--|
| Enable Fast Create | <p>This parameter is available only when you select a ZVHD2 or RAW image file.</p> <p>This function enables fast image creation and supports import of large files (maximum: 1 TB) as long as the files to be uploaded are converted to ZVHD2 or RAW format and optimized. If you have a file that meets the requirements, select Enable Fast Create and select the confirmation information following Image File Preparation.</p> <p>NOTE</p> <p>To learn how to convert image file formats and generate bitmap files, see Fast Import of an Image File.</p> |

Table 2-8 Image information

| Parameter | Description |
|--------------------------------|--|
| Enable automatic configuration | If you select this option, the system will automatically check and optimize the image file. For details, see What Will the System Do to an Image File When I Use the File to Register a Private Image? |
| Function | Specifies whether the image is used to create ECSs or BMSs. The value can be ECS system disk image or BMS system disk image . This section uses ECS system disk image as an example. |
| Architecture | Specify Architecture . Select x86 or ARM . <ul style="list-style-type: none">- If the system detects an architecture type different from that you set, the architecture type detected by the system will be used.- If the system fails to detect the architecture type, the architecture type you set will be used. |
| Boot Mode | <p>This parameter is optional. The value can be BIOS or UEFI. For details about the differences between them, see How Is BIOS Different from UEFI?</p> <p>For details about which OSs support UEFI boot, see OSs supporting UEFI Boot Mode.</p> <p>The boot mode must be the same as that in the image file. You need to confirm which boot mode is used in the image file. After you select the correct boot mode, the boot mode will be configured for the image at the background. Select the right boot mode, or ECSs created using the image will not be able to boot up.</p> |

| Parameter | Description |
|--------------------|---|
| OS | <p>To ensure that the image can be created and used properly, select an OS consistent with that in the image file. If you do not select an OS, the system attempts to automatically identify the OS in the image file.</p> <p>NOTE</p> <ul style="list-style-type: none"> - If the system detects that the image file OS is different from the one you selected, the OS detected by the system will be used. - If the system cannot detect the OS in the image file, the OS you selected will be used. - If the OS you selected or identified by the system is incorrect, ECSs created from the image file may be affected. |
| System Disk (GB) | <p>The system disk capacity (value range: 40 GB to 1024 GB). Ensure that this value is at least equal to the system disk capacity in the image file.</p> <p>NOTE</p> <p>If the uploaded VHD image is generated using qemu-img or similar tools, check the system disk capacity based on What Do I Do If the System Disk Capacity in a VHD Image File Exceeds the One I Have Specified on the Management Console When I Use This File to Register a Private Image?</p> |
| Data Disk (GB) | <p>You can also add data disks to the image. You need to obtain an image file containing data disks in advance. This function is used to migrate VMs and data disks from other platforms to the current platform.</p> <p>To add data disks, click , configure the data disk capacity, and click Select Image File. In the displayed dialog box, select the target bucket and then the target image file containing the data disk.</p> <p>A maximum of three data disks can be added.</p> |
| Name | Set a name for the image. |
| Encryption | <p>(Optional) If you want to encrypt the image, select KMS encryption and select the key to be used from the key list. After you select KMS encryption, the system will create a default key ims/default for you. You can also select a key from the key list.</p> <p>For how to encrypt an image, see Creating Encrypted Images.</p> |
| Enterprise Project | <p>Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account.</p> <p>An enterprise project provides central management of cloud resources on a project by project basis.</p> |

| Parameter | Description |
|-------------|---|
| Tag | (Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. |
| Description | (Optional) Enter a description of the image. |

3. Click **Next** and confirm the image specifications. Select **Statement of Commitment to Image Creation** and **Huawei Image Disclaimer**. Click **Submit**.

Step 3 Go back to the **Private Images** page. The image is successfully registered when its status becomes **Normal**.

If you add data disks during image creation, a system disk image and data disk images will be generated. The number of data disk images depends on the number of data disks you add (a maximum of 3).

 **NOTE**

The time required for image registration is determined by the image file size. You may need to wait a long period of time for the image file to be successfully registered as a private image.

----End

2.4.5 Creating a Windows ECS from an Image

Scenarios

After registering an external image file as a private image on the cloud platform, you can use the image to create ECSs or change the OSs of existing ECSs.

This section describes how to create an ECS from an image.

Procedure

Create an ECS by referring to [Creating an ECS from an Image](#).

Note the following when setting the parameters:

- **Region:** Select the region where the private image is located.
- **Specifications:** Select a flavor based on the OS type in the image and the OS versions described in [OSs Supported for Different Types of ECSs](#).
- **Image:** Select **Private image** and then the created image from the drop-down list.
- (Optional) **Data Disk:** Add data disks. These data disks are created from a data disk image generated together with a system disk image. In this way, you can migrate the data of data disks together with system disk data from the VM on the original platform to the current cloud platform.

Follow-up Procedure

After a system disk image is created, you can use it to change the OS of an ECS. For details, see [Changing the OS](#).

2.5 Creating a Linux System Disk Image from an External Image File

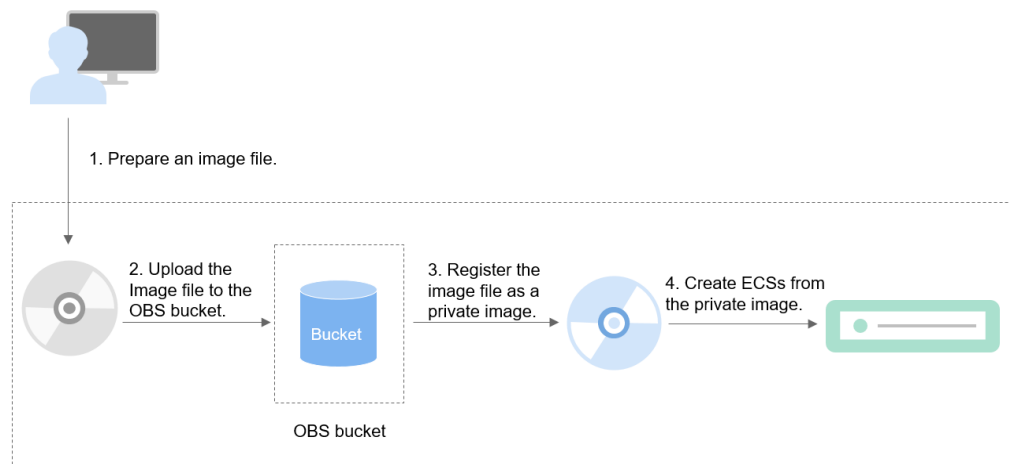
2.5.1 Overview

You can import a local image or a system disk image from another cloud platform to the current cloud. After an image is imported, you can use it to create ECSs or reinstall the OSs of existing ECSs.

Creation Process

[Figure 2-4](#) shows the process of creating a private image.

Figure 2-4 Creating a Linux system disk image



The procedure is as follows:

1. Prepare an external image file that meets platform requirements. For details, see [Preparing an Image File](#).
2. Upload the external image file to your OBS bucket. For details, see [Uploading an External Image File](#).
3. On the management console, select the uploaded image file and register it as a private image. For details, see [Registering an External Image File as a Private Image](#).
4. After the private image is registered, you can use it to create ECSs. For details, see [Creating a Linux ECS from an Image](#).

2.5.2 Preparing an Image File

You need to prepare an image file that can be used to create a private image.

 NOTE

Currently, a large image file (maximum: 1 TB) can be imported only in RAW or ZVHD2 format. In addition to the requirements described in [Table 2-10](#), a bitmap file needs to be generated alongside each RAW image file. The bitmap file is uploaded together with the image file. For details, see [Fast Import of an Image File](#).

Initial Configuration for an Image File

The initial configuration must be completed on the source VM before an image file is exported from it. If you did not configure it, use the image file to create an ECS, configure the ECS, and use the ECS to create a private image. For details, see [What Do I Do If a Linux Image File Is Not Pre-Configured When I Use It to Register a Private Image?](#)

Table 2-9 Initial configuration for an image file

| Configuration Item | How to Configure |
|--------------------|---|
| Network | <p>The NIC must be set to DHCP and files must be deleted from the network role directory. Otherwise, the ECS startup or network capability will be abnormal. For details, see:</p> <ul style="list-style-type: none">• Deleting files from the network rule directory• Setting the NIC to DHCP <p>The following value-added operations are optional:</p> <ul style="list-style-type: none">• Enabling NIC multi-queue NIC multi-queue enables multiple vCPUs to process NIC interrupts, thereby improving network PPS and I/O performance. For details, see How Do I Enable NIC Multi-Queue for an Image?• Configuring dynamic assignment of IPv6 addresses IPv6 addresses are used to deal with IPv4 address exhaustion. If dynamic configuration is enabled in an image file, the ECSs created from this file will be automatically assigned an IPv6 address. These ECSs will support both IPv4 and IPv6 addresses. Configure dynamic assignment of IPv6 addresses. For details, see How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses? |

| Configuration Item | How to Configure |
|--------------------|---|
| Tools | <p>You are advised to install Cloud-Init.</p> <p>Cloud-Init is an open-source tool for cloud instance initialization. When creating ECSs from an image with Cloud-Init, you can use user data injection to customize initialization details (for example, an ECS login password) to the ECSs. You can also configure and manage a running ECS by querying and using metadata. If Cloud-Init is not installed, you cannot apply these custom configurations to your ECSs, and you will have to use the original password in the image file to log in to the ECSs.</p> <p>For details, see Installing Cloud-Init.</p> |
| Drivers | Installing native KVM drivers |
| File system | <ul style="list-style-type: none">• Changing the disk identifier in the GRUB configuration file to UUID• Changing the disk identifier in the fstab file to UUID |
| Data disks | <p>If multiple data disks are attached to the ECS used to create a private image, ECSs created from the image may be unavailable. Therefore, you need to detach all data disks from the ECS before using it to create a private image.</p> <p>For details, see Detaching Data Disks from an ECS.</p> |

Image File Properties

Table 2-10 Linux image file properties

| Image File Property | Requirement |
|---------------------|--|
| OS | <ul style="list-style-type: none">• SUSE, Oracle Linux, Red Hat, Ubuntu, openSUSE, CentOS, Debian, Fedora, EulerOS, and NeoKylin• 32-bit or 64-bit• The OS cannot be bound to specific hardware.• The OS must support full virtualization. <p>For details about the supported OS versions, see External Image File Formats and Supported OSs. These OSs support automatic configuration. For details, see What Will the System Do to an Image File When I Use the File to Register a Private Image? For other OSs, check and install VirtIO drivers (see Installing Native KVM Drivers). On the image registration page, select Other Linux. After the image is imported, whether the system is started depends on the driver integrity.</p> |

| Image File Property | Requirement |
|---------------------|--|
| Image format | VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, and ZVHD |
| Image size | Maximum file size: 128 GB If the image size is between 128 GB and 1 TB, convert the image file into RAW or ZVHD2 and import it using fast import. <ul style="list-style-type: none">For details about how to convert the image file format, see Converting the Image Format Using qemu-img-hw.For details about fast import, see Fast Import of an Image File. |

Other

- Currently, images with data disks cannot be created. The image file must contain only a system disk, and the system disk size must be [40 GB, 1024 GB].
- The initial password in the image file must contain uppercase letters, lowercase letters, digits, and special characters (!@\$%^_-=+[]{};./?).
- The boot partition and system partition must be on the same disk.
- Supported boot modes:
Some x86 OS images support the UEFI boot mode. (For details, see [OSs Supporting UEFI Boot Mode](#).)
Arm OS images support only the UEFI boot mode.
- The image file cannot be encrypted, or ECSs created from the registered image may not work properly.
- The `/etc/fstab` file cannot contain automatic mounting information of non-system disks. Otherwise, the login to the created ECS may fail.
- If the external image file uses LVM as the system disk, ECSs created from the private image do not support file injection.
- If the VM where the external image file is located has been shut down, it must be a graceful shutdown. Otherwise, a blue screen may occur when the ECS created from the private image is started.
- A VMDK image file must be created from a VM generated by VMware Tools. Otherwise, the system may fail to start due to image parsing problems.

2.5.3 Uploading an External Image File

You are advised to use OBS Browser+ to upload external image files to OBS buckets.

 NOTE

- Only unencrypted external image files or those encrypted using SSE-KMS can be uploaded to the OBS bucket.
- The storage class of the OBS bucket must be Standard.
- If you want to create a data disk image along with the system disk image, you also need to upload an image file containing data disks to the OBS bucket. You can create one system disk image and no more than three data disk images.

2.5.4 Registering an External Image File as a Private Image

Scenarios

Register an image file uploaded to the OBS bucket as a private image.

Procedure

Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Register an external image file as a private image.

1. Click **Create Image** in the upper right corner.
2. Set image parameters.


Table 2-11 and **Table 2-12** list the parameters in the **Image Type and Source** and **Image Information** areas, respectively.

Table 2-11 Image type and source

| Parameter | Description |
|--------------------|--|
| Type | Select System disk image . |
| Source | Select Image File for Source . Select the bucket storing the image file from the list and then select the image file. |
| Enable Fast Create | <p>This parameter is available only when you select a ZVHD2 or RAW image file.</p> <p>This function enables fast image creation and supports import of large files (maximum: 1 TB) as long as the files to be uploaded are converted to ZVHD2 or RAW format and optimized. If you have a file that meets the requirements, select Enable Fast Create and select the confirmation information following Image File Preparation.</p> <p>NOTE To learn how to convert image file formats and generate bitmap files, see Fast Import of an Image File.</p> |

Table 2-12 Image information

| Parameter | Description |
|--------------------------------|--|
| Enable automatic configuration | If you select this option, the system will automatically check and optimize the image file. For details, see What Will the System Do to an Image File When I Use the File to Register a Private Image? |
| Function | Specifies whether the image is used to create ECSs or BMSs. The value can be ECS system disk image or BMS system disk image . This section uses ECS system disk image as an example. |
| Architecture | Specify Architecture . Select x86 or ARM . <ul style="list-style-type: none">- If the system detects an architecture type different from that you set, the architecture type detected by the system will be used.- If the system fails to detect the architecture type, the architecture type you set will be used. |
| Boot Mode | This parameter is optional. The value can be BIOS or UEFI . For details about the differences between them, see How Is BIOS Different from UEFI? For details about which OSs support UEFI boot, see OSs supporting UEFI Boot Mode . The boot mode must be the same as that in the image file. You need to confirm which boot mode is used in the image file. After you select the correct boot mode, the boot mode will be configured for the image at the background. Select the right boot mode, or ECSs created using the image will not be able to boot up. |
| OS | To ensure that the image can be created and used properly, select an OS consistent with that in the image file. If you do not select an OS, the system attempts to automatically identify the OS in the image file. NOTE <ul style="list-style-type: none">- If the system detects that the image file OS is different from the one you selected, the OS detected by the system will be used.- If the system cannot detect the OS in the image file, the OS you selected will be used.- If the OS you selected or identified by the system is incorrect, ECSs created from the image file may be affected. |

| Parameter | Description |
|--------------------|--|
| System Disk (GB) | <p>The system disk capacity (value range: 40 GB to 1024 GB). Ensure that this value is at least equal to the system disk capacity in the image file.</p> <p>NOTE If the uploaded VHD image is generated using qemu-img or similar tools, check the system disk capacity based on What Do I Do If the System Disk Capacity in a VHD Image File Exceeds the One I Have Specified on the Management Console When I Use This File to Register a Private Image?</p> |
| Data Disk (GB) | <p>You can also add data disks to the image. You need to obtain an image file containing data disks in advance. This function is used to migrate VMs and data disks from other platforms to the current platform.</p> <p>To add data disks, click , configure the data disk capacity, and click Select Image File. In the displayed dialog box, select the target bucket and then the target image file containing the data disk.</p> <p>A maximum of three data disks can be added.</p> |
| Name | Set a name for the image. |
| Encryption | <p>(Optional) If you want to encrypt the image, select KMS encryption and select the key to be used from the key list. After you select KMS encryption, the system will create a default key ims/default for you. You can also select a key from the key list.</p> <p>For how to encrypt an image, see Creating Encrypted Images.</p> |
| Enterprise Project | <p>Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account.</p> <p>An enterprise project provides central management of cloud resources on a project by project basis.</p> |
| Tag | (Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. |
| Description | (Optional) Enter a description of the image. |

3. Click **Next** and confirm the image specifications. Select **Statement of Commitment to Image Creation** and **Huawei Image Disclaimer**. Click **Submit**.

Step 3 Go back to the **Private Images** page. The image is successfully registered when its status becomes **Normal**.

If you add data disks during image creation, a system disk image and data disk images will be generated. The number of data disk images depends on the number of data disks you add (a maximum of 3).

 **NOTE**

The time required for image registration is determined by the image file size. You may need to wait a long period of time for the image file to be successfully registered as a private image.

----End

2.5.5 Creating a Linux ECS from an Image

Scenarios

After registering an external image file as a private image on the cloud platform, you can use the image to create ECSs or change the OSs of existing ECSs.

This section describes how to create an ECS from an image.

Procedure

Create an ECS by referring to [Creating an ECS from an Image](#).

Note the following when setting the parameters:

- **Region:** Select the region where the private image is located.
- **Specifications:** Select a flavor based on the OS type in the image and the OS versions described in [OSs Supported for Different Types of ECSs](#).
- **Image:** Select **Private image** and then the created image from the drop-down list.
- (Optional) **Data Disk:** Add data disks. These data disks are created from a data disk image generated together with a system disk image. In this way, you can migrate the data of data disks together with system disk data from the VM on the original platform to the current cloud platform.

Follow-up Procedure

After a system disk image is created, you can use it to change the OS of an ECS. For details, see [Changing the OS](#).

2.6 Creating a BMS System Disk Image

You can use either of the following methods to create a BMS private image:

- [Creating a Private Image from a BMS](#)
- [Creating a Private Image from an External Image File](#)

2.7 Creating a Data Disk Image from an ECS

Scenarios

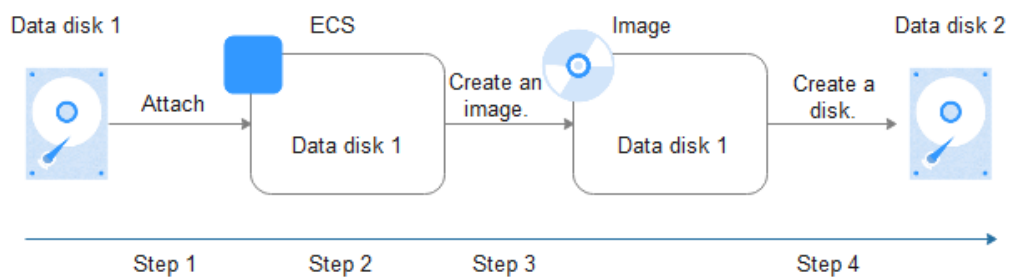
A data disk image contains only service data. You can create a data disk image from an ECS and then use the image to create new EVS disks. This is a convenient way to migrate data from an ECS to EVS disks.

For example, you can create a data disk image to clone the data of an ECS whose disk is about to expire.

Background

The following figure shows the process of creating a data disk image from an ECS.

Figure 2-5 Creating a data disk image and using it to create data disks



Prerequisites

- A data disk has been attached to the ECS, and the ECS is running or stopped. For details about how to attach a data disk, see *Elastic Cloud Server User Guide*.
- The data disk capacity of the ECS must be no greater than 1 TB. If the capacity is greater than 1 TB, you can only use the ECS to create a full-ECS image.

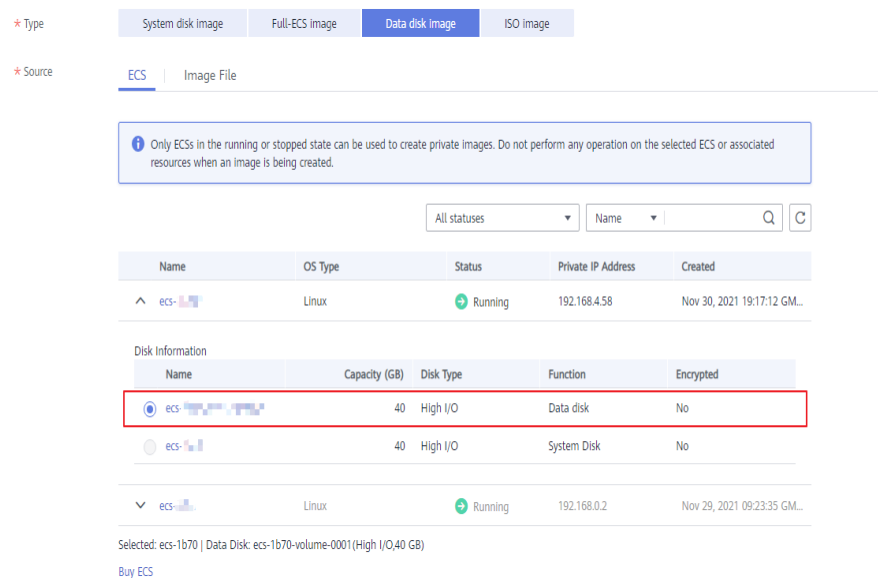
Procedure

Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**. The IMS console is displayed.

Step 2 Create a data disk image.

1. Click **Create Image** in the upper right corner.
2. In the **Image Type and Source** area, select **Data disk image** for **Type**.
3. Select **ECS** for **Source** and then select a data disk of the ECS.

Figure 2-6 Creating a data disk image

4. In the **Image Information** area, set **Name**, **Tag**, and **Description**, and select an enterprise project.
If the data disk is not encrypted, the private image created from it is also not encrypted. The encryption attribute cannot be changed during image creation. After the image is created, you can change its encryption attribute based on [Replicating Images Within a Region](#).
5. Click **Next**.
6. Confirm the settings. Read the image disclaimer and select **I have read and agree to the Image Disclaimer**, and click **Submit**.
The private image list is displayed. Wait until the data disk image is created successfully.

Step 3 Go back to the **Private Images** page and view the new data disk image.

----End

Follow-up Procedure

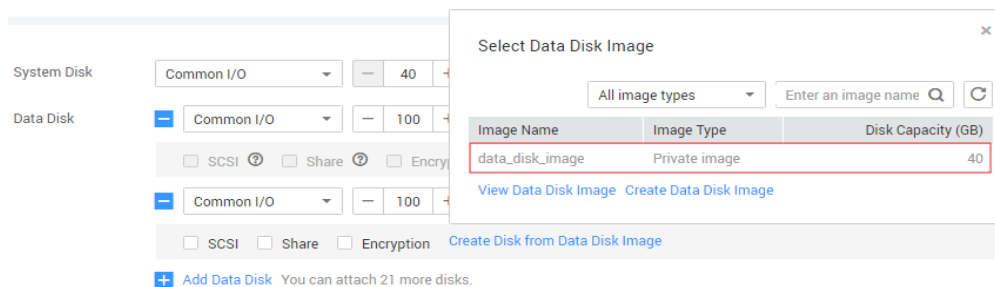
If you want to use the created data disk image to create an EVS disk and attach it to an ECS, you can perform either of the following operations:

- Locate the row that contains the created data disk image and click **Create Data Disk** to create one or multiple data disks. Then attach the data disks to an ECS.
- On the page for creating ECSs, click **Create Disk from Data Disk Image** and select the data disk image.

NOTE

In this way, a data disk image can be used to create a data disk for an ECS only once. For example, a data disk created from data disk image **data_disk_image** has been added to the ECS. No any other data disk created from this image can be added to the ECS.

Figure 2-7 Adding data disks



2.8 Creating a Data Disk Image from an External Image File

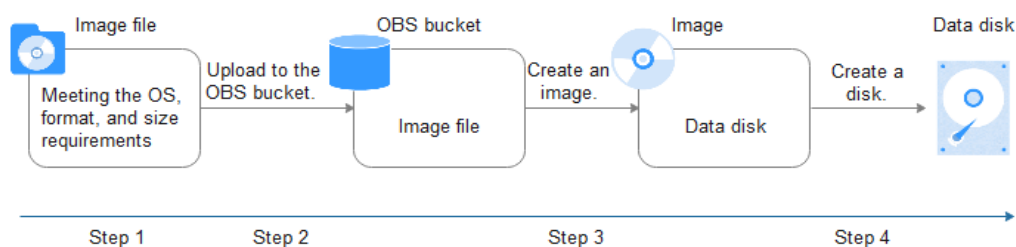
Scenarios

A data disk image contains only service data. You can create a data disk image using a local image file or an external image file (image file on another cloud platform). Then, you can use the data disk image to create EVS disks and migrate your service data to the cloud.

Background

The following figure shows the process of creating a data disk image from an external image file.

Figure 2-8 Creating a data disk image from an external image file



1. Prepare an external image file. The file must be in VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, QED, ZVHD, or ZVHD2 format. If you want to use an image file in other formats, convert the file into any of the listed formats before importing it to the cloud platform.

For details about image file format conversion, see [Converting the Image Format Using qemu-img](#) or [Converting the Image Format Using qemu-img-hw](#).

2. When uploading the external image file, you must select an OBS bucket with standard storage. For details, see [Uploading an External Image File](#).
3. Create a data disk image. For details, see [Procedure](#).
4. Use the data disk image to create data disks. For details, see [Follow-up Procedure](#).

Procedure

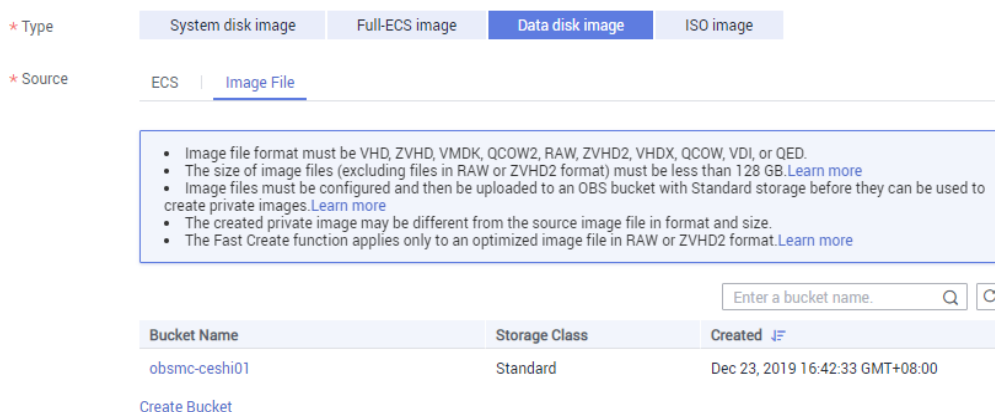
Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Create a data disk image.

1. Click **Create Image** in the upper right corner.
2. In the **Image Type and Source** area, select **Data disk image** for **Type**.
3. Select **Image File** for **Source**. Select the bucket storing the image file from the list and then select the image file.

Figure 2-9 Creating a data disk image from an external image file



4. To register the image file using Fast Create, select **Enable Fast Create**.

NOTE

- Currently, fast import is only available for ZVHD2 and RAW image files.
- For how to convert image file formats and generate bitmap files, see [Fast Import of an Image File](#).

After you select **Enable Fast Create**, select the confirmation information following **Image File Preparation** if you have prepared the required files.

5. In the **Image Information** area, set the following parameters.
 - **OS Type**: The value is **Linux**.
 - **Data Disk**: The value ranges from 40 GB to 2048 GB and must be no less than the data disk capacity in the image file.
 - **Name**: Enter a name for the image.
 - (Optional) **Encryption**: If you want to encrypt the image, select **KMS encryption** and then select the key to be used from the key list.
 - **Enterprise Project**: Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. To enable this function, contact your customer manager. An enterprise project provides central management of cloud resources on a project.
 - (Optional) **Tag**: Set a tag key and a tag value for the image to easily identify and manage it.

- (Optional) **Description:** Enter description of the image.
6. Click **Next**.
 7. Confirm the settings. Read the image disclaimer and select **I have read and agree to the Image Disclaimer**, and click **Submit**.

Step 3 Go back to the **Private Images** page and view the new data disk image.

When the image status changes to **Normal**, the image creation is complete.

----End

Follow-up Procedure

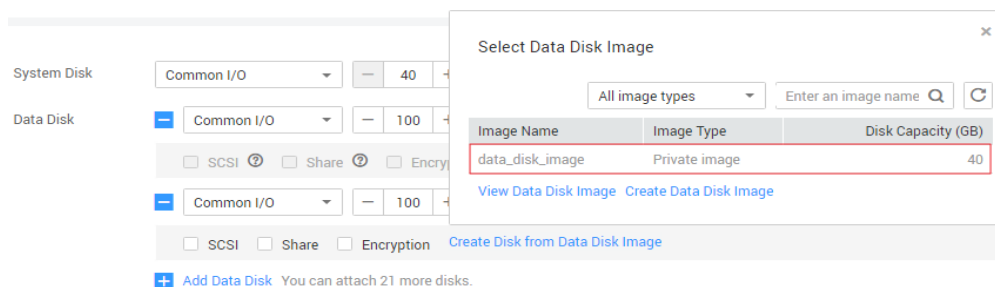
If you want to use the created data disk image to create an EVS disk and attach it to an ECS, you can perform either of the following operations:

- Locate the row that contains the created data disk image and click **Create Data Disk** to create one or multiple data disks. Then attach the data disks to an ECS.
- On the page for creating ECSs, click **Create Disk from Data Disk Image** and select the data disk image.

NOTE

In this way, a data disk image can be used to create a data disk for an ECS only once. For example, a data disk created from data disk image **data_disk_image** has been added to the ECS. No any other data disk created from this image can be added to the ECS.

Figure 2-10 Adding data disks



2.9 Creating a Full-ECS Image from an ECS

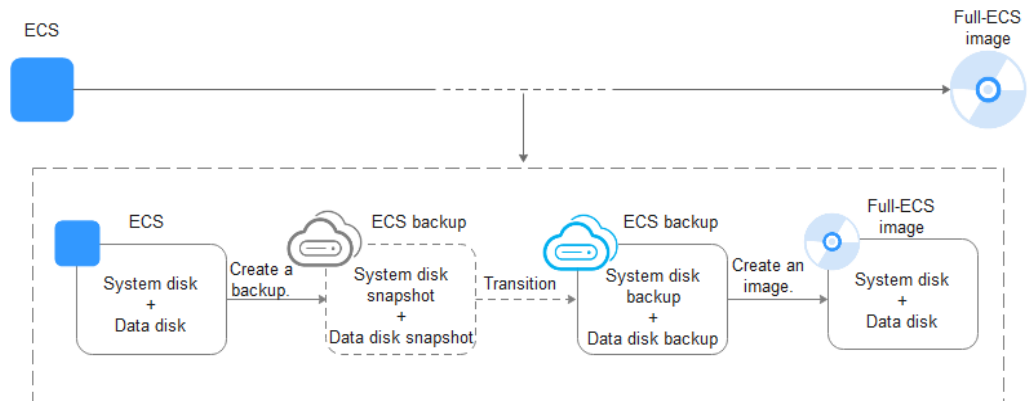
Scenarios

You can create an image of an entire ECS, including not just the OS, but also the software and all the service data. You can then use this image to migrate data by quickly provisioning exact clones of the original ECS.

Background

The following figure shows the process of creating an image from an entire ECS, with both the system and data disks included.

Figure 2-11 Creating a full-ECS image from an ECS



- The time required for creating a full-ECS image depends on the disk size, network quality, and the number of concurrent tasks.
- The ECS used to create a full-ECS image must be in **Running** or **Stopped** state. To create a full-ECS image containing a database, use a stopped ECS.
- If an ECS is in **Stopped** state, do not start it when you are using it to create a full-ECS image.
- When a full-ECS image is being created from an ECS, do not perform any operations on the ECS, or the image creation may fail.
- In [Figure 2-11](#), if there are snapshots of the system disk and data disks but the ECS backup creation is not complete, the full-ECS image you create will only be available in the AZ where the source ECS is and can only be used to provision ECSs in this AZ. You cannot provision ECSs in other AZs in the region until the original ECS is fully backed up and the full-ECS image is in the **Normal** state.
- If you use a full-ECS image to change an ECS OS, only the system disk data can be written into the ECS. Therefore, if you want to restore or migrate the data disk data of an ECS by using a full-ECS image, you can only use the image to create a new ECS rather than use it to change the ECS OS.

Constraints

- When creating a full-ECS image from an ECS, ensure that the ECS has been properly configured, or the image creation may fail.
For details, see
- A Linux ECS used to create a full-ECS image cannot have a disk group or logical disk that contains multiple physical disks, or data may be lost when ECSs are created from that image.
- An ECS used to create a full-ECS image cannot contain a Dedicated Distributed Storage Service (DSS) disk.
- A full-ECS image cannot be exported.
- A full-ECS image cannot be replicated within a region.
- Cross-region replication of full-ECS images is only available for certain regions.

If a full-ECS image cannot be replicated to a different region, you can use it to create an ECS, use the ECS to create a system disk image and a data disk image, and replicate the images to the destination region.

A full-ECS image created using an ECS backup can be replicated from the region where they reside to another region, but the replicated full-ECS image cannot be replicated across regions again.

- When creating a full-ECS image from a Windows ECS, you need to change the SAN policy of the ECS to **OnlineAll**. Otherwise, EVS disks attached to the ECSs created from the image may be offline.

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

Table 2-13 SAN policies in Windows

| Type | Description |
|-----------------|--|
| OnlineAll | All newly detected disks are automatically brought online. |
| OfflineShared | All disks on sharable buses, such as iSCSI and FC, are left offline by default, while disks on non-sharable buses are kept online. |
| OfflineInternal | All newly detected disks are left offline. |

- Execute **cmd.exe** and run the following command to query the current SAN policy of the ECS:
diskpart
- Run the following command to view the SAN policy of 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 **c**.
- Run the following command to change the SAN policy of the ECS to **OnlineAll**:
san policy=onlineall

Procedure

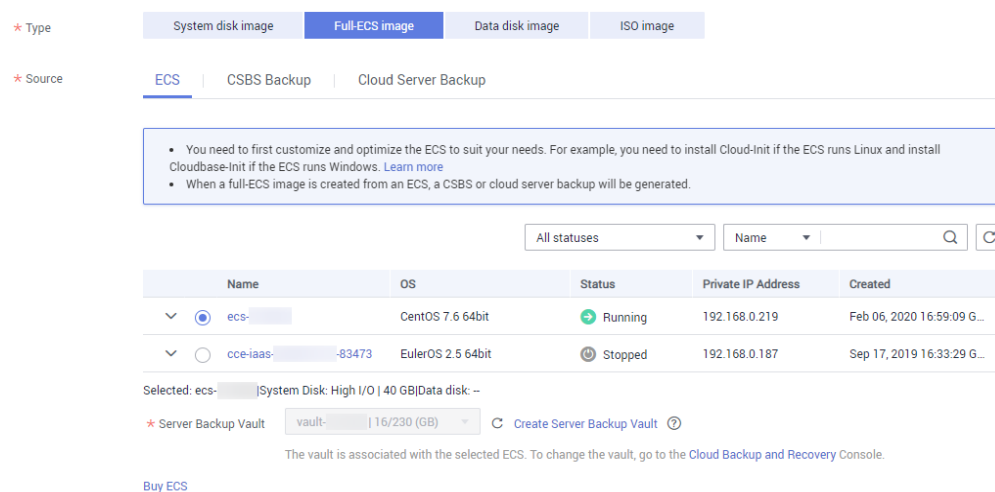
Step 1 Access the IMS console.

- Log in to the management console.
- Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Create a full-ECS image.

- Click **Create Image** in the upper right corner.
- In the **Image Type and Source** area, select **Full-ECS image** for **Type**.

3. Select **ECS** for **Source** and then select an ECS from the list.

Figure 2-12 Creating a full-ECS image using an ECS

4. Specify **Server Backup Vault** to store backups.
The created full-ECS image and backup are stored in the server backup vault. If no server backup vault is available, click **Create Server Backup Vault** to create one. Ensure that you select **Backup** for **Protection Type**. For more information about CBR backups and vaults, see [What Is CBR?](#)
5. In the **Image Information** area, configure basic image details, such as the image name and description.
6. Click **Next**.
7. Confirm the settings. Read the image disclaimer and select **I have read and agree to the Image Disclaimer**, and click **Submit**.

Step 3 Go back to the **Private Images** page and view the new full-ECS image.

- When the image status changes to **Normal**, the image creation is complete.
- If **Available in AZX** is displayed under **Normal** in the **Status** column for a full-ECS image, the backup for this ECS has not been created and only a disk snapshot is created. (**AZX** indicates the AZ where the source ECS of the image resides.)

In this case, the full-ECS image can be used to provision ECSs only in the specified AZ. If you want to use this image to provision ECSs in other AZs of the region, you need to wait until **Available in AZX** disappears from under **Normal**, which indicates that the ECS backup has been successfully created. This process takes about 10 minutes, depending on the data volume of the source ECS.

----End

Follow-up Procedure

- If you want to use the full-ECS image to create ECSs, click **Apply for Server** in the **Operation** column. On the displayed page, create ECSs by following the instructions in *Elastic Cloud Server User Guide*.

 **NOTE**

When you use a full-ECS image to create an ECS:

- The system and data disk information defaulted by the image will be automatically displayed.
- If the full-ECS image contains multiple data disks, it takes some time to load and display the disk information.
- If you use a full-ECS image to change an ECS OS, only the system disk data can be written into the ECS. Therefore, if you want to restore or migrate the data disk data of an ECS by using a full-ECS image, you can only use the image to create a new ECS rather than use it to change the ECS OS.
- If you want to share the full-ECS image with other tenants, you can use either of the following methods:
 - If the ECS the full-ECS image was created from has a CSBS backup, you must first migrate the backup to CBR before you share the image because CSBS is being deprecated.
 - If the ECS has no such a backup, you can share the full-ECS image directly.

2.10 Creating a Full-ECS Image from a CSBS Backup

Scenarios

Create a full-ECS image from a CSBS backup. This image can then be used to create ECSs.

Background

- If you use a CSBS backup to create a full-ECS image, you will only be charged for the CSBS backup. For detailed service pricing, see **Cloud Server Backup Service** in [Product Pricing Details](#).
- When deleting a full-ECS image, you can choose whether to delete the associated CSBS backup. If you choose not to delete the CSBS backup, you will continue to be charged for it.
- If you use a full-ECS image to change an ECS OS, only the system disk data can be written into the ECS. Therefore, if you want to restore or migrate the data disk data of an ECS by using a full-ECS image, you can only use the image to create a new ECS rather than use it to change the ECS OS.

Constraints

- When creating a full-ECS image from a CSBS backup, ensure that the source ECS of the CSBS backup has been properly configured, or the image creation may fail.
For details, see
- If an ECS is in **Stopped** state, do not start it when you are using it to create a full-ECS image.
- A CSBS backup used to create a full-ECS image cannot have shared disks.
- Only an available CSBS backup can be used to create a full-ECS image. A CSBS backup can be used to create only one full-ECS image.

- A full-ECS image cannot be exported.
- A full-ECS image cannot be replicated within a region.
- Cross-region replication of full-ECS images is only available for certain regions.

If a full-ECS image cannot be replicated to a different region, you can use it to create an ECS, use the ECS to create a system disk image and a data disk image, and replicate the images to the destination region.

A full-ECS image created using an ECS backup can be replicated from the region where they reside to another region, but the replicated full-ECS image cannot be replicated across regions again.

Procedure

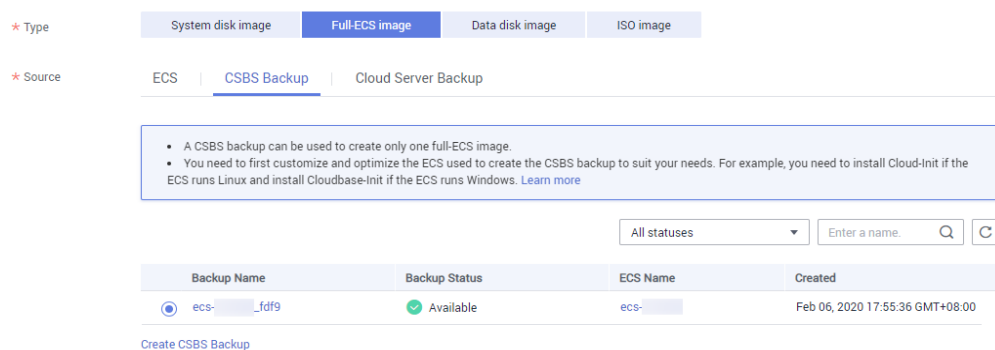
Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Create a full-ECS image.

1. Click **Create Image** in the upper right corner.
2. In the **Image Type and Source** area, select **Full-ECS image** for **Type**.
3. Select **CSBS Backup** for **Source** and then select a backup from the list.

Figure 2-13 Creating a full-ECS image using a CSBS backup



4. In the **Image Information** area, configure basic image details, such as the image name and description.
5. Click **Next**.
6. Confirm the settings. Read the image disclaimer and select **I have read and agree to the Image Disclaimer**, and click **Submit**.

Step 3 Switch back to the **Image Management Service** page to monitor the image status.

When the image status changes to **Normal**, the image creation is complete.

----End

Follow-up Procedure

- If you want to use the full-ECS image to create ECSs, click **Apply for Server** in the **Operation** column. On the displayed page, create ECSs by following the instructions in *Elastic Cloud Server User Guide*.

NOTE

- When you use a full-ECS image to create an ECS:
 - The system and data disk information defaulted by the image will be automatically displayed.
 - If the full-ECS image contains multiple data disks, it takes some time to load and display the disk information.
- If you use a full-ECS image to change an ECS OS, only the system disk data can be written into the ECS. Therefore, if you want to restore or migrate the data disk data of an ECS by using a full-ECS image, you can only use the image to create a new ECS rather than use it to change the ECS OS.
- If you want to share a full-ECS image with other tenants, you must migrate the associated backup to CBR first because only full-ECS images created from CBR backups can be shared.

2.11 Creating a Full-ECS Image from a CBR Backup

Scenarios

You can use a Cloud Backup and Recovery (CBR) backup to create a full-ECS image, which can be used to create ECSs.

Background

- CBR provides the backup service for EVS disks, BMSs, and ECSs. If you have created a backup for an ECS using CBR, you can use the backup to create a full-ECS image.
- If you use a CBR backup to create a full-ECS image, you will only be charged for the CBR backup. For pricing details, see "Cloud Backup and Recovery" in [Product Pricing Details](#).
- When deleting a full-ECS image, you can choose whether to delete the associated CBR backup. If you choose not to delete the CBR backup, you will continue to be charged for it.
- If you use a full-ECS image to change an ECS OS, only the system disk data can be written into the ECS. Therefore, if you want to restore or migrate the data disk data of an ECS by using a full-ECS image, you can only use the image to create a new ECS rather than use it to change the ECS OS.

Constraints

- When creating a full-ECS image from a CBR backup, ensure that the source ECS of the CBR backup has been properly configured, or the image creation may fail.
For details, see
- A CBR backup can be used to create only one full-ECS image.

- If an ECS is in **Stopped** state, do not start it when you are using it to create a full-ECS image.
- A full-ECS image created from a CBR backup can be shared with other tenants. However, if it is a shared CBR backup, the full-ECS image created from it cannot be shared.
- A full-ECS image cannot be exported.
- A full-ECS image cannot be replicated within a region.
- Cross-region replication of full-ECS images is only available for certain regions.

If a full-ECS image cannot be replicated to a different region, you can use it to create an ECS, use the ECS to create a system disk image and a data disk image, and replicate the images to the destination region.

A full-ECS image created using an ECS backup can be replicated from the region where they reside to another region, but the replicated full-ECS image cannot be replicated across regions again.

Procedure

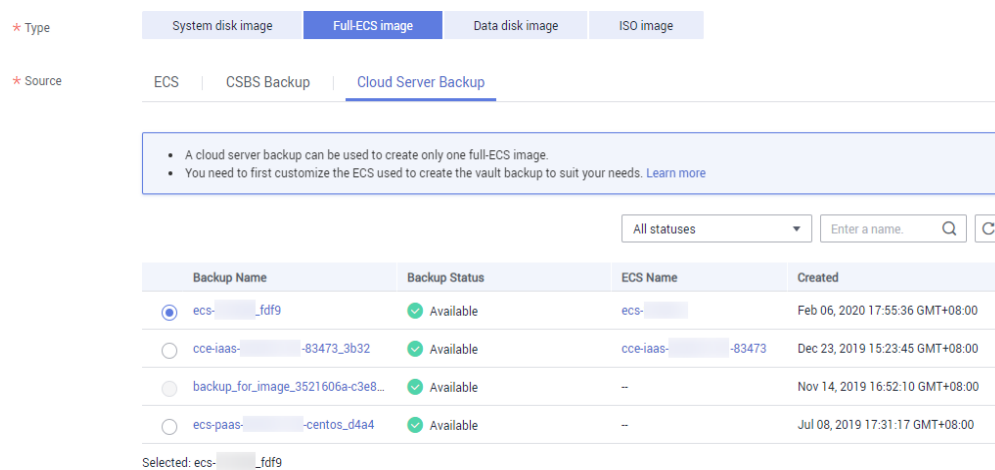
Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Create a full-ECS image.

1. Click **Create Image** in the upper right corner.
2. In the **Image Type and Source** area, select **Full-ECS image** for **Type**.
3. Select **Cloud Server Backup** for **Source** and then select an ECS from the list.

Figure 2-14 Creating a full-ECS image using a CBR backup



4. In the **Image Information** area, configure basic image details, such as the image name and description.
5. Click **Next**.
6. Confirm the settings. Read the image disclaimer and select **I have read and agree to the Image Disclaimer**, and click **Submit**.

Step 3 Switch back to the **Image Management Service** page to monitor the image status.

When the image status changes to **Normal**, the image creation is complete.

----End

Follow-up Procedure

After the full-ECS image creation is complete, you can perform the following operations:

- If you want to use the image to create ECSs, click **Apply for Server** in the **Operation** column. On the displayed page, select **Private image** and then select the full-ECS image. For details, see [Purchasing an ECS](#).

NOTE

When you use a full-ECS image to create an ECS:

- The system and data disk information defaulted by the image will be automatically displayed.
- If the full-ECS image contains multiple data disks, it takes some time to load and display the disk information.
- If you want to share the image with other tenants, click **More** in the **Operation** column and select **Share** from the drop-down list. In the displayed dialog box, enter the project IDs of the image recipients. For details, see [Sharing Specified Images](#).
- If you use a full-ECS image to change an ECS OS, only the system disk data can be written into the ECS. Therefore, if you want to restore or migrate the data disk data of an ECS by using a full-ECS image, you can only use the image to create a new ECS rather than use it to change the ECS OS.

2.12 Creating a Windows System Disk Image from an ISO File

2.12.1 Overview

An ISO file is a disk image of an optical disc. A large number of data files can be compressed into a single ISO file. Likewise, to access the files stored in an ISO, the ISO file needs to be decompressed. For example, you can use a virtual CD-ROM to open an ISO file, or burn the ISO file to a CD or DVD and then use the CD-ROM to read the image.

This section describes how to create a Windows system disk image from an ISO file.

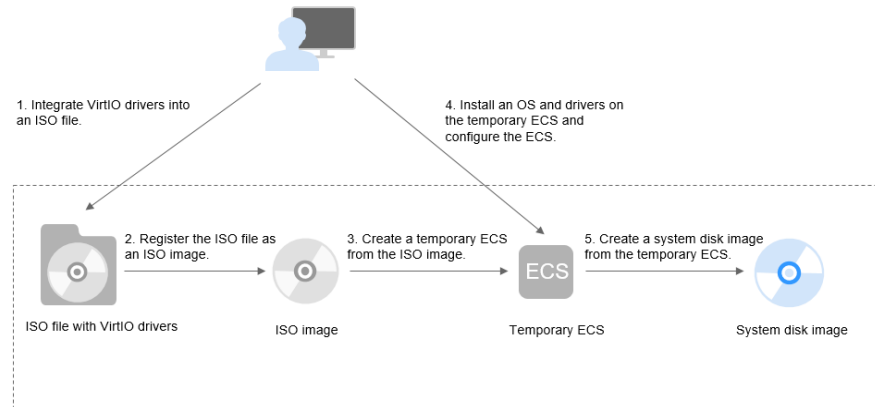
NOTE

This section is applicable only to the management console. If you are an API user, see [Creating an Image from an ISO File](#).

Creation Process

Figure 2-15 shows the process of creating a Windows system disk image from an ISO file.

Figure 2-15 Creating a Windows system disk image



The procedure is as follows:

1. Integrate VirtIO drivers into the ISO file.
Windows uses Integrated Drive Electronics (IDE) disks and VirtIO NICs. Before registering an image on the cloud platform, integrate VirtIO drivers into the Windows ISO file. For details, see [Integrating VirtIO Drivers into an ISO File](#).
2. Register the ISO file as an ISO image.
On the management console, register the ISO file with VirtIO drivers as an image. The image is an ISO image and cannot be used to provision ECSs. For details, see [Registering an ISO File as an ISO Image](#).
3. Create a temporary ECS from the ISO image.
Use the registered ISO image to create a temporary ECS. The ECS has no OS or driver installed. For details, see [Creating a Windows ECS from an ISO Image](#).
4. Install an OS and necessary drivers for the temporary ECS and configure related settings.
You need to install an OS, PV drivers, and VirtIO drivers, and configure NICs. For details, see [Installing a Windows OS and VirtIO Drivers](#) and [Step 1 in Configuring the ECS and Creating a Windows System Disk Image](#).
5. Create a system disk image from the temporary ECS.
On the management console, create a system disk image from the temporary ECS on which the installation and configuration have been completed. After the image is created, delete the temporary ECS to avoid generating any additional charges. For details, see [Creating a System Disk Image from a Windows ECS](#).

Constraints

- An ISO image created from an ISO file is used only for creating a temporary ECS. It will not be available on the ECS console. You cannot use it to create ECSs or change ECS OSs. You need to install an OS on the temporary ECS and use that ECS to create a system disk image which can be used to create ECSs or change ECS OSs.
- A temporary ECS has limited functionality. For example, you cannot attach disks to it. You are not advised to use it as a normal ECS.

2.12.2 Integrating VirtIO Drivers into an ISO File

Scenarios

Windows uses IDE disks and VirtIO NICs. Before registering an image on the cloud platform, integrate VirtIO drivers into the Windows ISO file. Typically, an ISO file contains all the files that would be included on an optical disc. Some software can be installed only from a CD-ROM drive. So, a virtual CD-ROM drive is required.

This section uses AnyBurn and UltraISO as examples to describe how to integrate VirtIO drivers into an ISO file.

NOTE

- AnyBurn is lightweight CD/DVD/Blu-ray burning software with a free version.
- UltraISO is an ISO CD/DVD image file handling tool. A free trial version is limited to ISO files of 300 MB or less. You are advised to buy a standard version.

Prerequisites

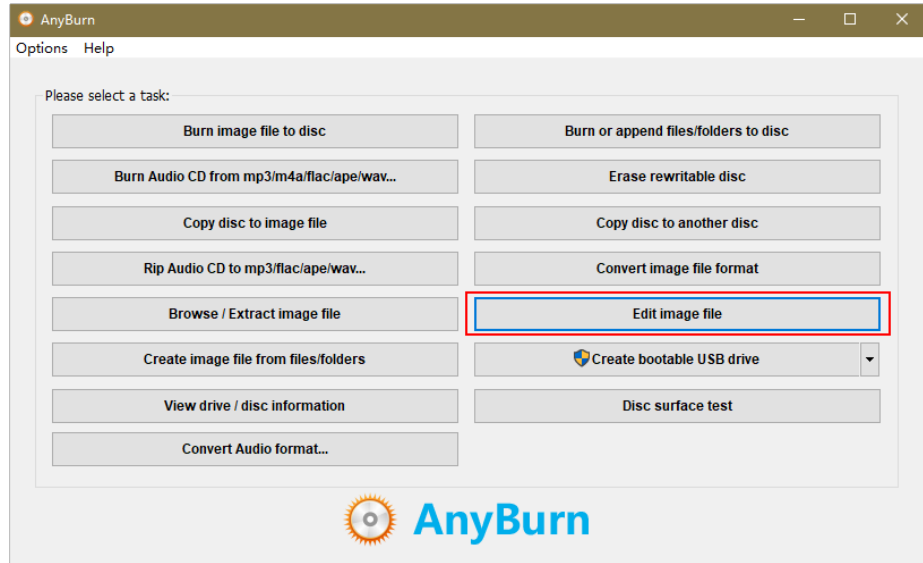
You have obtained an ISO file.

NOTE

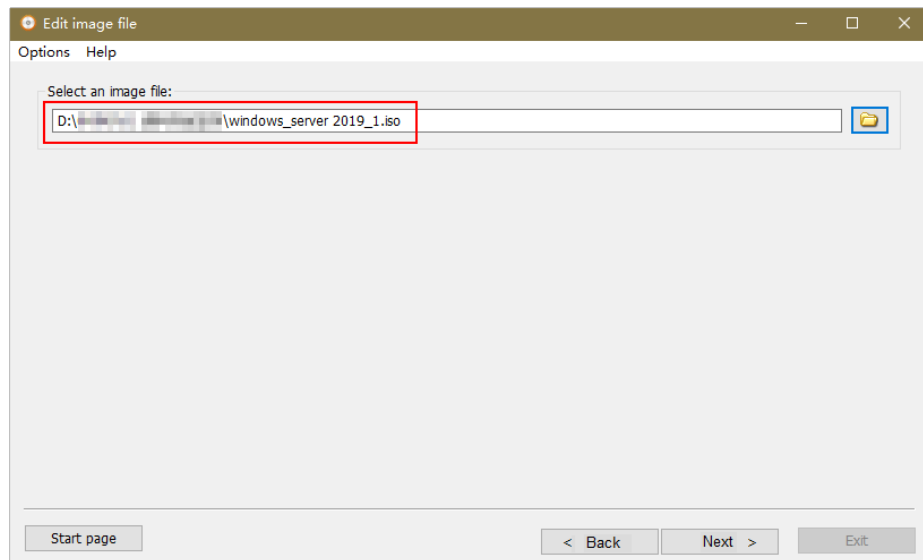
The ISO file name can contain only letters, digits, hyphens (-), and underscores (_). If the name does not meet the requirements, change it.

AnyBurn

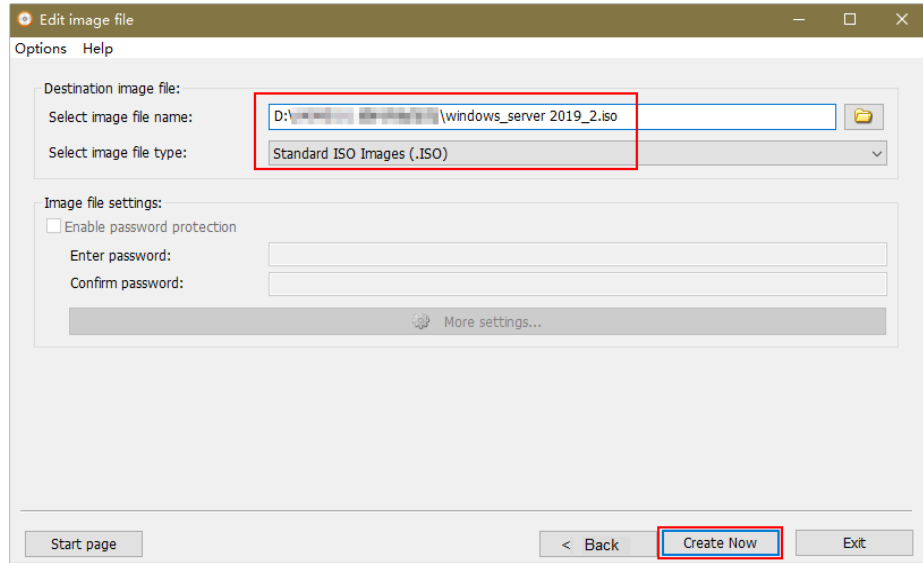
1. Download [AnyBurn](#) and install it on your local PC.
2. Download VirtIO drivers.
<https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtio-win.iso>
Other versions:
<https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/>
3. Use AnyBurn to open the ISO file.
 - a. Open AnyBurn and select **Edit Image File**.



- b. Select the ISO file and click **Next**.



- 4. Edit the ISO file to integrate VirtIO drivers into it.
 - a. Decompress the **virtio-win.iso** file downloaded in 2.
 - b. Click **Add**. Select all the decompressed files to add them to the parent node of the ISO file, and click **Next**.
 - c. Select a path to save the new ISO file and specify a name for the new file. Select **ISO** as the file type. Click **Create Now**.
After the new ISO file is generated, view VirtIO drivers in it.



UltraISO

1. Download UltraISO and install it on your local PC.
Download address: <https://www.ultraiso.com/>
2. Download VirtIO drivers.
<https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtio-win.iso>
Other versions:
<https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/>
3. Use UltraISO to open the ISO file.

CAUTION

Do not extract the ISO file or open it with any tool other than UltraISO, or the boot data will be lost.

4. Drag and drop the downloaded VirtIO driver files to the parent node of the ISO file.
5. Use UltraISO to export the ISO file with VirtIO drivers to an .iso file on your local PC.

2.12.3 Registering an ISO File as an ISO Image

Scenarios

Register an external ISO file on the cloud platform as a private image (ISO image). Before registering an image, upload the ISO file exported in [Integrating VirtIO Drivers into an ISO File](#) to the OBS bucket.

The ISO image cannot be replicated, exported, or encrypted.

Prerequisites

- The file to be registered must be in ISO format.
- The ISO image file has been uploaded to the OBS bucket. For details, see [Uploading an External Image File](#).

Procedure

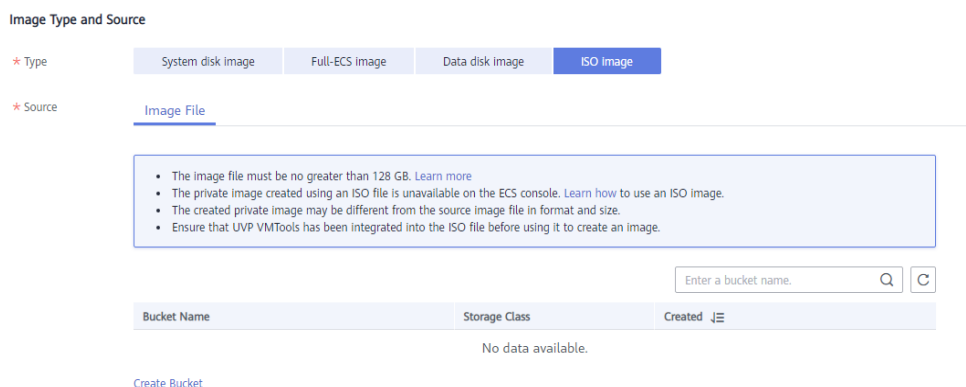
Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Register an ISO file as an ISO image.

1. Click **Create Image** in the upper right corner.
2. In the **Image Type and Source** area, select **ISO image** for **Type**.
3. In the image file list, select the bucket and then the image file.

Figure 2-16 Creating a private image from an ISO file



4. In the **Image Information** area, set the following parameters.

- **Architecture.** Select **x86** or **ARM**.

NOTE

This parameter is required only in regions that support both x86 and Arm.

- **Boot Mode:** Select **BIOS** or **UEFI**. Ensure that the selected boot mode is the same as that in the image file, or the ECSs created from this image will not be able to boot up. The Arm architecture does not support the BIOS boot mode.

NOTE

If the boot mode in the image file is **BIOS** but you select **UEFI** here for **Boot Mode**, you will not be able to adjust the resolution.

- **OS:** Select the OS specified in the ISO file. To ensure that the image can be created and used properly, select an OS consistent with that in the image file.

- **System Disk:** Set the system disk capacity (value range: 40 GB to 1024 GB), which must be no less than the capacity of the system disk in the image file.
 - **Name:** Enter a name for the image to be created.
 - **Enterprise Project:** Select the enterprise project to which your images belong.
 - **Tag:** (Optional) Add a tag to the image to be created.
 - **Description:** (Optional) Enter image description as needed.
5. Click **Next**.
 6. Confirm the settings. Select **Statement of Commitment to Image Creation** and **Huawei Image Disclaimer**. Click **Submit**.

Step 3 Switch back to the **Image Management Service** page to check the image status.

When the image status changes to **Normal**, the image is registered successfully.

----End

2.12.4 Creating a Windows ECS from an ISO Image

Scenarios

This section describes how to create an ECS from a registered ISO image.

Procedure

Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Use an ISO image to create a Windows ECS.

1. Click the **Private Images** tab. Locate the row that contains the ISO image and click **Create ECS** in the **Operation** column.
The created ECS is for temporary use only and needs to be deleted when you are finished with it. The system creates a pay-per-use ECS with fixed specifications. When you use the private image created from this ECS to create new ECSs, you can customize the specifications and billing mode then.
2. Configure the ECS as prompted and click **OK**.

----End

Follow-up Procedure

After the ECS is created, you can log in remotely to continue with OS and drivers installation.

2.12.5 Installing a Windows OS and VirtIO Drivers

Scenarios

This section uses Windows Server 2019 64-bit as an example to describe how to install Windows on an ECS.

The installation procedure varies depending on the image file you use. Perform operations as prompted.

NOTE

Set the time zone, KMS address, patch server, input method, and language based on service requirements.

Prerequisites

You have remotely logged in to the ECS and entered the installation page.

Procedure

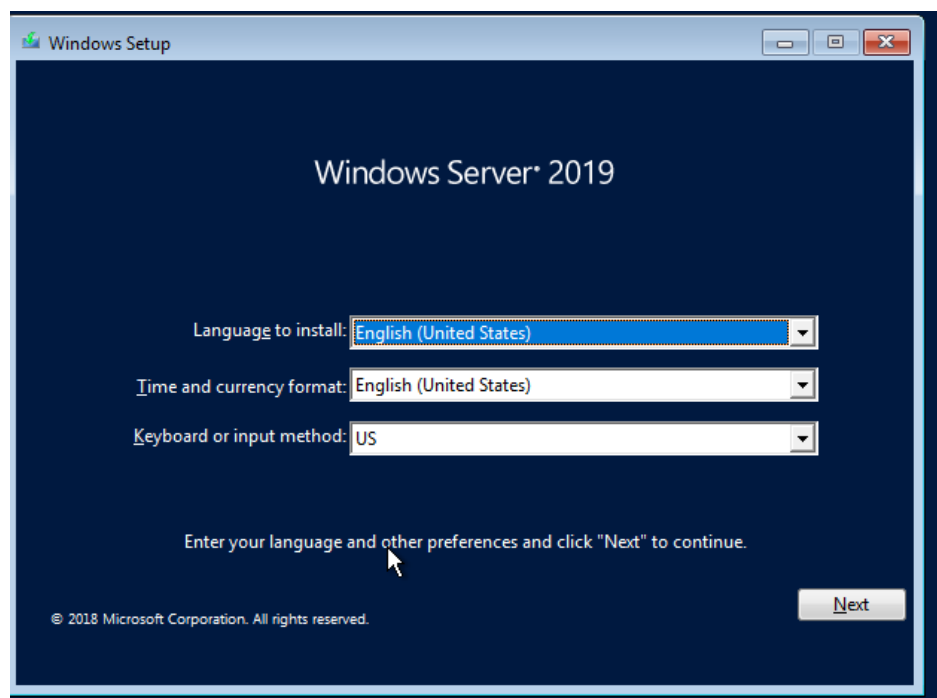
CAUTION

Do not stop or restart the ECS during the OS installation. Otherwise, the OS installation will fail.

Step 1 Install the Windows OS.

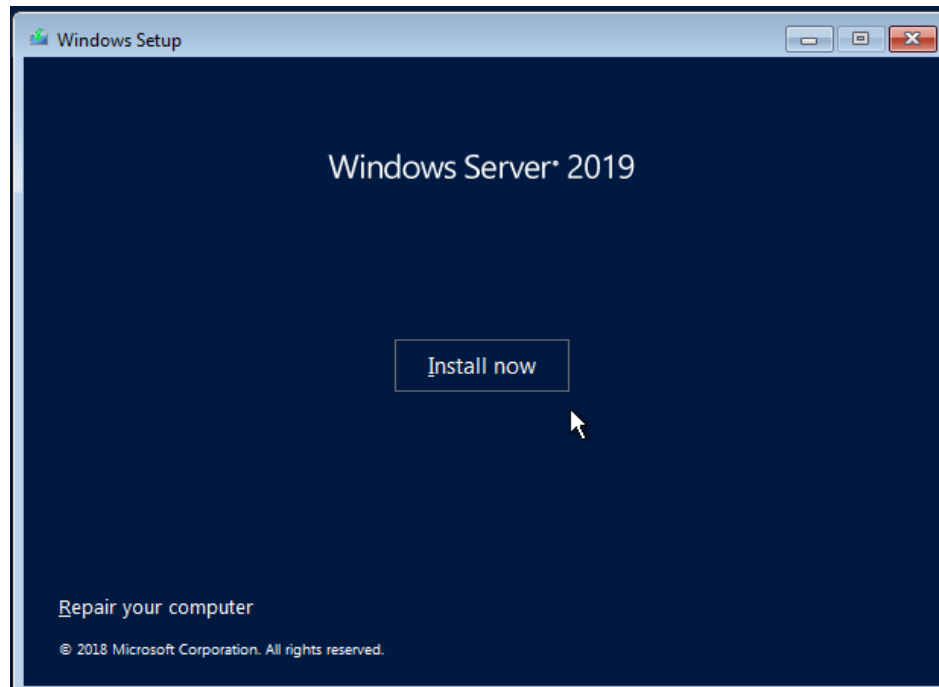
1. Configure Windows setup.

Figure 2-17 Windows setup



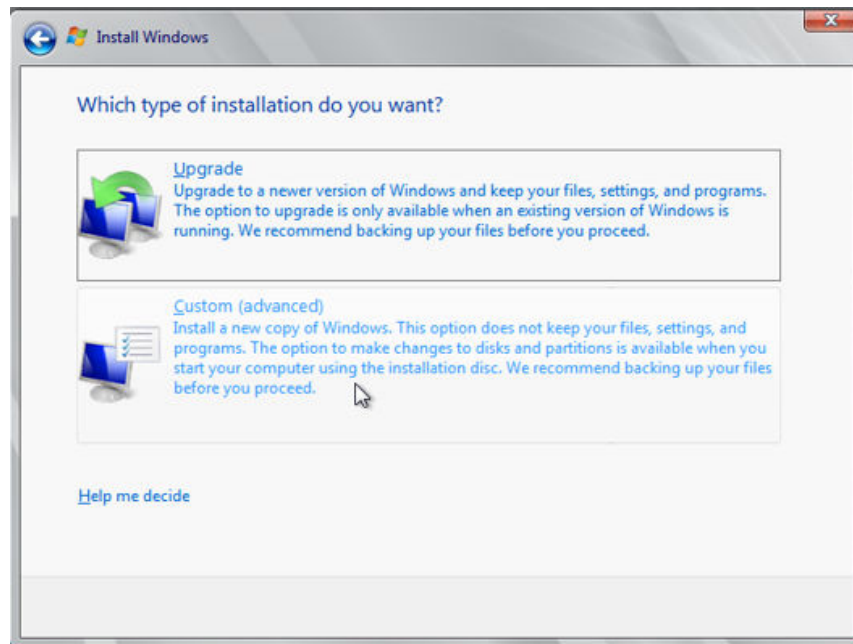
2. Click **Next**.
The installation confirmation window is displayed.

Figure 2-18 Installation confirmation window



3. Click **Install now**.
The **Select the operating system you want to install** dialog box is displayed.
4. Select the version of the OS to be installed and click **Next**.
The **Please read the license terms** dialog box is displayed.
5. Select **I accept the license terms**, and click **Next**.
The **Which type of installation do you want?** window is displayed.

Figure 2-19 Installation type

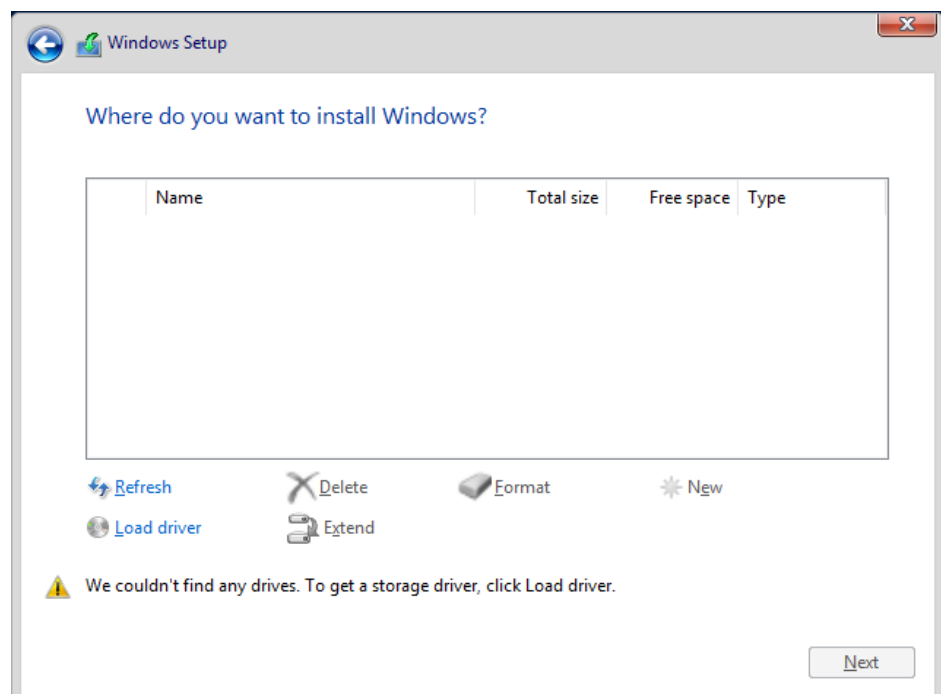


- 6. Select **Custom (advanced)**.

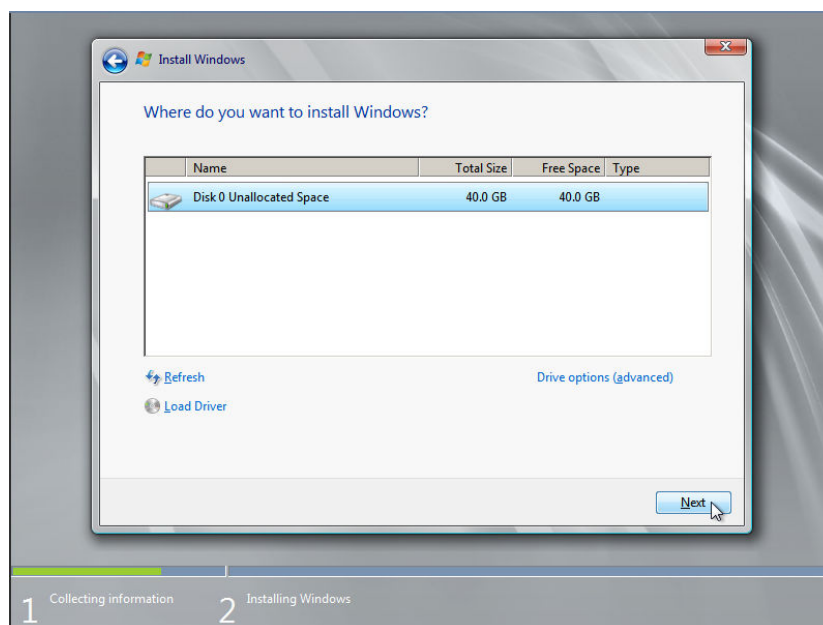
The **Where do you want to install Windows?** window is displayed.

- If the system displays a message indicating that no driver is found, go to [Step 1.7](#).

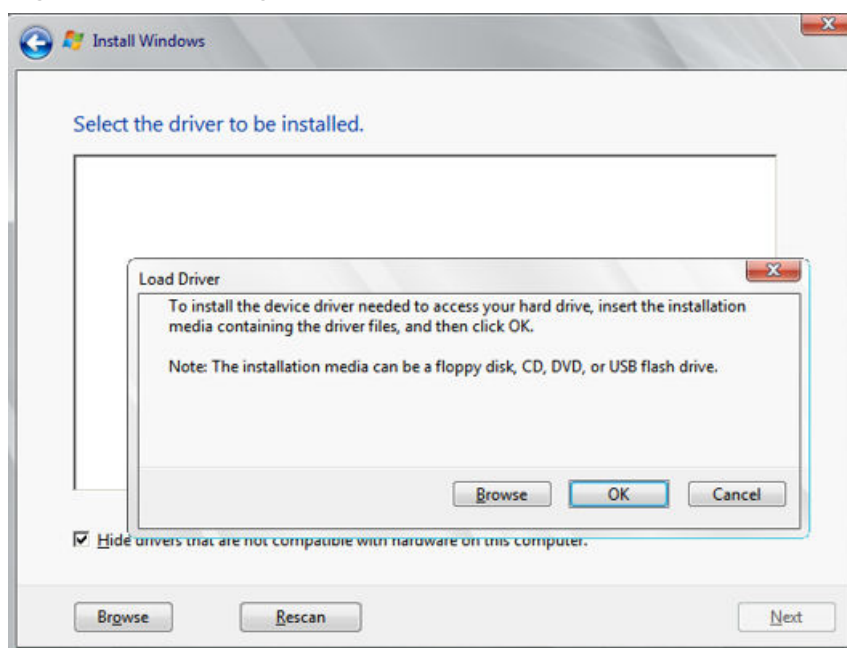
Figure 2-20 Installation path



- If a disk is displayed, go to [Step 1.9](#).

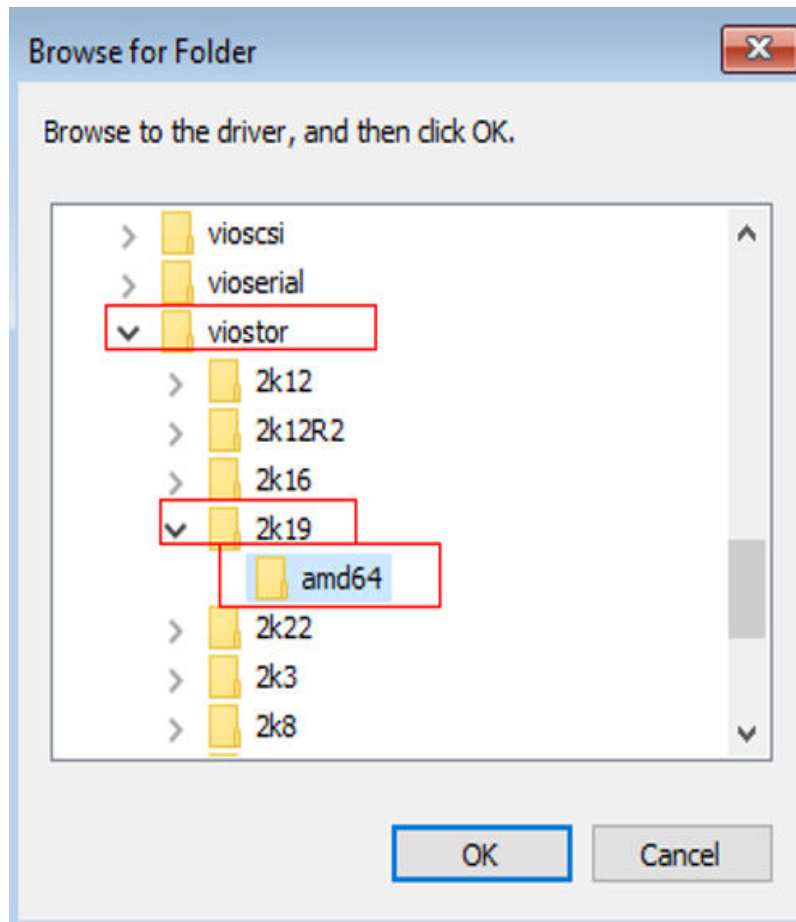
Figure 2-21 Installation path

7. Click **Load driver** and then **Browse**.

Figure 2-22 Loading drivers

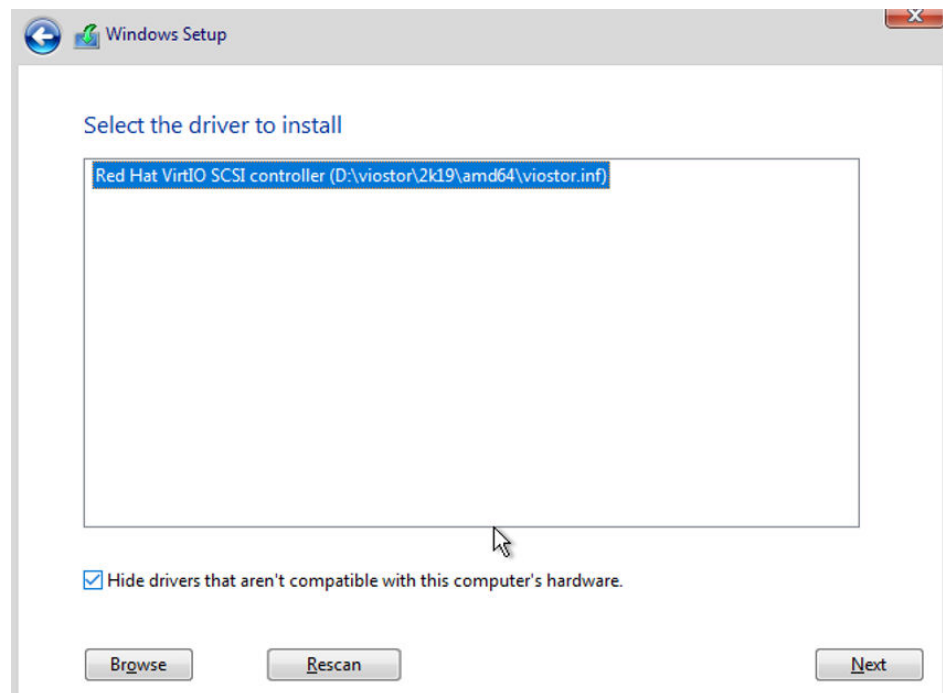
8. Select a driver based on the disk type.
 - If the disk type is VBD, choose **viostor > 2k19 > amd64** and click **OK**.

Figure 2-23 Browsing for a folder



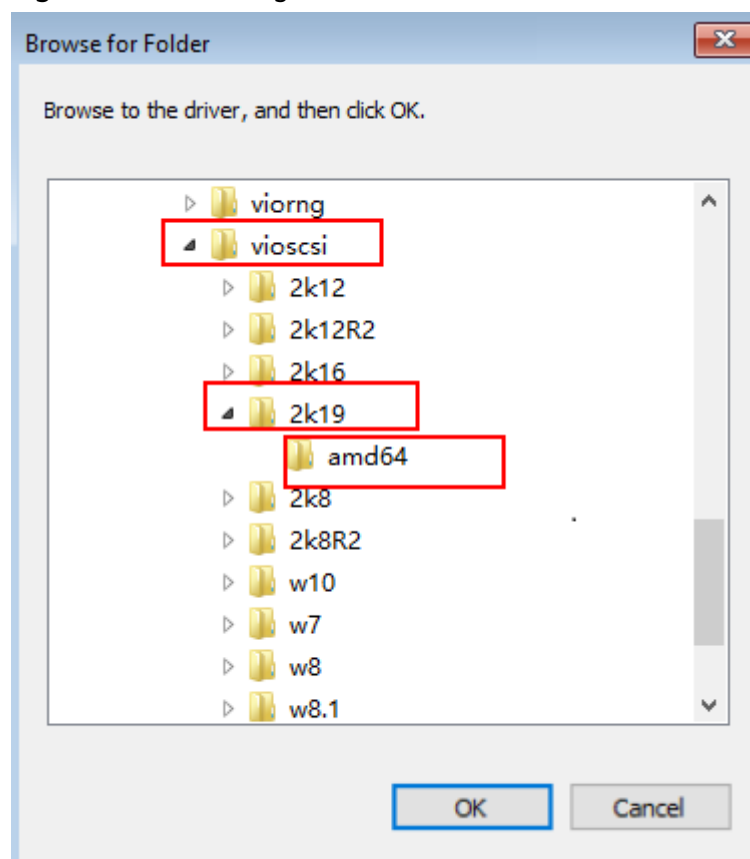
Select the **viostor.inf** driver and click **Next**.

Figure 2-24 Selecting the driver to install



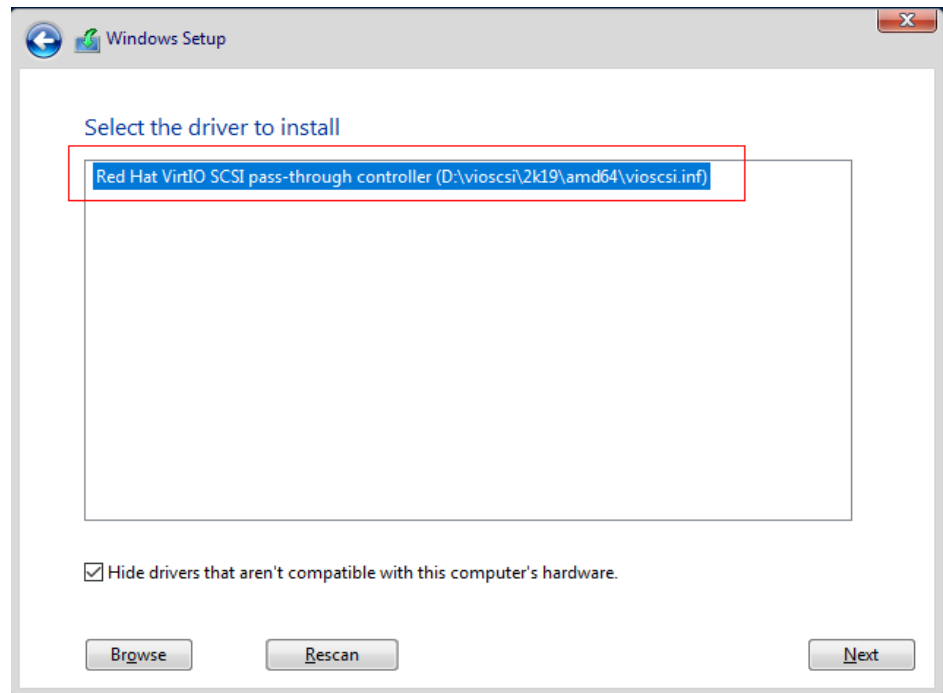
- If the disk type is SCSI, choose **vioscsi** > **2k19** > **amd64** and click **OK**.

Figure 2-25 Browsing for a folder



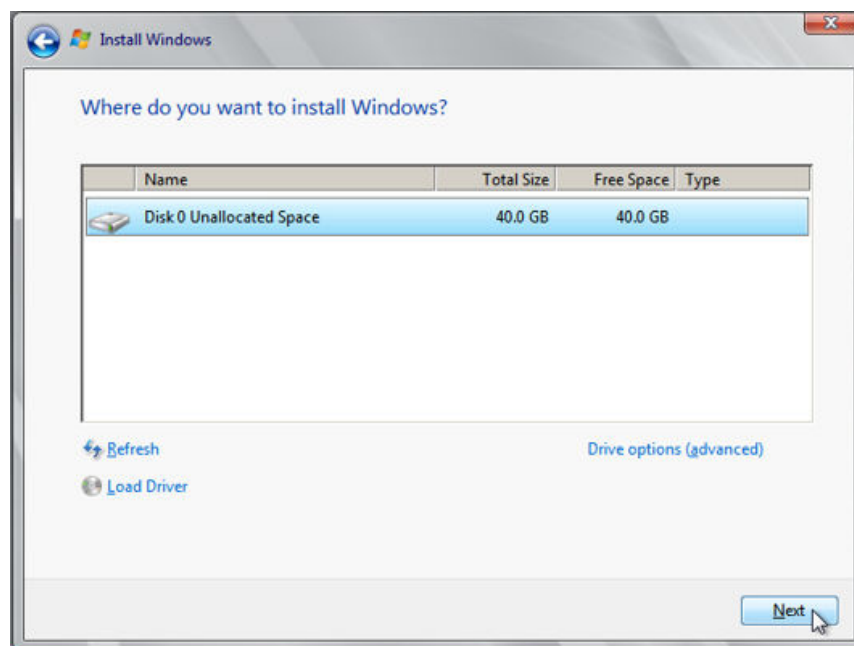
Select the **vioscsi.inf** driver and click **Next**.

Figure 2-26 Selecting the driver to install



9. Select the disk and click **Next**.

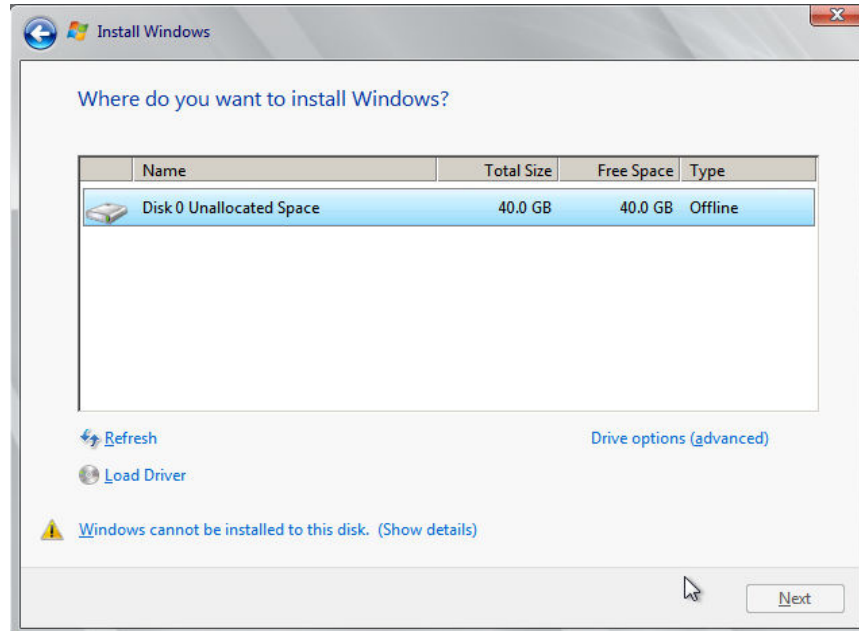
Figure 2-27 Installation path



 **NOTE**

If the disk type is **Offline**, you can stop and then start the ECS, and restart the OS installation process.

Figure 2-28 Offline disk



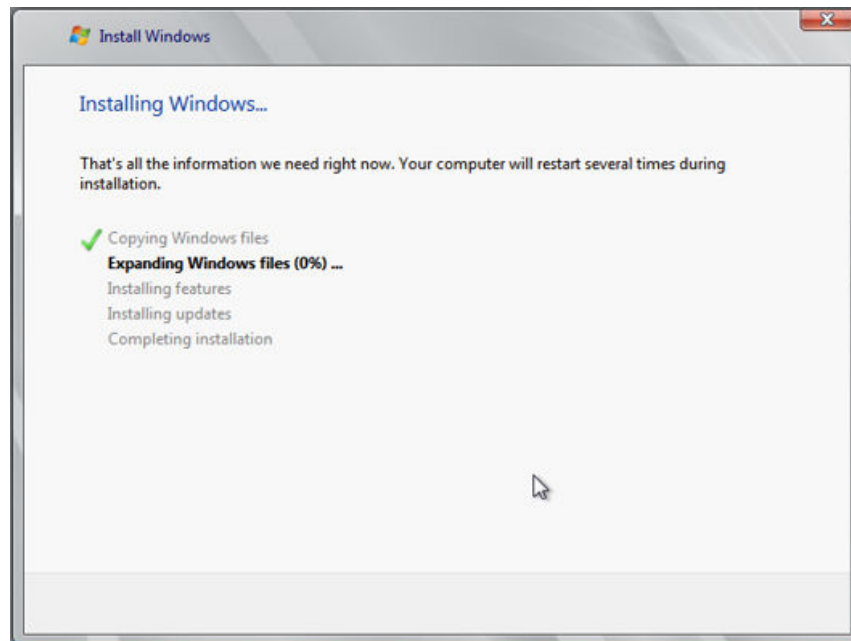
10. The **Installing Windows** window is displayed, and the OS installation starts. The installation takes about 50 minutes. The ECS restarts during the installation. After the ECS successfully restarts, log in to it again and configure the OS as prompted.

 **NOTE**

You are required to set a password for the OS user.

Supported special characters include !@\$%^_-=+[{]};.,/?

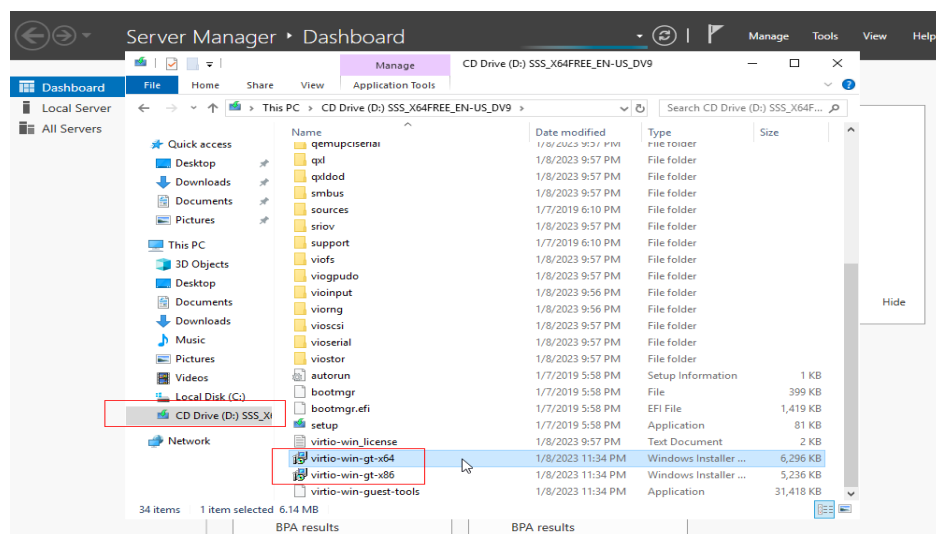
Figure 2-29 Installation progress



Step 2 Install drivers.

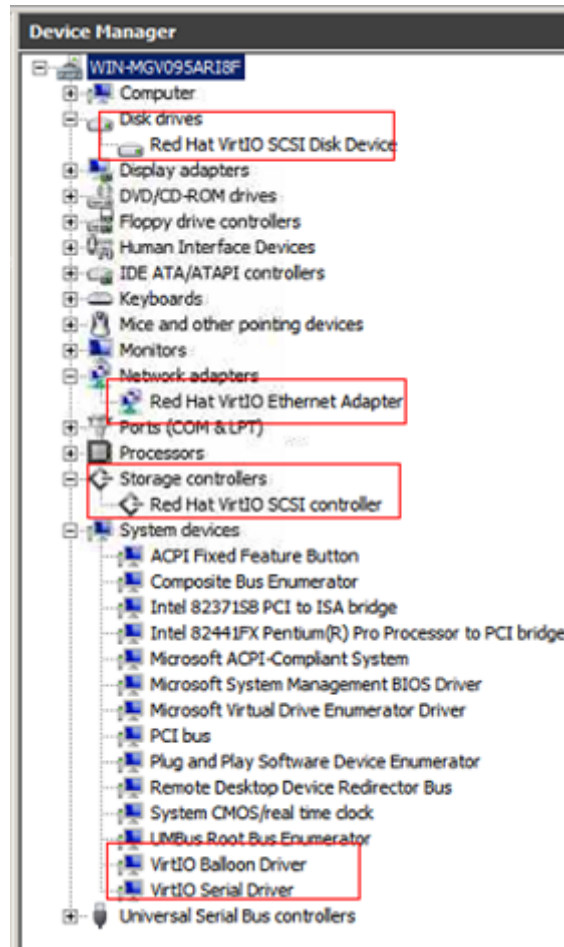
1. Open **Computer** and double-click the CD drive.

Figure 2-30 Starting the CD drive



2. Double-click **virtio-win-gt-x64** or **virtio-win-gt-x86**. Install drivers as prompted.
3. After the installation is complete, start **Device Manager** and check that all the drivers shown in the red box are successfully installed.

Figure 2-31 Device Manager

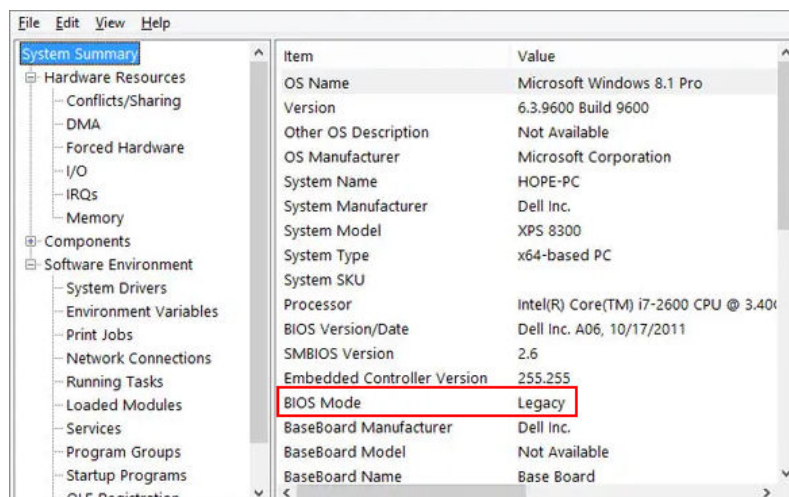


----End

Follow-up Procedure

Check whether the resolution can be changed. If it cannot, address it based on the system boot modes.

Hold down the **Windows** key and press **R** on your keyboard, enter **msinfo32** in the **Run** box, and press **Enter**. In the right pane of the **System Information** dialog box, locate **BIOS Mode**.



- If the value of **BIOS Mode** is **Legacy**, the system boot mode is BIOS. Go to the step for [configuring image information](#), select **BIOS** for **Boot Mode**.
- If the value of **BIOS Mode** is **UEFI**, address the resolution change failure by referring to

2.12.6 Configuring the ECS and Creating a Windows System Disk Image

Scenarios

After installing an OS for the temporary ECS, configure the ECS and install Guest OS drivers provided by the cloud platform so that ECSs that will be created with this temporary ECS as a source can work properly.

NOTE

The Guest OS drivers are VirtIO and PV drivers. VirtIO drivers have been installed on the ECS in the preceding section, so this section only describes how to install PV drivers.

This section describes how to configure a Windows ECS, install the Guest OS drivers, and create a Windows system disk image.

Procedure

Step 1 Configure the ECS.

1. Check whether NICs are set to DHCP. If the ECS is configured with a static IP address, change its IP address assignment mode to DHCP as instructed in [Setting the NIC to DHCP](#).
2. Enable remote desktop connection for the ECS as needed. For details about how to enable this function, see [Enabling Remote Desktop Connection](#).
3. Install PV drivers. For details, see [Installing PV Drivers](#).
After drivers are installed, you need to clear system logs. For details, see [Clearing System Logs](#).
4. Install and configure Cloudbase-Init. User data injection on the management console is available for the new ECSs created from the image only after this tool is installed. For example, you can use data injection to set the login

password for a new ECS. For details, see [Installing and Configuring Cloudbase-Init](#).

5. (Optional) Configure value-added functions.
 - Enable NIC multi-queue. For details, see [How Do I Enable NIC Multi-Queue for an Image?](#)
 - Configure dynamic assignment of IPv6 addresses. For details, see [How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses?](#)

Step 2 Stop the ECS to make the configurations take effect.

Step 3 Use the ECS to create a Windows system disk image.

For details, see [Creating a System Disk Image from a Windows ECS](#).

----End

Follow-up Procedure

After the system disk image is created, delete the temporary ECS in a timely manner to avoid generating any additional charges.

2.13 Creating a Linux System Disk Image from an ISO File

2.13.1 Overview

An ISO file is a disk image of an optical disc. A large number of data files can be compressed into a single ISO file. Likewise, to access the files stored in an ISO, the ISO file needs to be decompressed. For example, you can use a virtual CD-ROM to open an ISO file, or burn the ISO file to a CD or DVD and then use the CD-ROM to read the image.

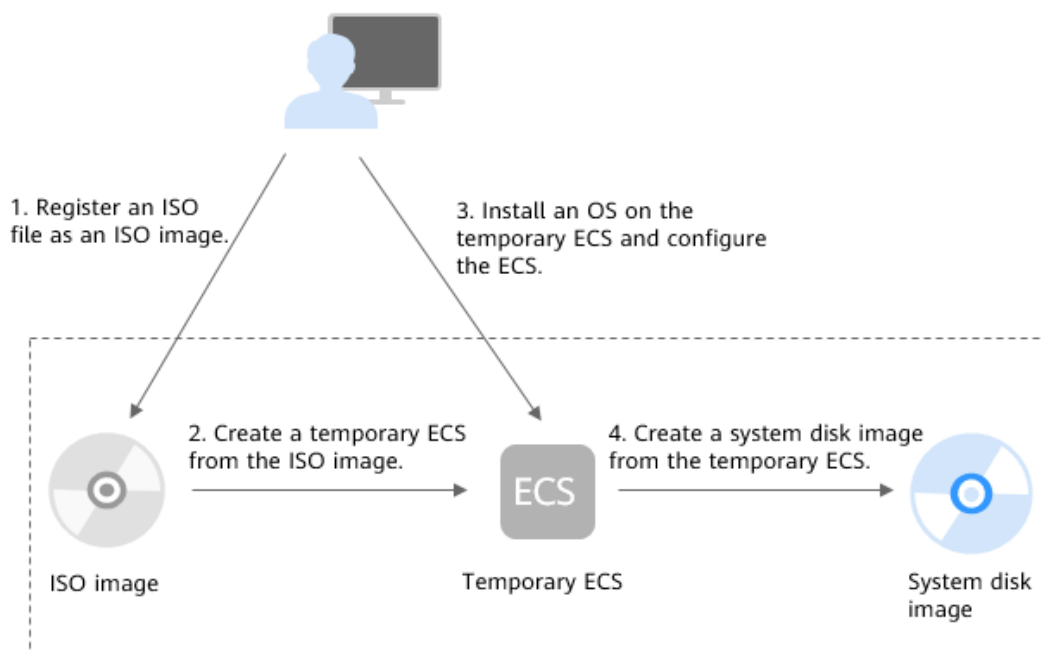
This section describes how to create a Linux system disk image using an ISO file.

NOTE

This section is applicable only to the management console. If you are an API user, see [Creating an Image from an ISO File](#).

Creation Process

[Figure 2-32](#) shows the process of creating a Linux system disk image from an ISO file.

Figure 2-32 Creating a Linux system disk image

The procedure is as follows:

1. Register an ISO file as an ISO image.
On the management console, register the prepared ISO file as an image. The image is an ISO image and cannot be used to provision ECSs. For details, see [Registering an ISO File as an ISO Image](#).
2. Create a temporary ECS from the ISO image.
Use the registered ISO image to create a temporary ECS. The ECS has no OS or driver installed. For details, see [Creating a Linux ECS from an ISO Image](#).
3. Install an OS and necessary drivers for the temporary ECS and configure related settings.
The operations include installing an OS, installing native Xen and KVM drivers, configuring NIC attributes, and deleting files from the network rule directory. For details, see [Installing a Linux OS](#) and [Step 1 in Configuring the ECS and Creating a Linux System Disk Image](#).
4. Create a system disk image from the temporary ECS.
On the management console, create a system disk image from the temporary ECS on which the installation and configuration have been completed. After the image is created, delete the temporary ECS to avoid generating any additional charges. For details, see [Creating a System Disk Image from a Linux ECS](#).

Constraints

- An ISO image created from an ISO file is used only for creating a temporary ECS. It will not be available on the ECS console. You cannot use it to create ECSs or change ECS OSs. You need to install an OS on the temporary ECS and use that ECS to create a system disk image which can be used to create ECSs or change ECS OSs.

- A temporary ECS has limited functionality. For example, you cannot attach disks to it. You are not advised to use it as a normal ECS.

2.13.2 Registering an ISO File as an ISO Image

Scenarios

Register an external ISO file on the cloud platform as a private image (ISO image). Before registering an image, upload the ISO file to the OBS bucket.

The ISO image cannot be replicated, exported, or encrypted.

Prerequisites

- The file to be registered must be in ISO format.
- The ISO image file has been uploaded to the OBS bucket. For details, see [Uploading an External Image File](#).

NOTE

The ISO image file name can contain only letters, digits, hyphens (-), and underscores (_). If the image file name does not meet the requirements, change the name before uploading the image file to the OBS bucket.

Procedure

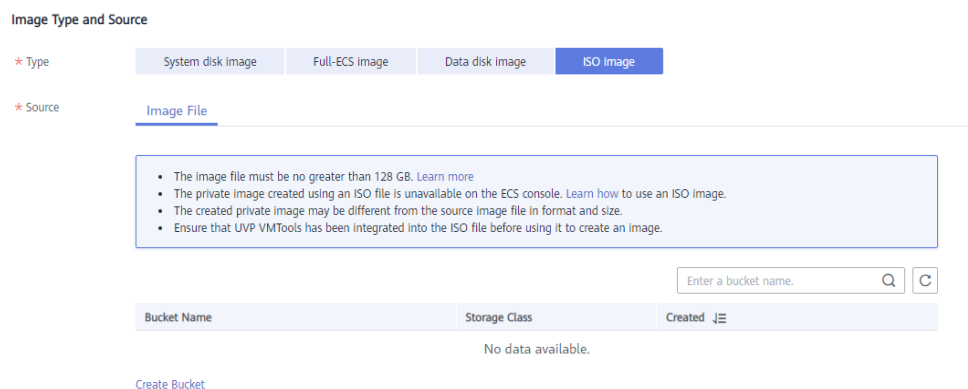
Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Register an ISO file as an ISO image.

1. Click **Create Image** in the upper right corner.
2. In the **Image Type and Source** area, select **ISO image** for **Type**.
3. In the image file list, select the bucket and then the image file.

Figure 2-33 Creating a private image from an ISO file



4. In the **Image Information** area, set the following parameters.

- **Architecture.** Select **x86** or **ARM**.

 **NOTE**

This parameter is required only in regions that support both x86 and Arm.

- **Boot Mode:** Select **BIOS** or **UEFI**. Ensure that the selected boot mode is the same as that in the image file, or the ECSs created from this image will not be able to boot up. The Arm architecture does not support the BIOS boot mode.

 **NOTE**

If the boot mode in the image file is **BIOS** but you select **UEFI** here for **Boot Mode**, you will not be able to adjust the resolution.

- **OS:** Select the OS specified in the ISO file. To ensure that the image can be created and used properly, select an OS consistent with that in the image file.
- **System Disk:** Set the system disk capacity (value range: 40 GB to 1024 GB), which must be no less than the capacity of the system disk in the image file.
- **Name:** Enter a name for the image to be created.
- **Enterprise Project:** Select the enterprise project to which your images belong.
- **Tag:** (Optional) Add a tag to the image to be created.
- **Description:** (Optional) Enter image description as needed.

5. Click **Next**.

6. Confirm the settings. Select **Statement of Commitment to Image Creation** and **Huawei Image Disclaimer**. Click **Submit**.

Step 3 Switch back to the **Image Management Service** page to check the image status.

When the image status changes to **Normal**, the image is registered successfully.

----End

2.13.3 Creating a Linux ECS from an ISO Image

Scenarios

This section describes how to create an ECS from a registered ISO image.

Procedure

Step 1 Access the IMS console.

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.

Step 2 Use an ISO image to create a Linux ECS.

1. Click the **Private Images** tab. Locate the row that contains the ISO image and click **Create ECS** in the **Operation** column.

The created ECS is for temporary use only and needs to be deleted when you are finished with it. The system creates a pay-per-use ECS with fixed specifications. When you use the private image created from this ECS to create new ECSs, you can customize the specifications and billing mode then.

2. Configure the ECS as prompted and click **OK**.

----End

Follow-up Procedure

After the ECS is created, you can log in remotely to continue with OS and drivers installation.

2.13.4 Installing a Linux OS

Scenarios

This section uses CentOS 7 64-bit as an example to describe how to install Linux on an ECS.

The installation procedure varies depending on the image file you use. Perform operations as prompted.

NOTE

Set the time zone, repo source update address, input method, language, and other items based on service requirements.

Prerequisites

You have remotely logged in to the ECS and entered the installation page.

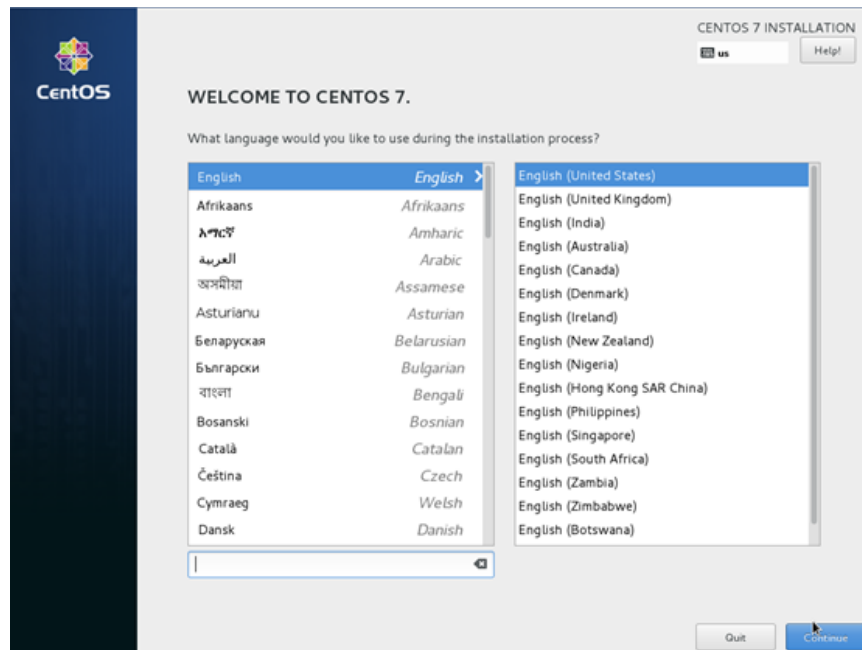
Procedure

CAUTION

Do not stop or restart the ECS during the OS installation. Otherwise, the OS installation will fail.

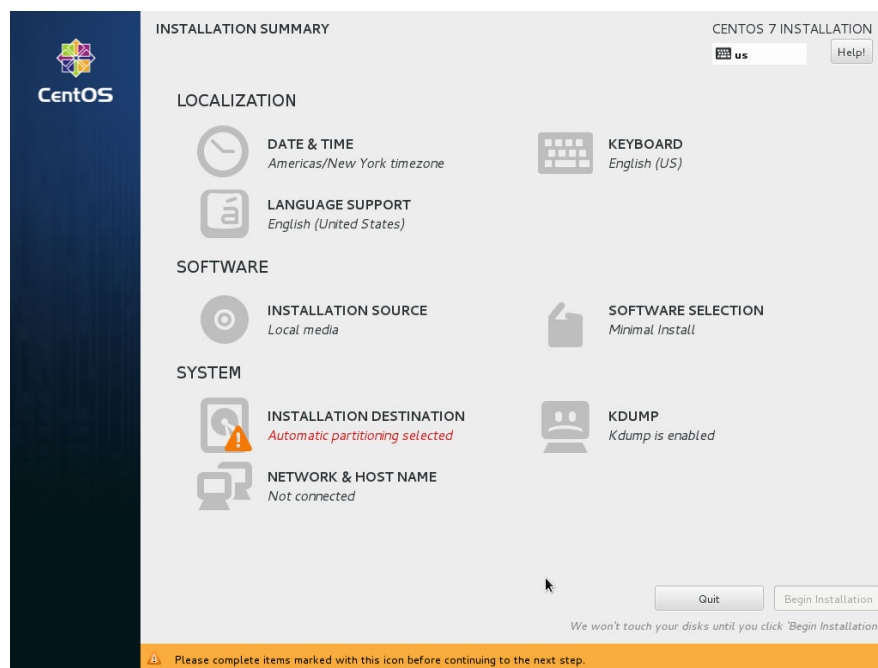
1. On the installation page, select the language and click **Continue**.

Figure 2-34 Installation page



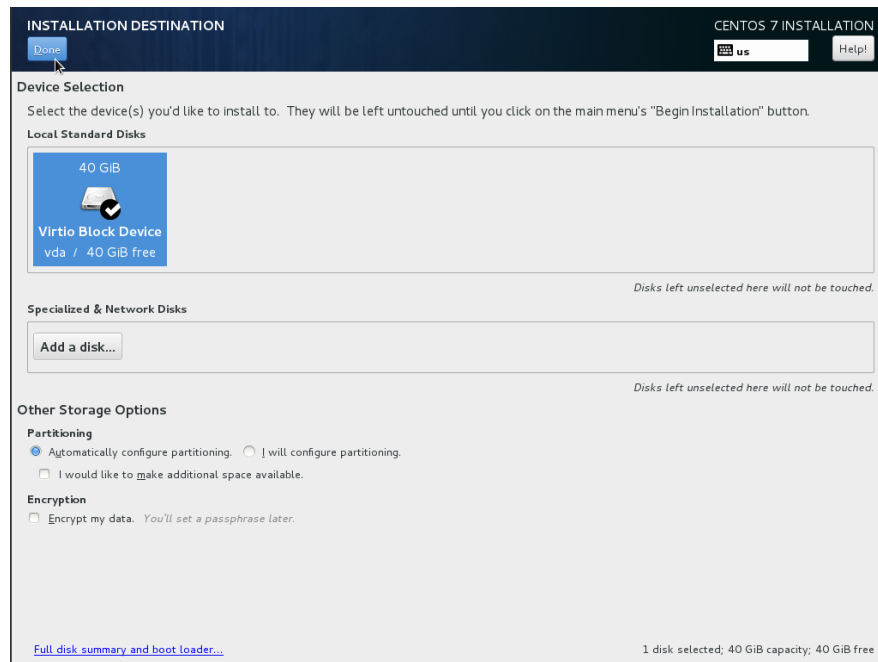
2. On the **INSTALLATION SUMMARY** page, choose **SYSTEM > INSTALLATION DESTINATION**.

Figure 2-35 INSTALLATION SUMMARY page



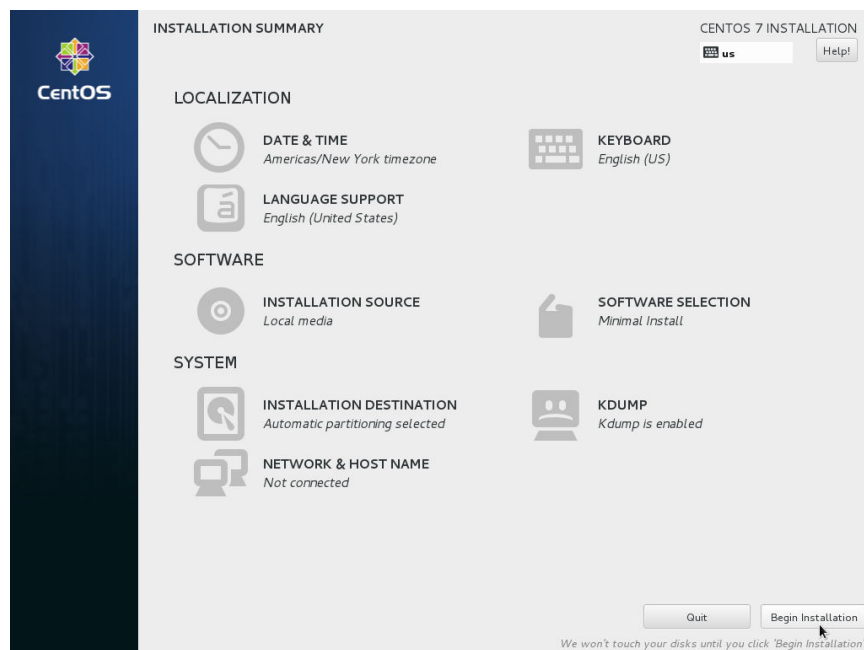
3. Select the target disk and click **Done**.

Figure 2-36 Installation location



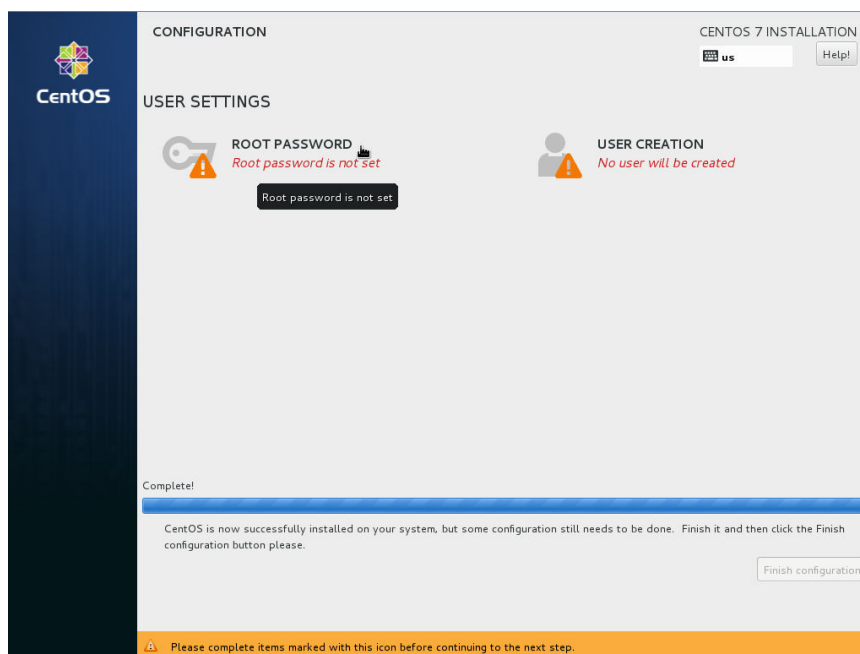
4. Click **Begin Installation**.

Figure 2-37 Starting installation



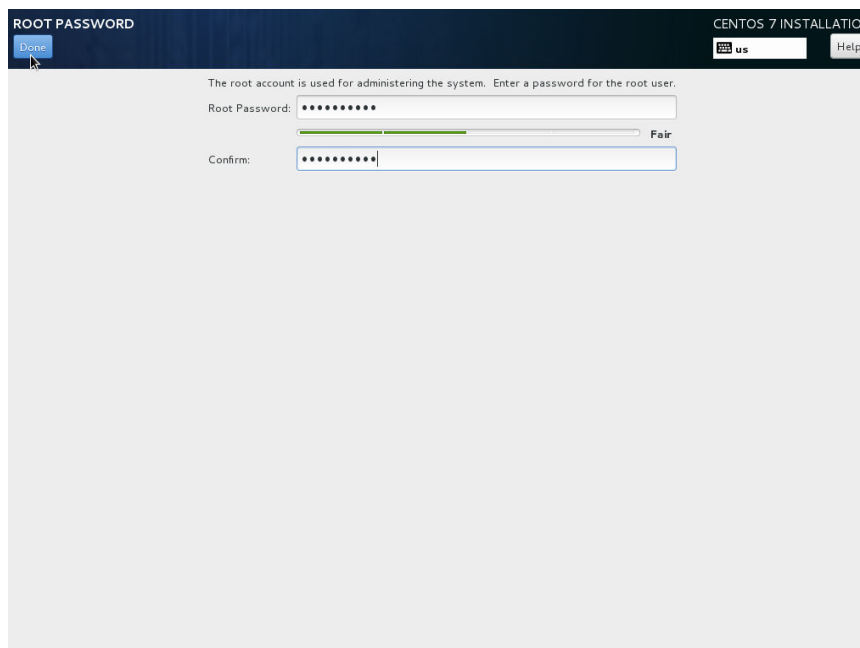
5. Wait for the automatic OS installation to complete. When the progress reaches 100%, CentOS is installed successfully.

Figure 2-38 Successful installation



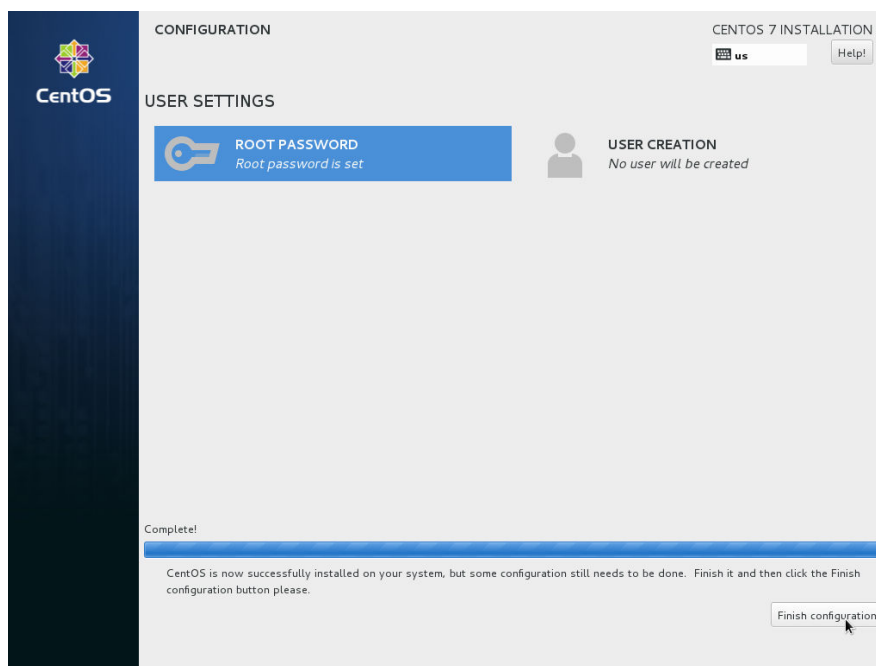
6. In the **USER SETTINGS** area, click **ROOT PASSWORD**.
The **ROOT PASSWORD** page is displayed.
7. Set a password for user **root** as prompted and click **Done**.

Figure 2-39 Setting a password for user root



8. Click **Finish configuration**.

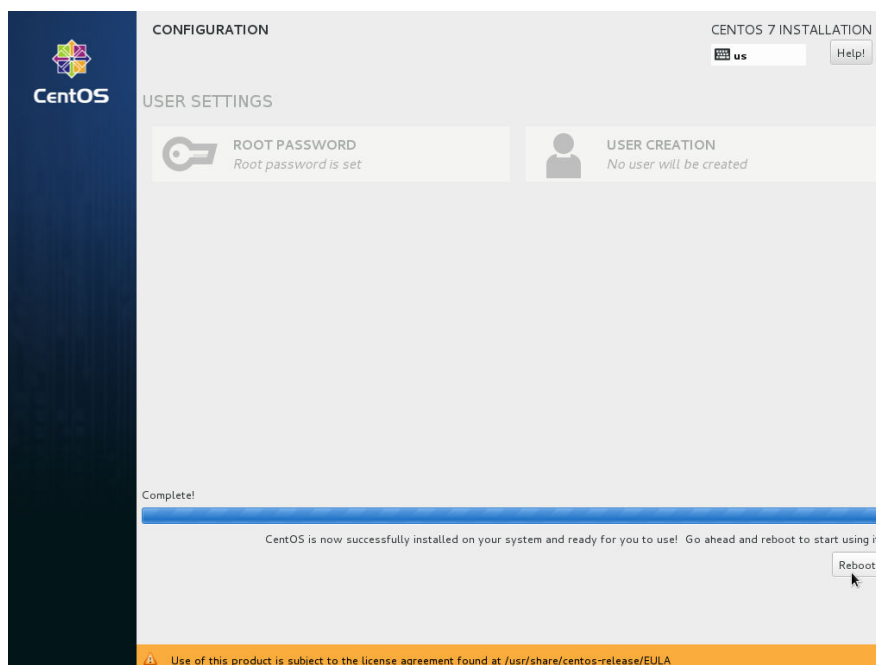
Figure 2-40 Completing configuration



9. Click **Reboot**.

If you are prompted to install the OS again after the ECS is restarted, exit the VNC login page and restart the ECS on the console.

Figure 2-41 Restarting the ECS



2.13.5 Configuring the ECS and Creating a Linux System Disk Image

Scenarios

After installing an OS for the temporary ECS, configure the ECS and install Xen and KVM drivers to ensure that ECSs created from this temporary ECS can work properly.

This section describes how to configure a Linux ECS, install drivers, and create a Linux system disk image.

Procedure

Step 1 Configure the ECS.

1. Configure the network.
 - Run the **ifconfig** command to check whether the private IP address of the ECS is the same as that displayed on the console. If they are inconsistent, delete files from the network rule directory as instructed in [Deleting Files from the Network Rule Directory](#).
 - Check whether NICs are set to DHCP. If the ECS is configured with a static IP address, change its IP address assignment mode to DHCP as instructed in [Setting the NIC to DHCP](#).
 - Run the **service sshd status** command to check whether SSH is enabled. If it is disabled, run the **service sshd start** command to enable it. Ensure that your ECS firewall, for example, Linux iptables, allows access to SSH.

2. Install drivers.

To ensure that the network performance and basic functions of the ECSs created from the private image are normal, install native Xen and KVM drivers on the ECS used to create the image. Before installing native Xen and KVM drivers, uninstall PV drivers.

NOTE

Disable your antivirus and intrusion detection software. You can enable them after the installation of Xen and KVM drivers.

- Uninstall PV drivers. For details, see [Uninstalling PV Drivers from a Linux ECS](#).
 - Install native Xen and KVM drivers. For details, see [How Do I Install Native Xen and KVM Drivers?](#)
 - After the drivers are installed, you need to clear log files and historical records. For details, see [Clearing System Logs](#).
3. Configure a file system.
 - Change the disk identifier in the GRUB configuration file to UUID. For details, see [Changing the Disk Identifier in the GRUB Configuration File to UUID](#).
 - Change the disk identifier in the fstab file to UUID. For details, see [Changing the Disk Identifier in the fstab File to UUID](#).
 - Clear the automatic mount configuration of non-system disks in the **/etc/fstab** file. For details, see [Detaching Data Disks from an ECS](#).

4. (Optional) Configure value-added functions.
 - Install and configure Cloud-Init. For details, see [Installing Cloud-Init](#) and [Configuring Cloud-Init](#).
 - Enable NIC multi-queue. For details, see [How Do I Enable NIC Multi-Queue for an Image?](#)
 - Configure dynamic assignment of IPv6 addresses. For details, see [How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses?](#)

Step 2 Create a Linux system disk image.

For details, see [Creating a System Disk Image from a Linux ECS](#).

----End

Follow-up Procedure

After the system disk image is created, delete the temporary ECS in a timely manner to avoid generating any additional charges.

2.14 Importing an Image

You need to prepare an image file that meets the platform requirements.

Constraints

- For details about the restrictions on Windows image files, see [Preparing an Image file \(Windows\)](#).
- For details about the restrictions on Linux image files, see [Preparing an Image file \(Linux\)](#).

NOTE

- You are advised to complete network, tool, and driver configurations on the source VM and then export the image file. You can also complete the configurations on the created ECSs. For details, see [What Do I Do If a Windows Image File Is Not Pre-Configured When I Use It to Register a Private Image?](#) and [What Do I Do If a Linux Image File Is Not Pre-Configured When I Use It to Register a Private Image?](#)
- Currently, a large image file (maximum: 1 TB) can be imported only in RAW or ZVHD2 format. In addition to meeting the requirements for common image files, a bitmap file needs to be generated alongside each RAW image file. The bitmap file will be uploaded together with the image file. For details, see [Fast Import of an Image File](#).

Import

IMS provides multiple methods for importing images. You can select a method based on the image file type, format, or size.

Table 2-14 Importing an image

| Format | File Size | Reference |
|---|------------------------|--|
| VMDK, VHD, QCOW2, VHDX, QED, VDI, QCOW, or ZVHD | Not larger than 128 GB | <ul style="list-style-type: none">• Creating a Windows System Disk Image from an External Image File• Creating a Linux System Disk Image from an External Image File• Creating a Data Disk Image from an External Image File |
| RAW or ZVHD2 | No larger than 1 TB | <ul style="list-style-type: none">• Creating a Data Disk Image from an External Image File |
| ISO | Not larger than 128 GB | <ul style="list-style-type: none">• Creating a Windows System Disk Image from an ISO File• Creating a Linux System Disk Image from an ISO File |

2.15 Fast Import of an Image File

2.15.1 Overview

If an image file is larger than 128 GB, you can import it using fast import.

Constraints

- The image file must be in RAW or ZVHD2 format.
- The image file size cannot exceed 1 TB.

Methods

You can import an image file in any of the following methods depending on the file format:

- ZVHD2
 - a. Optimize the image file.
 - b. Upload the image file to an OBS bucket.
 - c. Register the image file on the cloud platform.
- RAW
 - a. Optimize the image file.
 - b. Generate a bitmap file for the image file.
 - c. Upload the image file and bitmap file to an OBS bucket.
 - d. Register the image file on the cloud platform.
- Others

- If the file format is converted to ZVHD2:
 - i. Optimize the image file.
 - ii. Convert the image file format to ZVHD2.
 - iii. Upload the image file to an OBS bucket.
 - iv. Register the image file on the cloud platform.
- If the file format is converted to RAW:
 - i. Optimize the image file.
 - ii. Convert the image file format to RAW and generate a bitmap file for the image file.
 - iii. Upload the image file and bitmap file to an OBS bucket.
 - iv. Register the image file on the cloud platform.

 **NOTE**

- Fast import is used to quickly import large files. It depends on lazy loading which defers loading of file data until the data is needed. This reduces the initial loading time. However, RAW files do not support lazy loading. When you upload a RAW file, you need to upload its bitmap together.
- For details about how to optimize an image file, see [Optimization Process](#) (Windows) or [Optimization Process](#) (Linux) depending on the OS type specified in the image file.

Import Process

Assume that you need to convert the file format to ZVHD2 or RAW.

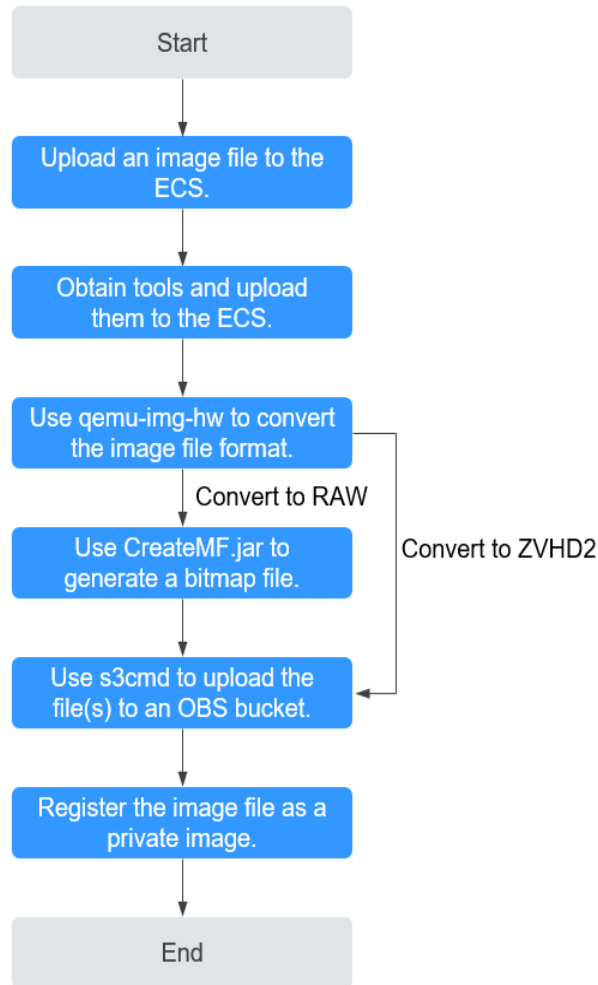
You can use **qemu-img-hw** or the open-source tool **qemu-img** to convert the image format. **qemu-img-hw** can only be used in Linux.

 **NOTE**

The tool package contains **qemu-img-hw** (for converting image formats) and **CreateMF.jar** (for generating bitmap files).

- Linux
You are advised to use an EulerOS ECS to convert the file format.

Figure 2-42 Import process (Linux)



For details, see [Fast Import in Linux](#).

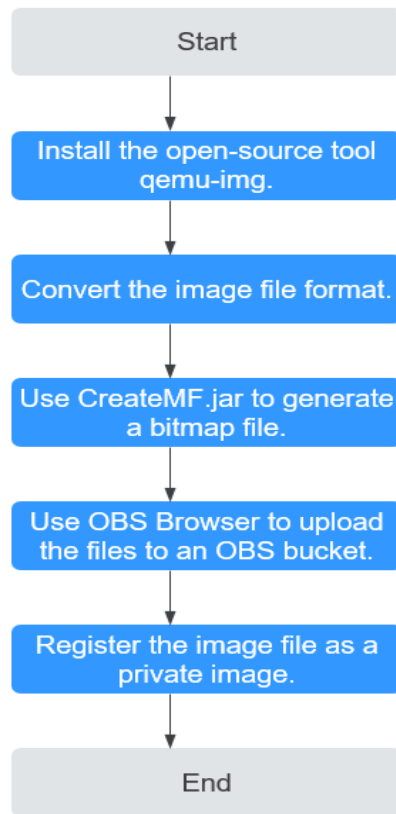
- Windows

You are advised to use a local PC running Windows to convert the file format.

NOTE

qemu-img cannot convert image files to the ZVHD2 format. You need to convert an image file to the RAW format and then use **CreateMF.jar** to generate a bitmap file.

Figure 2-43 Import process (Windows)



For details, see [Fast Import in Windows](#).

2.15.2 Fast Import in Linux

Scenarios

This section describes how to convert the format of a large image file on a Linux server and then quickly import it to the cloud platform. You are advised to use an EulerOS ECS for converting image file formats and generating bitmap files.

In Linux, you are advised to use **qemu-img-hw** to convert image formats.

Prerequisites

- The image file has been optimized. For details, see [Optimization Process \(Windows\)](#) or [Optimization Process \(Linux\)](#). Ensure that the image file meets the requirements in [Table 2-6 \(Windows\)](#) or [Table 2-10 \(Linux\)](#).

NOTE

Select the reference content based on the OS type in the image file.

- You have created an ECS running EulerOS on the management console and bound an EIP to the ECS.
- An OBS bucket has been created on the management console.

Procedure

Step 1 Upload an image file.

- If the image file is uploaded from a Linux PC, run the **scp** command.
For example, to upload **image01.qcow2** to the **/usr/** directory of the ECS, run the following command:
scp /var/image01.qcow2 root@xxx.xxx.xx.xxx:/usr/
xxx.xxx.xx.xxx indicates the EIP bound to the ECS.
- If the image file is uploaded from a Windows PC, use a file transfer tool, such as WinSCP, to upload the image file.

Step 2 Obtain the image conversion tool (**qemu-img-hw.zip**) and bitmap file generation tool (**createMF.zip**), upload them to the ECS, and decompress the packages.

Table 2-15 Tool packages

| Tool Package | How to Obtain |
|-----------------|---|
| qemu-img-hw.zip | https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/imageImportTools/qemu-img-hw.zip |
| createMF.zip | https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/imageImportTools/createMF.zip |

Step 3 Use **qemu-img-hw** to convert the image format.

1. Go to the directory where **qemu-img-hw** is stored, for example, **/usr/qemu-img-hw**.

```
cd /usr/qemu-img-hw
```

2. Run the following command to make **qemu-img-hw** executable:

```
chmod +x qemu-img-hw
```

3. Execute **qemu-img-hw** to convert the image file format to ZVHD2 (recommended) or RAW.

Command format:

```
./qemu-img-hw convert -p -O Target_image_format Source_image_file Target_image_file
```

For example, run the following command to convert an **image01.qcow2** file to an **image01.zvhd2** file:

```
./qemu-img-hw convert -p -O zvhd2 image01.qcow2 image01.zvhd2
```

- If the image file is converted to the ZVHD2 format, go to **Step 5**.
- If the image file is converted to the RAW format, go to **Step 4**.

Step 4 Use **CreateMF.jar** to generate a bitmap file.

1. Ensure that JDK has been installed on the ECS.

Run the following commands to check whether JDK is installed:

```
source /etc/profile
```

java -version

If a Java version is displayed, JDK has been installed.

2. Run the following command to enter the directory where **CreateMF.jar** is stored:

```
cd /usr/createMF
```

3. Run the following command to generate a bitmap file:

```
java -jar CreateMF.jar /Original RAW file path/Generated .mf file path
```

Example:

```
java -jar CreateMF.jar image01.raw image01.mf
```

**CAUTION**

- The generated .mf bitmap file must have the same name as the RAW image file. For example, if the image file name is **image01.raw**, the generated bitmap name is **image01.mf**.
-

Step 5 Use **s3cmd** to upload the file(s) to an OBS bucket.

1. Install **s3cmd** on the ECS.

If **s3cmd** has been installed, skip this step.

- a. Run the following command to install **setuptools**:

```
yum install python-setuptools
```

- b. Run the following command to install **wget**:

```
yum install wget
```

- c. Run the following commands to obtain the **s3cmd** software package:

```
wget https://github.com/s3tools/s3cmd/archive/master.zip  
mv master.zip s3cmd-master.zip
```

- d. Run the following commands to install **s3cmd**:

```
unzip s3cmd-master.zip  
cd s3cmd-master  
python setup.py install
```

2. Configure **s3cmd**.

Run the following command to configure **s3cmd**:

```
s3cmd --configure
```

Access Key: *Enter an AK.*

Secret Key: *Enter an SK.*

Default Region: *Enter the region where the bucket is located.*

S3 Endpoint: *Refer to the OBS endpoint.*

DNS-style bucket+hostname:port template for accessing a bucket: *Enter a server address with a bucket name, for example, mybucket.obs.myclouds.com.*

Encryption password: *Press Enter.*

Path to GPG program: *Press Enter.*

Use HTTPS protocol: *Specifies whether to use HTTPS. The value can be Yes or No.*

HTTP Proxy server name: *Specifies the proxy address used to connect the cloud from an external network. (If you do not need it, press Enter.)*

HTTP Proxy server port: *Specifies the proxy port used to connect to the cloud from an external network (If you do not need it, press Enter.)*

Test access with supplied credentials? *y*

(If "Success. Your access key and secret key worked fine :-)" is displayed, the connection is successful.)

Save settings? y (Specifies whether to save the configurations. If you enter y, the configuration will be saved.)

 NOTE

The configurations will be stored in `/root/.s3cfg`. If you want to modify these configurations, run the `s3cmd --configure` command to configure the parameters or run the `vi .s3cfg` command to edit the `.s3cfg` file.

3. Run the following command to upload the ZVHD2 image file (or the RAW image file and its bitmap file) to an OBS bucket.

```
s3cmd put image01.zvhd2 s3://mybucket/
```

 CAUTION

The `.mf` bitmap file must be in the same OBS bucket as the RAW image file.

Step 6 Register a private image.

You can register a private image using the converted ZVHD2 or RAW file on the console or using an API.

Method 1: Register a private image on the console.

1. Access the IMS console.
 - a. Log in to the management console.
 - b. Under **Compute**, click **Image Management Service**.
The IMS console is displayed.
2. In the upper right corner, click **Create Image**.
3. In the **Image Type and Source** area, select **System disk image** or **Data disk image** for **Type**.
4. Select **Image File** for **Source**. Select the bucket storing the ZVHD2 or RAW image file and then select the image file. If the image file is in the RAW format, you also need to select its bitmap file.
5. Select **Enable Fast Create**, and select the sentence following **Image File Preparation**.
6. Set parameters as prompted.

For details about the parameters, see [Registering an External Image File as a Private Image](#).

 CAUTION

- The OS must be the same as that in the image file.
- The system disk capacity must be greater than that specified in the image file.

Run the following command to check the system disk capacity in the image file:

```
qemu-img-hw info test.zvhd2
```

Method 2: Register a private image using an API.

The API is POST `/v2/cloudimages/quickimport/action`.


For details about how to call this API, see [Importing an Image File Quickly](#).

----End

Appendix 1: Common qemu-img-hw Commands

- Converting image file formats: `qemu-img-hw convert -p -O Target_image_format Source_image_file Target_image_file`
The parameters are described as follows:
`-p`: indicates the conversion progress.
The part following `-O` (which must be in upper case) consists of the target image format, source image file, and target image file.
For example, run the following command to convert a QCOW2 image file to a ZVHD2 file:
`qemu-img-hw convert -p -O zvhd2 test.qcow2 test.zvhd2`
- Querying image file information: `qemu-img-hw info Source_image_file`
An example command is `qemu-img-hw info test.zvhd2`.
- Viewing help information: `qemu-img-hw -help`

Appendix 2: Common Errors During qemu-img-hw Running

- Symptom:
The following information is displayed when you run the `qemu-img-hw` command:
`./qemu-img-hw: /lib64/libc.so.6: version `GLIBC_2.14' not found (required by ./qemu-img-hw)`
Solution:
Run the `strings /lib64/libc.so.6 | grep glibc` command to check the glibc version. If the version is too early, install the latest version. Run the following commands in sequence:
`wget http://ftp.gnu.org/gnu/glibc/glibc-2.15.tar.gz`
`wget http://ftp.gnu.org/gnu/glibc/glibc-ports-2.15.tar.gz`
`tar -xvf glibc-2.15.tar.gz`
`tar -xvf glibc-ports-2.15.tar.gz`
`mv glibc-ports-2.15 glibc-2.15/ports`
`mkdir glibc-build-2.15`
`cd glibc-build-2.15`
`../glibc-2.15/configure --prefix=/usr --disable-profile --enable-add-ons --with-headers=/usr/include --with-binutils=/usr/bin`
 NOTE
If `configure: error: no acceptable C compiler found in $PATH` is displayed, run the `yum -y install gcc` command.
`make`
`make install`
- Symptom:

The following information is displayed when you run the **qemu-img-hw** command:

```
./qemu-img-hw: error while loading shared libraries: libaio.so.1: cannot open shared object file: No such file or directory
```

Solution: Run the **yum install libaio** command first.

2.15.3 Fast Import in Windows

Scenarios

This section describes how to convert the format of an image file on a Windows server and then quickly import it to the cloud platform. You are advised to use a local Windows PC for converting image formats and generating bitmap files.

In Windows, use the open-source tool **qemu-img** to convert image formats. **qemu-img** supports conversion between image files of the VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, and QED formats. Convert an image to the RAW format and then use the **CreateMF.jar** tool to generate a bitmap file.

Prerequisites

- The image file has been optimized. For details, see [Optimization Process \(Windows\)](#) or [Optimization Process \(Linux\)](#). Ensure that the image file meets the requirements in [Table 2-6 \(Windows\)](#) or [Table 2-10 \(Linux\)](#).

NOTE

Select the reference content based on the OS type in the image file.

- An OBS bucket has been created on the management console, and OBS Browser+ has been ready.

Procedure

- Step 1** Install the open-source image conversion tool **qemu-img**. For details, see [Converting the Image Format Using qemu-img](#).
- Step 2** Run the **cmd** command to go to the **qemu-img** installation directory and run the **qemu-img** command to convert the image file to the RAW format.
- For example, run the following command to convert an **image.qcow2** file to an **image.raw** file:
- ```
qemu-img convert -p -O raw image.qcow2 image.raw
```
- Step 3** Use **CreateMF.jar** to generate a bitmap file.
- Obtain the **CreateMF.jar** package and decompress it.

**Table 2-16** CreateMF.jar package

| Tool Package | How to Obtain                                                                                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| createMF.zip | <a href="https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/imageImportTools/createMF.zip">https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/imageImportTools/createMF.zip</a> |

2. Ensure that JDK has been installed in the current environment.  
You can verify the installation by running **cmd.exe** and then **java -version**. If Java version information is displayed, JDK has been installed.
3. Go to the directory where **CreateMF.jar** is stored.  
For example, if you have downloaded **CreateMF.jar** to **D:/test**, run the following commands to access the directory:  
**D:**  
**cd test**
4. Run the following command to generate a bitmap file for the RAW image file:  
**java -jar CreateMF.jar D:/image01.raw D:/image01.mf**

---

 **CAUTION**

- The generated .mf bitmap file must have the same name as the RAW image file. For example, if the image file name is **image01.raw**, the generated bitmap name is **image01.mf**.
- 

**Step 4** Use OBS Browser+ to upload the converted image file and its bitmap file to an OBS bucket.

You must upload the RAW image file and its bitmap file to the same OBS bucket.

**Step 5** Register a private image.

You can register a private image using the converted ZVHD2 or RAW file on the console or using an API.

Method 1: Register a private image on the console.

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. In the upper right corner, click **Create Image**.
3. In the **Image Type and Source** area, select **System disk image** or **Data disk image** for **Type**.
4. Select **Image File** for **Source**. Select the bucket storing the ZVHD2 or RAW image file and then select the image file. If the image file is in the RAW format, you also need to select its bitmap file.
5. Select **Enable Fast Create**, and select the sentence following **Image File Preparation**.
6. Set parameters as prompted.  
For details about the parameters, see [Registering an External Image File as a Private Image](#).

 **CAUTION**

- The OS must be the same as that in the image file.
- The system disk capacity must be greater than that specified in the image file.

Run the following command to check the system disk capacity in the image file:

```
qemu-img-hw info test.zvhd2
```

---

Method 2: Register a private image using an API.

The API is POST /v2/cloudimages/quickimport/action.

For details about how to call this API, see [Importing an Image File Quickly](#).

----**End**

# 3 Managing Private Images

---

## 3.1 Modifying an Image

### Scenarios

You can modify the following attributes of a private image:

- Name
- Description
- Minimum memory
- Maximum memory
- NIC multi-queue

NIC multi-queue enables multiple CPUs to process NIC interrupts for load balancing. For details, see [How Do I Enable NIC Multi-Queue for an Image?](#)

- Boot mode

### Constraints

- You can only modify a private image in the **Normal** state.

### Procedure

Use any of the following methods to modify an image:

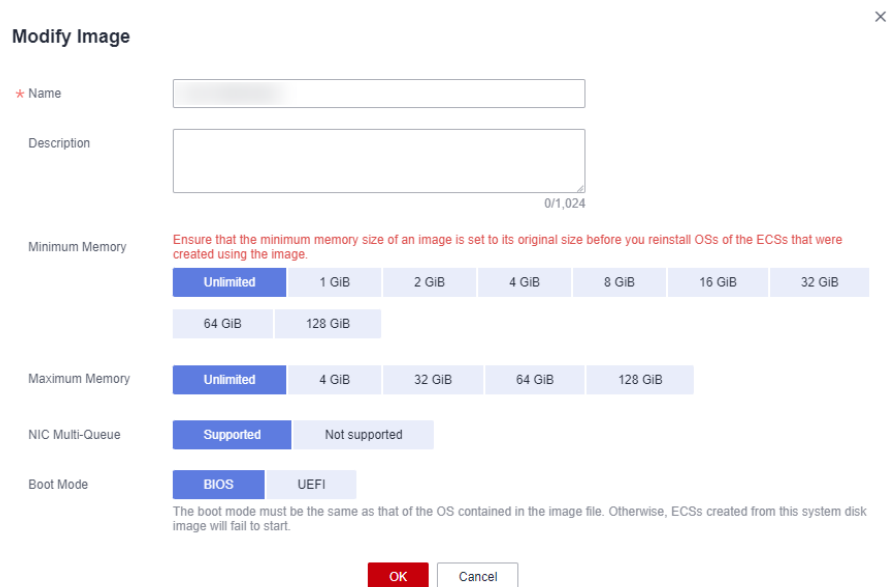
Method 1:

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Private Images** tab to display the image list.
3. Locate the row that contains the image and click **Modify** in the **Operation** column.



- In the **Modify Image** dialog box, modify the image.

**Figure 3-1** Modifying an image




Method 2:

- Access the IMS console.
  - Log in to the management console.
  - Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
- Click the **Private Images** tab to display the image list.
- On the image list, click the name of the target image.
- On the image details page, click **Modify** in the upper right corner. In the **Modify Image** dialog box, modify image attributes.

Method 3:

The system allows you to quickly change the name of a private image.

- Access the IMS console.
  - Log in to the management console.
  - Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
- Click the **Private Images** tab.
- In the private image list, locate the target image and move the cursor to the **Name** column.
- Click  to change the image name.
- Click **OK**.

## 3.2 Exporting Image List


### Scenarios

You can export the public or private image list in the current region as a CSV file to your local PC.

- For public images, the file describes the image name, image status, OS, image type, image creation time, system disk, and minimum memory.
- For private images, the file describes the image name, image ID, image status, OS, image type, image creation time, disk capacities, shared disks, image size, minimum memory, and encryption.

### Exporting Private Image Information

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.


2. Click the **Private Images** tab and click .  
The system will automatically export the private image list in the current region under your account to a local directory.

#### NOTE

The file name is in the format of **private-images-Region ID-Export time**.

### Exporting Public Image Information

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.

2. Click the **Public Images** tab and click .  
The system will automatically export all public images in the current region to a local directory.

#### NOTE

The file name is in the format of **public-images-Region ID-Export time**.

## 3.3 Checking the Disk Capacity of an Image

### Scenarios

You can check the disk capacity of a private image.

- To check the disk capacity of a system disk image, data disk image, or ISO image, see [Check the Disk Capacity of a System Disk Image, Data Disk Image, or ISO Image](#).
- To check the disk capacity of a full-ECS image, see [Check the Disk Capacity of a Full-ECS Image](#).

## Check the Disk Capacity of a System Disk Image, Data Disk Image, or ISO Image

Check the disk capacity in the **Disk Capacity** column of the private image list.

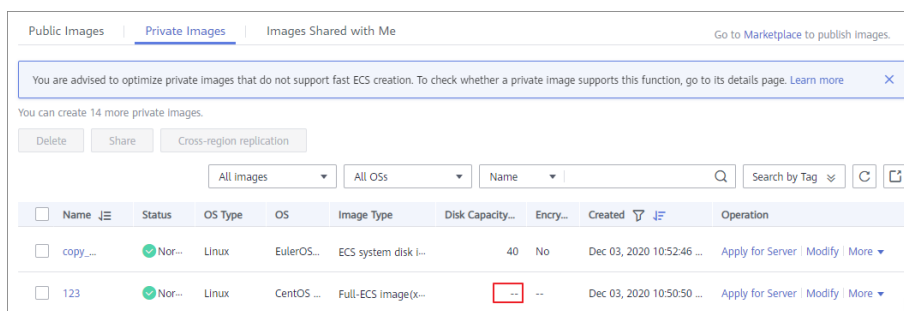
1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Private Images** tab to display the image list.
3. Check the value in the **Disk Capacity** column. The unit is **GB**.

## Check the Disk Capacity of a Full-ECS Image

The disk capacity of a full-ECS image is the sum of the system disk capacity and data disk capacity in the backup from which the full-ECS image is created.

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Private Images** tab to display the image list.  
The value in the **Disk Capacity** column is --.

**Figure 3-2** Checking the disk capacity of a full-ECS image



3. Click the full-ECS image name.
4. Click the **Backups** tab and view the capacities of the system disk and data disks in the backup.

Disk capacity of a full-ECS image = Capacity of the system disk in the backup + Capacity of data disks in the backup

For example:

- If the system disk capacity is 40 GB and no data disk is attached, the capacity of the full-ECS image disk is 40 GB.

- If the system disk capacity is 40 GB and data disk capacity is 40 GB, the full-ECS image disk capacity is 80 GB.

## 3.4 Creating an ECS from an Image

### Scenarios

You can use a public, private, or shared image to create an ECS.

- If you use a public image, the created ECS contains an OS and preinstalled public applications. You need to install applications as needed.
- If you use a private or shared image, the created ECS contains an OS, preinstalled public applications, and a user's personal applications.

### Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Public Images**, **Private Images**, or **Images Shared with Me** tab to display the image list.
3. Locate the row that contains your desired image and click **Apply for Server** in the **Operation** column.
4. For details about how to create an ECS, see [Purchasing an ECS](#).

When you use a system disk image to create an ECS, you can set the ECS specifications and system disk type without considering those in the image, but the system disk capacity can only be larger than that in the image.

When you use a full-ECS image to create an ECS, the system and data disk information defaulted by the image will be automatically displayed. You can increase the capacity of a system disk or data disks, but cannot decrease it.

#### NOTE

If a full-ECS image contains multiple data disks, it takes some time to load and display the disk information.

## 3.5 Deleting Images

### Scenarios

You can delete private images that will no longer be used.

- Deleted private images cannot be retrieved. Perform this operation only when absolutely necessary.
- After a private image is deleted, it cannot be used to create ECSs or EVS disks.
- After a private image is deleted, ECSs created from the image can still be used and are still billed. However, the OS cannot be reinstalled for the ECSs and ECSs with the same configuration cannot be created.

- Deleting the source image of a replicated image has no effect on the replicated image. Similarly, deleting a replicated image has no effect on its source.

## Constraints

- Private images that have been published in KooGallery cannot be deleted.

## Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Private Images** tab to display the image list.
3. Locate the row that contains the image, choose **More > Delete** in the **Operation** column.

### NOTE

To delete multiple images:

1. Select the images you want to delete in the image list.
  2. Click **Delete** above the image list.
4. (Optional) Select **Delete CSBS backups or cloud server backups of the full-ECS images**.

This parameter is available only when you have selected full-ECS images from the image list.

If you select this option, the system will delete CSBS or CBR backups of the full-ECS images. After the CSBS backups or CBR backups are deleted, they are no longer charged.

### NOTE

If CSBS or CBR backups failed to be deleted, the cause may be that these backups are being created and cannot be deleted. In this case, manually delete them as prompted.

5. Click **Yes**.

## 3.6 Sharing Images

### 3.6.1 Overview

You can share your private images with other tenants. The tenants who accept the shared images can use the images to create ECSs of the same specifications.

---

#### CAUTION

The cloud platform is not responsible for the integrity or security of shared images. When you use a shared image, ensure that the image is from a trusted sharer.

---

## Constraints

- You can share images only within the region where they reside.
- A system disk image or data disk image can be shared with up to 128 tenants, and a full-ECS image can be shared with up to 10 tenants.
- A full-ECS image is shareable only when it is created from a CBR backup or from an ECS that has never had a CSBS backup.

## Procedure

If you want to share a private image with another tenant, the procedure is as follows:

1. You obtain the project ID from the tenant.
2. You share an image with the tenant.
3. The tenant accepts the shared image.

After accepting the image, the tenant can use it to create ECSs.

## Related FAQs

If you have any questions, see [Image Sharing FAQs](#).

## 3.6.2 Obtaining the Project ID

### Scenarios

Before a tenant shares an image with you, you need to provide your project ID.

### Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the username in the upper right corner and select **My Credentials** from the drop-down list.

On the **My Credentials** page, view the project ID.

Images can be shared only within the region where they reside. So, obtain the project ID in the same region.

## 3.6.3 Sharing Specified Images

### Scenarios

After obtaining the project ID from a tenant, you can share specified private images with the tenant. You can share a single image or multiple images as needed.

## Prerequisites

- You have obtained the project ID from the target tenant.
- Before sharing an image, ensure that any sensitive data has been deleted from the image.

## Procedure

- Share multiple images.
  - a. Access the IMS console.
    - i. Log in to the management console.
    - ii. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
  - b. Click the **Private Images** tab.
  - c. Select the private images to share and click **Share** above the image list.
  - d. In the **Share Image** dialog box, enter the project ID of the target tenant.  
To share images with more than one tenant, separate their project IDs with commas (,).

### NOTE

- You can enter a maximum of 100 project IDs at a time.
- You can share images only within the region where they reside.
- If the target tenant is a multi-project user, you can share images to any project of the tenant.

- e. Click **OK**.
- Share a single image.
    - a. Access the IMS console.
      - i. Log in to the management console.
      - ii. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
    - b. Click the **Private Images** tab.
    - c. Locate the row that contains the private image you are to share, click **More** in the **Operation** column, and select **Share** from the drop-down list.
    - d. In the **Share Image** dialog box, enter the project ID of the target tenant.  
To share an image with more than one tenant, separate their project IDs with commas (,).

### NOTE

- You can enter a maximum of 100 project IDs at a time.
- You can share images only within the region where they reside.
- If the target tenant is a multi-project user, you can share images to any project of the tenant.

- e. Click **OK**.

## Related Operations

After you share images with a tenant, the tenant can accept the shared images on the **Images Shared with Me** page on the IMS console. For detailed operations, see [Accepting or Rejecting Shared Images](#).

### 3.6.4 Accepting or Rejecting Shared Images

#### Scenarios

After another tenant shares images with you, you will receive a message. You can choose to accept or reject all or some of the shared images.

#### NOTE

- If you are not in the same region as the tenant sharing the images with you, you will not receive the message.

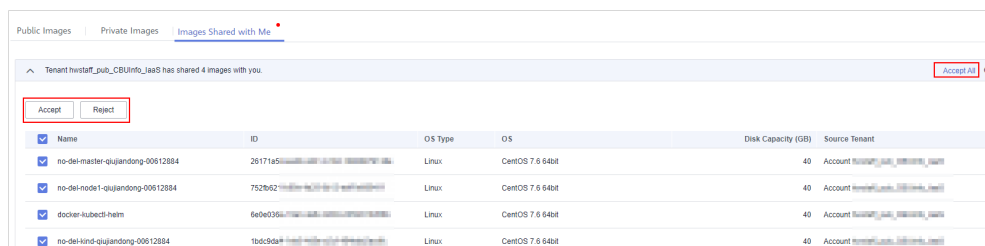
#### Prerequisites

- Another tenant has shared images with you.
- If the shared image is a full-ECS image, you need to create a server backup vault to store the full-ECS image and the backups of the full-ECS image before accepting the shared image. When creating a server backup vault, set **Protection Type** to **Backup**.

#### Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. In the upper left corner, switch to the region where the target project is and then select the project.
3. Click the **Images Shared with Me** tab.  
A message is displayed above the image list asking you whether to accept the shared images.
  - To accept all the shared images, click **Accept All** in the upper right corner.
  - To accept some images, select the images and click **Accept**.
  - To reject some images, select the images and click **Reject**.

**Figure 3-3** Accepting or rejecting shared images





 **NOTE**

If no message is displayed, check whether you have selected a correct region.

4. (Optional) In the **Accept Full-ECS Image** dialog box, select a server backup vault with the **Backup** protection type and click **OK**.

This dialog box is displayed when the shared image is a full-ECS image.

When accepting a full-ECS image, you must specify a vault for storing the CBR backups associated with the full-ECS image. The vault capacity must be no less than the total capacities of the system disk and data disk backups.

 **NOTE**

For more information about server backup vaults, see [What Is CBR?](#)

## Results

- **Pending:** If you do not immediately accept or reject a shared image, the image is in the **Pending** state.  
A pending shared image is not displayed in the shared image list.
- **Accepted:** After an image is accepted, it is displayed in the shared image list. You can use the image to create ECSs.
- **Rejected:** After an image is rejected, it is not displayed in the shared image list. You can click **Rejected Images** to view the images you have rejected and you can still choose to accept them.

## Follow-up Procedure

After accepting a system disk image shared by another tenant, you can:

- Use the image to create one or more ECSs (select **Shared Image** during ECS creation). For details, see [Purchasing an ECS](#).
- Use the image to change the OS of existing ECSs. For details, see [Changing the OS](#).

**Figure 3-4** Changing the OS

Change OS ×

Selected specifications s3.small.1 | 1 vCPUs | 1 GB

Current Image EulerOS 2.2 64bit  
System Disk Capacity: 40 GB OS Bit: 64-bit

Select an image

Image Type Public image Private image **Shared image** Marketplace image

Image  ↕

Login Mode **Password** Key pair

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

**OK** Cancel

After accepting a data disk image shared by another tenant, you can use the image to create EVS disks (locate the row that contains the image and click **Create Data Disk** in the **Operation** column).

## 3.6.5 Rejecting Accepted Images

### Scenarios

You can reject accepted images if you no longer need them.

After an image is rejected, it will not be displayed on the **Images Shared with Me** page.

### Prerequisites

You have accepted images shared by other users.

### Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Images Shared with Me** tab.
3. Determine the next step based on how many images you are to reject.
  - To reject multiple images: select the images to be rejected and click **Reject** above the image list. In the displayed dialog box, click **Yes**.

- To reject a specific image: locate the image to be rejected and choose **More > Reject** in the **Operation** column. In the displayed dialog box, click **Yes**.

## 3.6.6 Accepting Rejected Images

### Scenarios

If you want to use the shared images you have rejected, you can accept them from the list of rejected images.

### Prerequisites

- You have rejected the images shared by others.
- The image owners have not stopped sharing the images.

### Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Images Shared with Me** tab.

**Figure 3-5** Images Shared with Me

| <input type="checkbox"/> | Name              | OS Type | OS               | Image Type            | Disk Capacity | Source Tenant | Source Project | Source project ID  | Operation             |
|--------------------------|-------------------|---------|------------------|-----------------------|---------------|---------------|----------------|--------------------|-----------------------|
| <input type="checkbox"/> | data_disk_image   | Linux   | -                | Data disk image       | 100           | Account*      | cn-north-1     | 0503dda89700fed... | Create Data Disk More |
| <input type="checkbox"/> | discuz_centos6... | Linux   | CentOS 6.5 64bit | ECS system disk im... | 40            | Account*      | cn-north-1     | 0503dda89700fed... | Apply for Server More |

3. Click **Rejected Images**. All the rejected images are displayed.
4. Select the images you want to accept and click **Accept**.
5. Check the accepted images in the shared image list.

## 3.6.7 Stopping Sharing Images

### Scenarios

You can stop sharing images. After you stop sharing an image:

- The image will be invisible to the recipient on the management console and no data will be returned when the recipient query the image through an API.
- The recipient cannot use the image to create an ECS or EVS disk, or change the OS of an ECS.
- The recipient cannot reinstall the OS of the ECSs created from the shared image or create instances identical with these ECSs.

## Prerequisites

You have shared private images with others.

## Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Private Images** tab.
3. Locate the row that contains the private image that you no longer want to share, and choose **More > Share** in the **Operation** column.
4. In the **Share Image** dialog box, click the **Stop Sharing** tab.
5. Select the project for which you want to stop the image sharing and click **OK**.

## 3.6.8 Adding Tenants Who Can Use Shared Images

### Scenarios

In addition to the tenants you have shared images with, you can add more tenants who can use the shared images.

### Prerequisites

- You have shared private images.
- You have obtained the project IDs of the tenants to be added.

### Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Private Images** tab.
3. Click the image name to view image details.
4. Click **Add Tenant**.
5. In the **Add Tenant** dialog box, enter the project ID of the tenant to be added, and click **OK**.

To add multiple tenants, enter their project IDs and separate them with commas (,). Click **OK**.

#### NOTE

- You can share images only within the region where they reside.
- A project ID uniquely identifies a tenant in a specific region. If you enter a project ID that belongs to a different region from the images, a message will display indicating that the tenant cannot be found.

## 3.6.9 Deleting Image Recipients Who Can Use Shared Images

### Scenarios

This section describes how to delete image recipients who can use shared images.

### Prerequisites

- You have shared private images.
- You have obtained the project IDs of the image recipients.

### Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Private Images** tab.
3. Click the image name to view image details.
4. View the tenants who can use shared image.
5. Delete one or all of the recipients:
  - To delete a single image recipient, locate the target recipient and click **Delete**.
  - To delete all image recipients, click **Delete All** above the image recipient list.
6. Click **Yes**.

## 3.6.10 Replicating a Shared Image

### Scenarios

Replicate a private image that was shared with you. The image is displayed in the private image list. You can export, share, and replicate this image, or use it to create ECSs.

### Constraints

- Currently, only system and data disk images can be replicated. Full-ECS images are not supported.
- Currently, images can only be replicated within a region.
- An image to be replicated cannot be larger than 128 GB.
- An image cannot be replicated to generate an encrypted image.

### Procedure

1. Access the IMS console.
  - a. Log in to the management console.

- b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. On the displayed IMS console, click the **Images Shared with Me** tab.  
Shared images that are accepted are displayed.
3. Locate a shared image, click **More** in the **Operation** column, and select **Replicate** from the drop-down list.

**Figure 3-6** Replicating an image

**Replicate Image** ×

• The image size must be less than 128 GB.

**Image Details**

|            |                  |            |                                 |
|------------|------------------|------------|---------------------------------|
| Name       | image-001        | Image Type | ECS system disk image           |
| Image Size | 1.56 GB          | OS Type    | Linux                           |
| OS         | CentOS 7.3 64bit | Created    | Mar 16, 2022 15:35:16 GMT+08:00 |

\* Name

\* Enterprise Project  C ?

Description   
0/1,024

4. In the **Replicate Image** dialog box, specify **Name**, **Enterprise Project**, and **Description**.
  5. Click **OK**.
- You can click the **Private Images** tab and view the creation progress of the image in the private image list. When the image status changes to **Normal**, the image creation is complete.

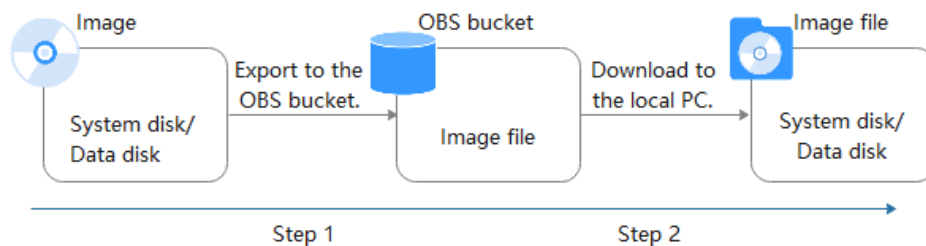
## 3.7 Exporting an Image

### Scenarios

You can export a private image to a standard OBS bucket and then download it to your local PC.

### Background

- You can reproduce cloud servers and their running environments in on-premises clusters or private clouds by exporting their images from the cloud platform. The following figure shows the process of exporting an image.

**Figure 3-7** Exporting an image

- The time required for exporting an image depends on the image size and the number of concurrent export tasks.
- You can export images in ZVHD2, QCOW2, VMDK, VHD, or ZVHD format. The default format of a private image is ZVHD2. Images exported in different formats may vary in size.
- If an image is larger than 128 GB, you can select **Enable** for **Fast Export** when exporting the image to an OBS bucket. The image will be exported as a ZVHD2 file. You can convert the image format after it is exported.

**NOTE**

is unavailable for encrypted images. To export an encrypted image, decrypt it first.

## Constraints

- An image can only be exported to a Standard bucket that is in the same region as the image.
- The following private images cannot be exported:
  - Full-ECS images
  - ISO images
  - Private images created from an Ubuntu public image
- The image size must be less than 1 TB. Images larger than 128 GB support only fast export.

## Prerequisites

- You have Administrator permissions for OBS.
- An OBS bucket is available in the region where the private image is located. If no OBS bucket is available, create one by referring to [Creating a Bucket](#). Select **Standard** for **Storage Class**.

**NOTE**

You will be charged for storing exported images in the OBS bucket. For details, see [OBS Pricing Details](#).


## Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.

2. Locate the row that contains the image to be exported, click **More** in the **Operation** column and select **Export**.
3. In the displayed **Export Image** dialog box, set the following parameters:
  - **Fast Export:** To export an image larger than 128 GB, you must enable fast export, and you cannot specify the format of the exported image (which can only be ZVHD2). After exporting the image, you can use **qemu-img-hw** to convert it to your desired format. For details, see [Converting the Image Format Using qemu-img-hw](#).

 NOTE

For details about differences between export and fast export, see [Comparison Between Import and Fast Import, and Between Export and Fast Export](#).

- **Format:** Select one from **qcow2**, **vmdk**, **vhd**, and **zvhd** as you need.
- **Name:** Enter a name that is easy to identify.
- **Storage Path:** Click  to expand the bucket list and select an OBS bucket for storing the exported image.

 NOTE

An image can only be exported to a Standard bucket that is in the same region as the image. So, only such buckets are available in the list.

4. Click **OK**.  
You can view the image export progress above the private image list.

## Follow-up Procedure

After the image is exported successfully, you can download it from the OBS bucket through the management console or OBS Browser+. For details, see [Downloading a File](#).

## 3.8 Optimizing a Windows Private Image

### 3.8.1 Optimization Process

An ECS can run properly only after Xen Guest OS drivers (PV drivers) and KVM Guest OS drivers (VirtIO drivers) are installed on it. To ensure that ECSs support both Xen and KVM and to improve network performance, PV and VirtIO drivers must be installed for the image.

1. Create an ECS from the Windows private image to be optimized and log in to the ECS.
2. Install the latest version of PV drivers on the ECS.  
For details, see [Installing PV Drivers](#).
3. Install VirtIO drivers that are needed to create KVM ECSs.  
For details, see [Installing VirtIO Drivers](#).
4. On the ECS, choose **Control Panel > Power Options**. Click **Choose when to turn off the display**, select **Never** for **Turn off the display**, and save the changes.



5. Clear system logs and then stop the ECS.  
For details, see [Clearing System Logs](#).
6. Create a Windows private image from the ECS.

### 3.8.2 Viewing the Virtualization Type of a Windows ECS

Open the cmd window and run the following command to query the virtualization type of the ECS:

#### systeminfo

If the values of **System Manufacturer** and **BIOS Version** are **Xen**, the ECS uses Xen. To make the Windows private image support KVM at the same time, perform operations in the following sections on the ECS.

#### NOTE

If the ECS uses KVM, you are also advised to optimize the private image to prevent any exceptions with the ECSs created from the image.

**Figure 3-8** Viewing the virtualization type of a Windows ECS

```

systeminfo
Host Name: ECS-E5AF
OS Name: Microsoft Windows Server 2012 R2 Datacenter
OS Version: 6.3.9600 N/A Build 9600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00253-50000-00000-AA442
Original Install Date: 11/2/2015, 21:05:21
System Boot Time: 8/2/2018, 10:31:04
System Manufacturer: Xen
System Model: HVM domU
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
 [01]: Intel64 Family 6 Model 62 Stepping 4 GenuineIn
 tel ~3200 Mhz
BIOS Version: Xen 4.1.2_115-908.762., 3/21/2018
Windows Directory: C:\windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Total Physical Memory: 1.016 MB
Available Physical Memory: 226 MB
Virtual Memory: Max Size: 1.336 MB
Virtual Memory: Available: 476 MB
Virtual Memory: In Use: 860 MB

```

### 3.8.3 Obtaining Required Software Packages

#### PV Drivers

**Table 3-1** lists the PV driver packages required for optimizing Windows private images.

**Table 3-1** PV driver packages

| Software Package             | OS                           | How to Obtain                                                                                                                                                                                     |
|------------------------------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pvdriver-win2008R2-64bit.zip | Windows Server 2008 R2 64bit | <a href="https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2008R2-64bit.zip">https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2008R2-64bit.zip</a> |

| Software Package             | OS                           | How to Obtain                                                                                                                                                                                     |
|------------------------------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pvdriver-win2012-64bit.zip   | Windows Server 2012 64bit    | <a href="https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2012-64bit.zip">https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2012-64bit.zip</a>     |
| pvdriver-win2012R2-64bit.zip | Windows Server 2012 R2 64bit | <a href="https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2012R2-64bit.zip">https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2012R2-64bit.zip</a> |
| pvdriver-win2016-64bit.zip   | Windows Server 2016 64bit    | <a href="https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2016-64bit.zip">https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2016-64bit.zip</a>     |
| pvdriver-win2019-64bit.zip   | Windows Server 2019 64bit    | <a href="https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2019-64bit.zip">https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2019-64bit.zip</a>     |

## VirtIO Drivers

Download a VirtIO driver package from:

<https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/>

You can select a version as needed.

### 3.8.4 Installing PV Drivers

This section only applies to Xen ECSs, which have been discontinued and no longer been available for new users. If you are a new user or you are an existing user that will use this image to create a non-Xen ECS, skip this section.

## Scenarios

Before using an ECS or external image file to create a private image, ensure that PV drivers have been installed in the OS so that ECSs created from this image can support Xen virtualization, the I/O performance can be improved, and advanced functions such as hardware monitoring can be available.

---

**⚠ CAUTION**

If you do not install PV drivers, the ECS network performance will be poor, and the security groups and firewall configured for the ECS will not take effect.

---

PV drivers have been installed by default when you use a public image to create ECSs. You can perform the following operations to verify the installation:

Open the **version** configuration file to check whether the PV drivers are the latest:

**C:\Program Files (x86)\Xen PV Drivers\bin\version**

- If the PV driver version is later than 2.5, you do not need to install new PV drivers.
- If the PV driver version is not displayed or the version is 2.5 or earlier, perform operations in [Installing PV Drivers](#).

## Prerequisites

- An OS has been installed for the ECS, and an EIP has been bound to the ECS.
- The remaining capacity of the ECS system disk must be greater than 32 MB.
- If the ECS uses Windows 2008, you must install PV drivers as an administrator.
- The PV driver package has been downloaded on the ECS. For how to obtain the software package, see [Obtaining Required Software Packages](#).
- To avoid an installation failure, perform the following operations before starting the installation:
  - Uninstall third-party virtualization platform tools, such as Citrix Xen Tools and VMware Tools. For how to uninstall the tools, see the corresponding official documents of the tools.
  - Disable your anti-virus and intrusion detection software. You can enable them after PV drivers are installed.

## Installing PV Drivers

1. Log in to the Windows ECS using VNC.  
For details about how to log in to an ECS, see *Elastic Cloud Server User Guide*.

### NOTE

You must log in to the ECS using VNC. Remote desktop connection is not allowed because the NIC driver needs to be updated during the installation but the NIC is in use for the remote desktop connection. As a result, the installation will fail.

2. On the ECS, choose **Start > Control Panel**.
3. Click **Uninstall a program**.
4. Uninstall **GPL PV drivers for Windows x.x.x.xx** as prompted.
5. Download PV drivers of the required version based on the ECS OS and [Obtaining Required Software Packages](#).
6. Decompress the PV driver package.
7. Right-click **GPL PV Drivers for Windows x.x.x.xx**, select **Run as administrator**, and complete the installation as prompted.
8. Restart the ECS as prompted to make the PV drivers take effect.  
ECSs running Windows Server 2008 must be restarted twice.

### NOTE

After the PV drivers are installed, the ECS NIC configuration will be lost. If you have configured NICs before, you need to configure them again.

## Installing the PV Driver Upgrade Package

1. Log in to the Windows ECS using VNC.  
For details about how to log in to an ECS, see *Elastic Cloud Server User Guide*.

**NOTE**

You must log in to the ECS using VNC. Remote desktop connection is not allowed because the NIC driver needs to be updated during the installation but the NIC is in use for the remote desktop connection. As a result, the installation will fail.

2. On the ECS, choose **Start > Control Panel**.
  3. Choose **Programs > Uninstall a program**, find PV drivers, and uninstall them.
  4. After the uninstallation is complete, restart the ECS to clear the environment.
  5. Download **pvdriver-windows.zip** from the following link:  
<https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-windows.zip>
  6. Download **pvdriver-windows.zip** from the following link:
  7. Click **Setup.exe** to install new PV drivers. The package will automatically adapt to the OS version.
  8. Restart the ECS as prompted to make the PV drivers take effect.
- ECSs running Windows Server 2008 must be restarted twice.

**NOTE**

After the PV drivers are installed, the ECS NIC configuration will be lost. If you have configured NICs before, you need to configure them again.

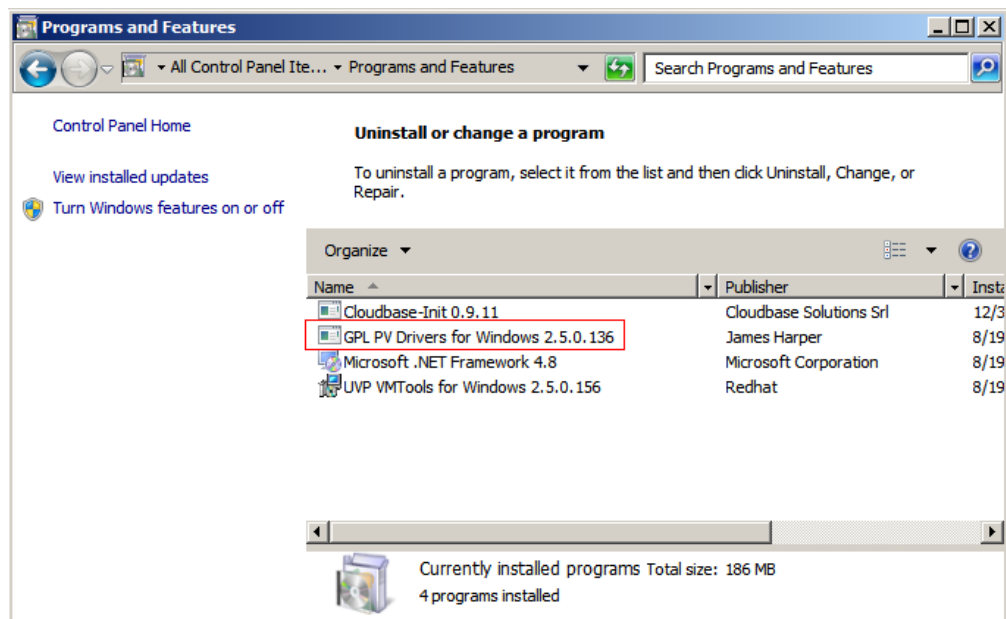
## Verifying the Installation

Perform the following steps to verify the installation of PV drivers:

1. Click **Start**. Choose **Control Panel > Programs and Features**.
2. Locate PV drivers for Windows.

If PV drivers for Windows exist, the installation is successful, as shown in [Figure 3-9](#).

**Figure 3-9** Verifying the installation



## 3.8.5 Installing VirtIO Drivers

### Scenarios

This section only applies to KVM ECSs, which will replace Xen ECSs gradually. Before using an ECS or external image file to create a private image, ensure that VirtIO drivers have been installed in the OS so that ECSs created from this image can support KVM virtualization and the network performance can be improved.

#### CAUTION

If you do not install VirtIO drivers, ECS NICs cannot be detected. As a result, the ECSs cannot communicate with other resources.

If an ECS is created from a public image, VirtIO drivers have been installed by default.

### Prerequisites

An EIP has been bound to the ECS. (This ECS is used to optimize a private image.)

### Installing VirtIO Drivers

The following uses **virtio-win-gt-x64.msi** in **version virtio-win-0.1.189-1** as an example to describe how to install VirtIO drivers.

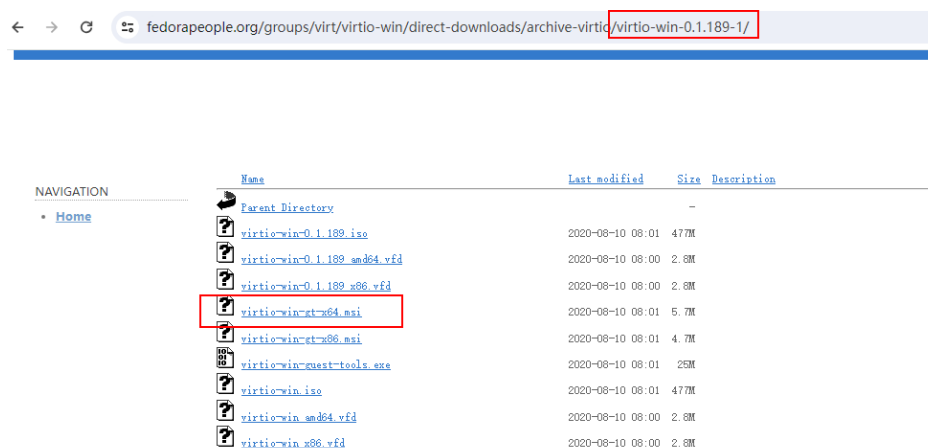
1. Log in to the Windows ECS using VNC.  
For details about how to log in to an ECS, see *Elastic Cloud Server User Guide*.

#### NOTE

You must log in to the ECS using VNC. Remote desktop connection is not allowed because the NIC driver needs to be updated during the installation but the NIC is in use for the remote desktop connection. As a result, the installation will fail.

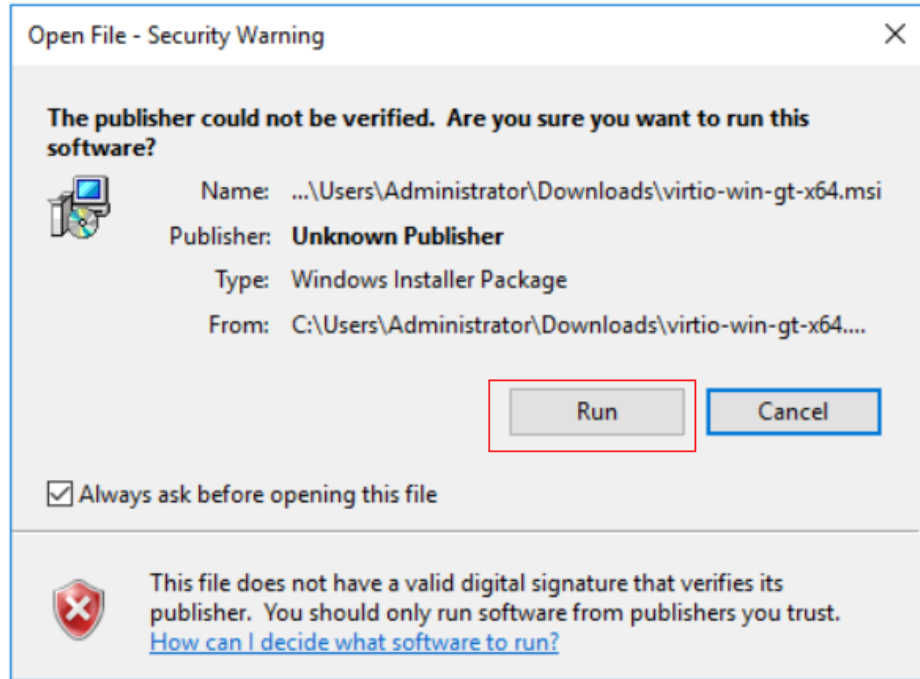
2. Download a VirtIO driver package (**virtio-win-gt-x64.msi** as an example) of the required version by referring to [Obtaining Required Software Packages](#).

**Figure 3-10** Downloading a driver package



3. After the download is complete, right-click **virtio-win-gt-x64.msi** and choose **Run as administrator** from the shortcut menu.

**Figure 3-11** Starting the installation



**Figure 3-12** Installation wizard

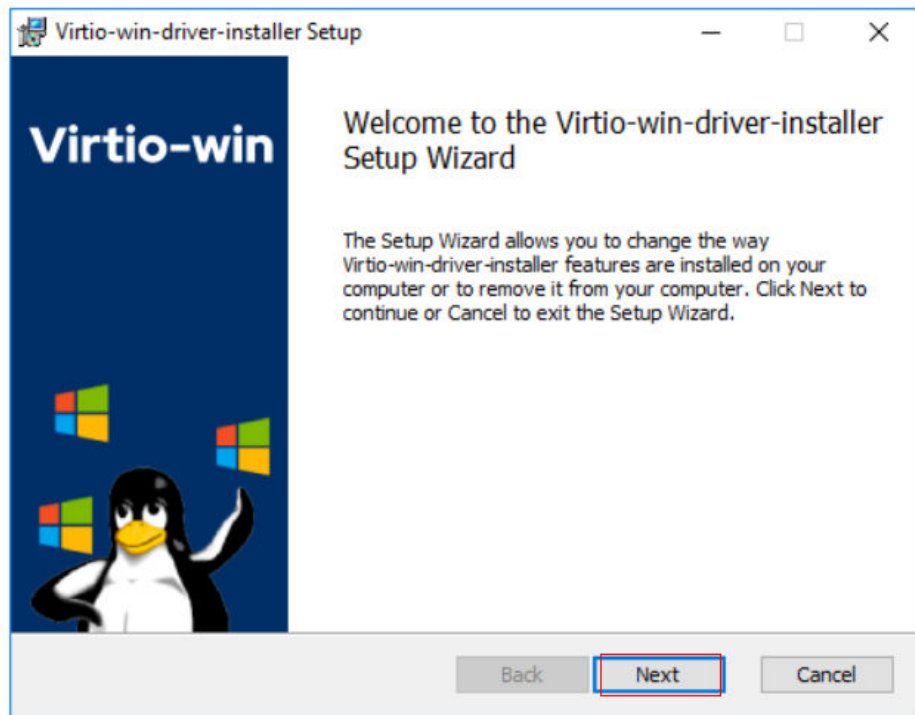
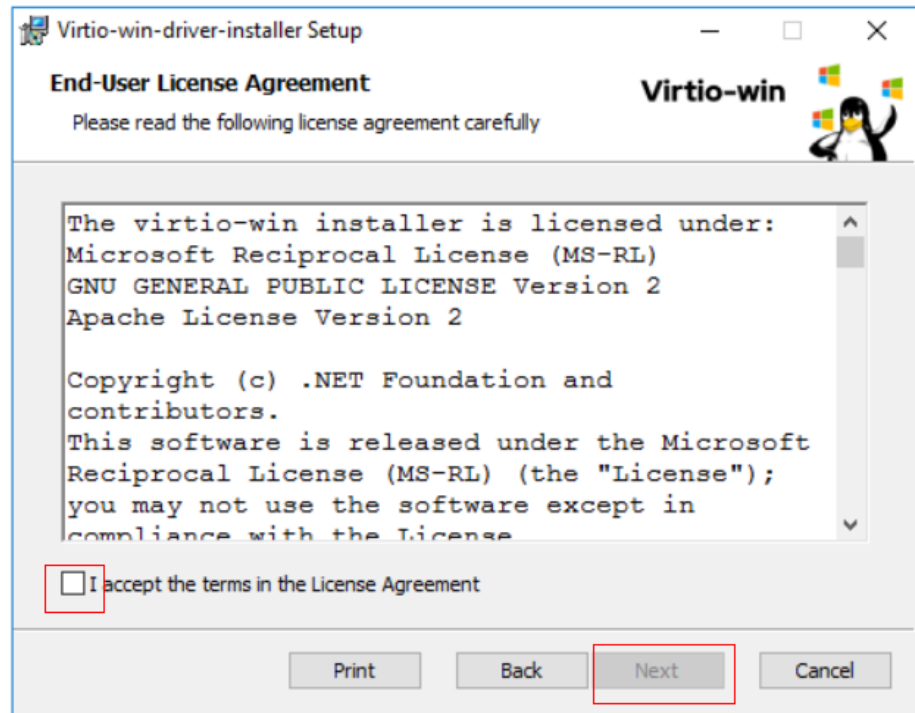
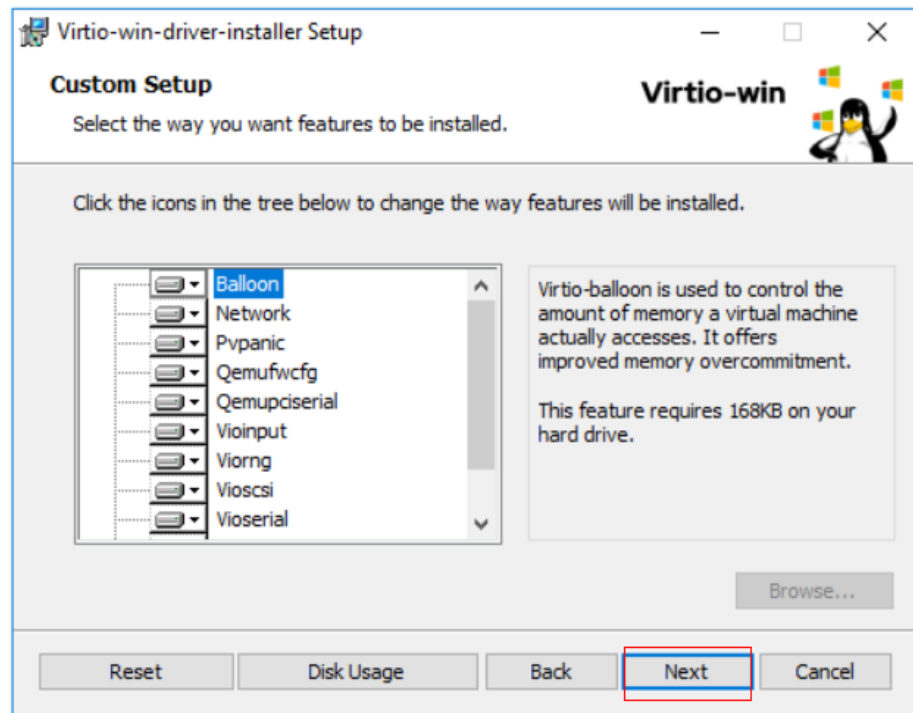


Figure 3-13 Accepting the agreement

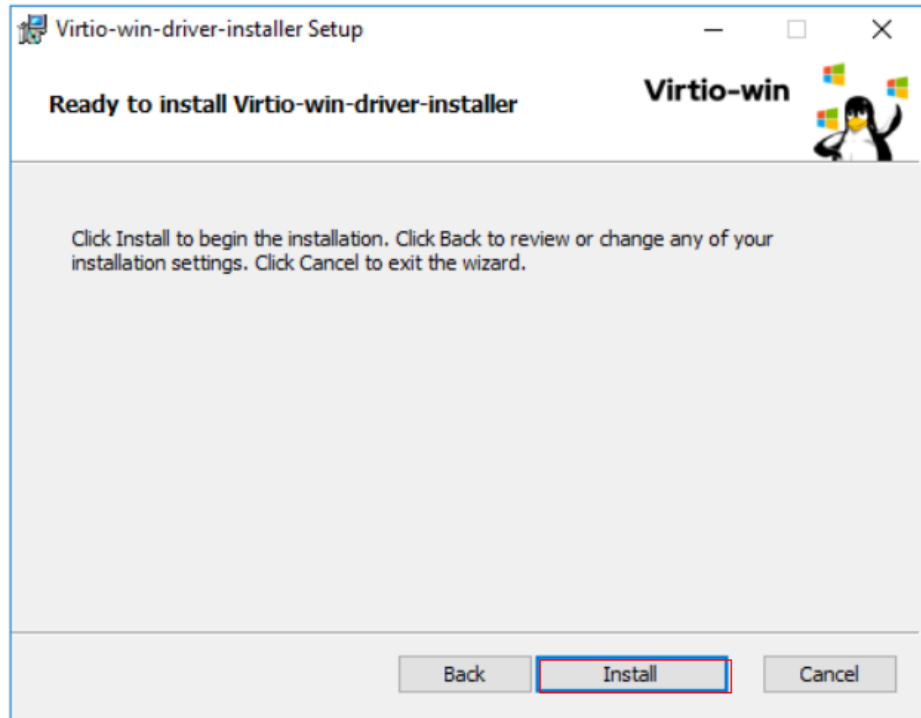


Select the VirtIO drivers to be installed. In this example, select all VirtIO drivers.

Figure 3-14 Selecting VirtIO drivers to install

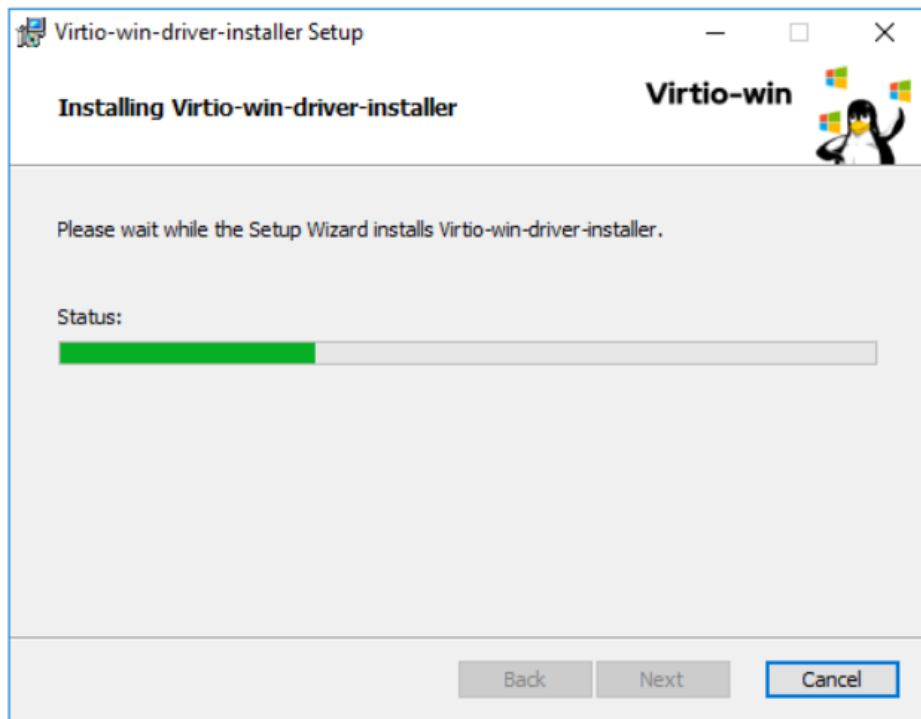


**Figure 3-15** Proceeding with the installation.



4. Wait until the installation is complete.

**Figure 3-16** Installation in process



5. Restart the ECS after the installation is complete.



Figure 3-17 Installation completed

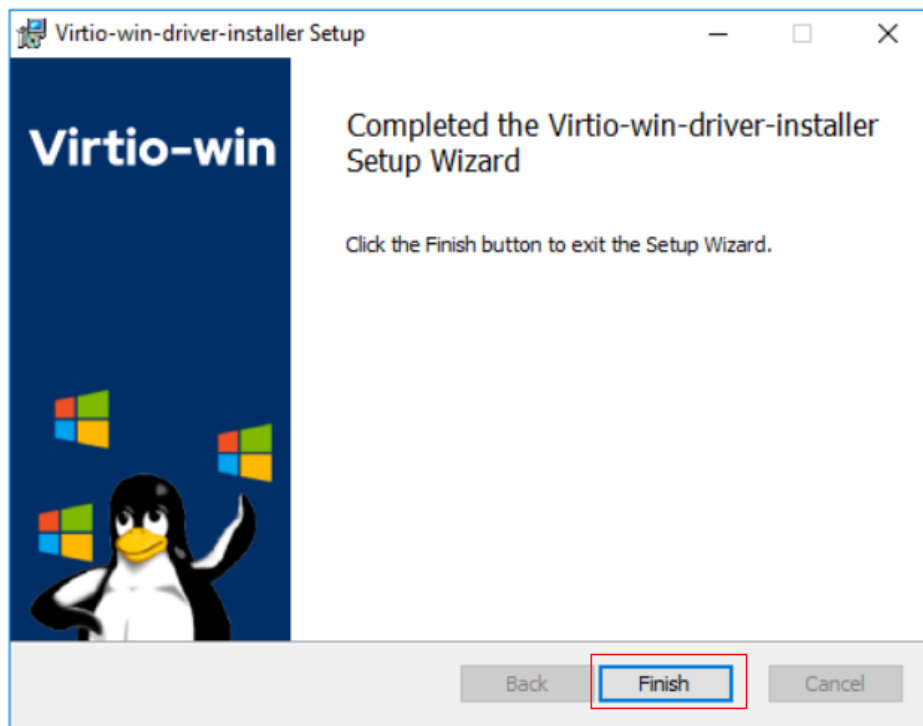
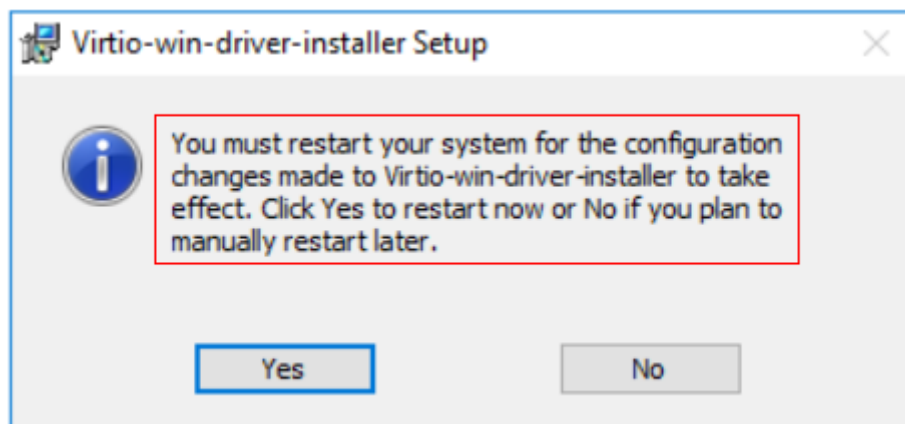


Figure 3-18 Restart prompt



6. After the restart, perform the operations in [Verifying the Installation](#) to verify that the VirtIO drivers have been successfully installed.

## Verifying the Installation

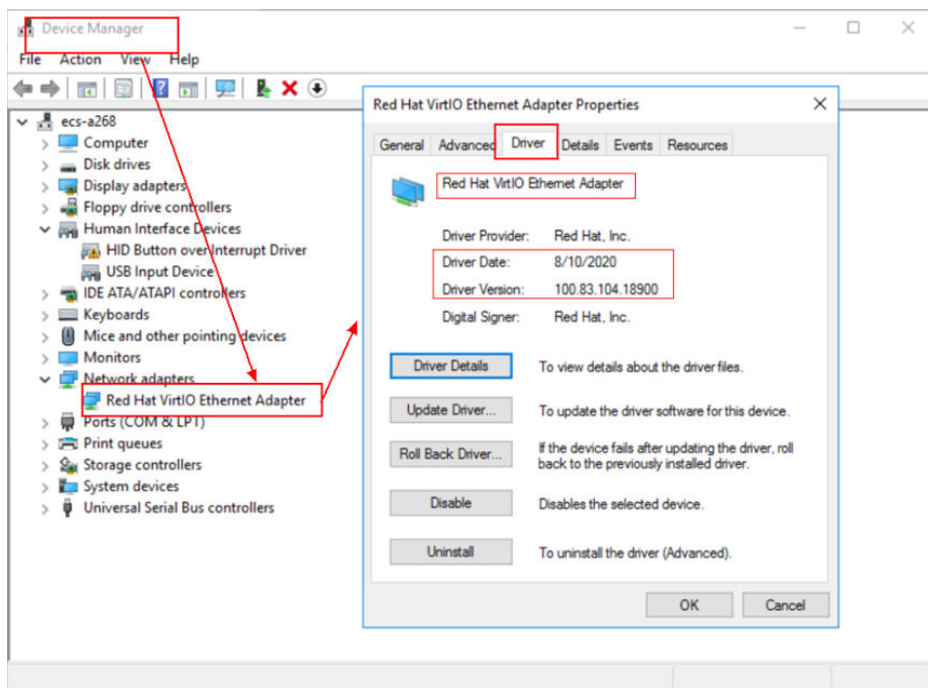
Perform the following steps to verify the installation of the VirtIO drivers:

1. Open **Device Manager** and search for VirtIO drivers.
2. Check whether the VirtIO driver version and date displayed in **Device Manager** are the same as those of the VirtIO drivers you downloaded. If they are the same, the VirtIO drivers have been installed successfully.

Figure 3-19 Version and date of downloaded drivers

| Name                         | Last modified    | Size | Description |
|------------------------------|------------------|------|-------------|
| Parent Directory             |                  | -    |             |
| virtio-win-0.1.189.iso       | 2020-08-10 08:01 | 477M |             |
| virtio-win-0.1.189_amd64.vfd | 2020-08-10 08:00 | 2.8M |             |
| virtio-win-0.1.189_x86.vfd   | 2020-08-10 08:00 | 2.8M |             |
| virtio-win-gt-x64.msi        | 2020-08-10 08:01 | 5.7M |             |
| virtio-win-gt-x86.msi        | 2020-08-10 08:01 | 4.7M |             |
| virtio-win-guest-tools.exe   | 2020-08-10 08:01 | 25M  |             |
| virtio-win.iso               | 2020-08-10 08:01 | 477M |             |
| virtio-win_amd64.vfd         | 2020-08-10 08:00 | 2.8M |             |
| virtio-win_x86.vfd           | 2020-08-10 08:00 | 2.8M |             |

Figure 3-20 Version and date of drivers in Device Manager



### 3.8.6 Clearing System Logs

After installing PV and VirtIO drivers, perform the following operations to clear system logs:

1. For Windows Server 2008 and Windows Server 2012, right-click **Computer** and select **Manage**.
2. In the displayed dialog box, choose **System Tools > Event Viewer > Windows Logs** and delete logs of five items.
3. Stop the ECS.

## 3.9 Optimizing a Linux Private Image

### 3.9.1 Optimization Process


The virtualization of ECSs is gradually changing from Xen to KVM. Therefore, private images need to support both Xen and KVM. To ensure that ECSs created from a private image can run properly, you are advised to optimize it no matter it is using Xen or KVM.

A Linux ECS can run properly only when native KVM (VirtIO) drivers have been installed on it and the disk ID in its GRUB configuration file and fstab file has been changed to UUID.

#### Preparations

1. Use the Linux image to be optimized to **create** an ECS, and start and log in to the ECS.
2. Check whether the private image needs to be optimized.  
For details, see [Checking Whether a Private Image Needs to be Optimized](#).  
The virtualization type may cause slice differences in an optimization process.

#### Process

1. Uninstall PV drivers from the ECS.  
For details, see [Uninstalling PV Drivers from a Linux ECS](#).
-  **NOTE**
- If the ECS is using KVM virtualization, skip this step.
2. Change the disk ID in the GRUB configuration file to UUID.  
For details, see [Changing the Disk Identifier in the GRUB Configuration File to UUID](#).
  3. Change the disk ID in the fstab file to UUID.  
For details, see [Changing the Disk Identifier in the fstab File to UUID](#).
  4. Install native virtualization drivers.
    - For Xen, install native Xen and KVM drivers. For details, see [Installing Native Xen and KVM Drivers](#).
    - For KVM, install native KVM drivers. For details, see [Installing Native KVM Drivers](#).
  5. Delete log files and historical records, and stop the ECS.  
For details, see [Clearing System Logs](#).
  6. Create a Linux private image from the ECS.

## 3.9.2 Checking Whether a Private Image Needs to be Optimized

- If the virtualization type is Xen, optimization is required.
- If the virtualization type is KVM and VirtIO drivers are not installed, optimization is required.
- If the virtualization type is KVM and VirtIO drivers are installed, optimization is not required.

### Procedure

1. Run the following command to check the virtualization type of an ECS:

#### **lscpu**

- If the value of **Hypervisor vendor** is **Xen**, optimize the private image as instructed in [Process](#).
- If the value of **Hypervisor vendor** is **KVM**, go to the next step for further check.

**Figure 3-21** Checking the virtualization type of a Linux ECS

```
lscpu
Architecture: x86_64
CPU op-mode(s): 32-bit, 64-bit
Byte Order: Little Endian
CPU(s): 4
On-line CPU(s) list: 0-3
Thread(s) per core: 1
Core(s) per socket: 4
Socket(s): 1
NUMA node(s): 1
Vendor ID: GenuineIntel
CPU family: 6
Model: 62
Model name: Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz
Stepping: 4
CPU MHz: 3000.079
BogoMIPS: 6000.15
Hypervisor vendor: Xen
Virtualization type: full
L1d cache: 32K
L1i cache: 32K
L2 cache: 256K
L3 cache: 25600K
NUMA node0 CPU(s): 0-3
You have new mail in /var/spool/mail/root
root@SZV-home1#
```

2. Check whether VirtIO drivers have been installed.
  - CentOS/EulerOS  
For initramfs, run the following command:  
**lsinitrd /boot/initramfs-`uname -r`.img | grep virtio**  
For initrd, run the following command:  
**lsinitrd /boot/initrd-`uname -r` | grep virtio**
  - Ubuntu/Debian  
**lsinitramfs /boot/initrd.img-`uname -r` | grep virtio**
  - SUSE/openSUSE

- SUSE 12 SP1/openSUSE 13 or earlier:  
**lsinitrd /boot/initrd-`uname -r` | grep virtio**
- SUSE 12 SP1 or later than SUSE 12 SP1/openSUSE 13:  
For initramfs, run the following command:  
**lsinitrd /boot/initramfs-`uname -r`.img | grep virtio**  
For initrd, run the following command:  
**lsinitrd /boot/initrd-`uname -r` | grep virtio**

If **virtio** is displayed, VirtIO drivers have been installed. For more information, see [Creating a Linux System Disk Image from an External Image File](#).

```
[root@~]# lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
-rw-r--r-- 1 root root 8384 Sep 30 2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/block/virtio_b
lk.ko.xz
-rw-r--r-- 1 root root 14836 Sep 30 2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/char/virtio_co
nsole.ko.xz
-rw-r--r-- 1 root root 25740 Sep 30 2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/net/virtio_net
.ko.xz
-rw-r--r-- 1 root root 8684 Sep 30 2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/scsi/virtio_sc
si.ko.xz
```

Otherwise, VirtIO drivers have not been installed. Optimize the private image as instructed in [Process](#).

### 3.9.3 Uninstalling PV Drivers from a Linux ECS

#### Scenarios

When optimizing a Linux private image with Xen virtualization, you need to install native Xen and KVM drivers on the source ECS of the image.

To ensure that you can successfully install native Xen and KVM drivers, you must uninstall PV drivers from the ECS first.

#### Procedure

1. Log in to the ECS as user **root** using VNC.
2. Run the following command to check whether PV drivers are installed in the OS:

```
ps -ef | grep uvp-monitor
```

- If the following information is displayed, PV drivers have been installed.
- Otherwise, PV drivers are not installed. No further actions will be required.

```
root 4561 1 0 Jun29 ? 00:00:00 /usr/bin/uvp-monitor
root 4567 4561 0 Jun29 ? 00:00:00 /usr/bin/uvp-monitor
root 6185 6085 0 03:04 pts/2 00:00:00 grep uvp-monitor
```

3. In the VNC login window, open the CLI.  
For how to open the CLI, see the OS manual.
4. Run the following command to uninstall PV drivers:

```
/etc/.uvp-monitor/uninstall
```

- PV drivers are uninstalled successfully if the following command output is displayed:  
The PV driver is uninstalled successfully. Reboot the system for the uninstallation to take effect.
- If the command output indicates that **.uvp-monitor** is not found, go to [5](#).  
-bash: /etc/.uvp-monitor/uninstall: No such file or directory

5. Perform the following operations to delete `uvp-monitor` that failed to take effect, preventing log overflow:
  - a. Run the following command to check whether UVP user-mode programs are installed in the OS:

```
rpm -qa | grep uvp
```

Information similar to the following is displayed:

```
libxenstore_uvp3_0-3.00-36.1.x86_64
uvp-monitor-2.2.0.315-3.1.x86_64
kmod-uvpmod-2.2.0.315-3.1.x86_64
```

- b. Run the following commands to delete the installation packages:

```
rpm -e kmod-uvpmod
```

```
rpm -e uvp-monitor
```

```
rpm -e libxenstore_uvp
```

## 3.9.4 Changing the Disk Identifier in the GRUB Configuration File to UUID

### Scenarios

When optimizing a Linux private image, you need to change the disk identifier to UUID in the GRUB configuration file of the ECS.

Modify the `menu.lst` or `grub.cfg` configuration file (`/boot/grub/menu.lst`, `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, `/boot/grub/grub.conf`, or `/boot/efi/EFI/euleros/grub.cfg`), and configure the boot partition using the UUID.

#### NOTE

The root partition identified in the configuration file varies depending on the OS. It may be `root=/dev/xvda` or `root=/dev/disk`.

### Procedure

- Ubuntu 14.04: Run `blkid` to obtain the UUID of the root partition. Modify the `/boot/grub/grub.cfg` file and use the UUID of the root partition to configure the boot item. If the root partition already uses UUID, no modification is required. The procedure is as follows:
  - a. Log in to the ECS as user `root`.
  - b. Run the following command to query all types of mounted file systems and device UUIDs:

```
blkid
```

The following information is displayed:

```
/dev/xvda1: UUID="ec51d860-34bf-4374-ad46-a0c3e337fd34" TYPE="ext3"
/dev/xvda5: UUID="7a44a9ce-9281-4740-b95f-c8de33ae5c11" TYPE="swap"
```

- c. Run the following command to query the `grub.cfg` file:

```
cat /boot/grub/grub.cfg
```

The following information is displayed:

```
.....menuentry 'Ubuntu Linux, with Linux 3.13.0-24-generic' --class ubuntu --class gnu-linux --
class gnu --class os --unrestricted $menuentry_id_option 'gnulinux-3.13.0-24-generic-advanced-
ec51d860-34bf-4374-ad46-a0c3e337fd34' {
```

```
recordfail
load_video
gfxmode $linux_gfx_mode
insmod gzio
insmod part_msdos
insmod ext2
if [x$feature_platform_search_hint = xy]; then
search --no-floppy --fs-uuid --set=root ec51d860-34bf-4374-ad46-a0c3e337fd34
else
search --no-floppy --fs-uuid --set=root ec51d860-34bf-4374-ad46-a0c3e337fd34
fi
echo 'Loading Linux 3.13.0-24-generic ...'
linux /boot/vmlinuz-3.13.0-24-generic root=/dev/xvda1 ro
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-3.13.0-24-generic
}
```

- d. Check whether the root partition in the **/boot/grub/grub.cfg** configuration file contains **root=/dev/xvda1** or **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34**.
    - If **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34** is contained, the root partition is in the UUID format and requires no change.
    - If **root=/dev/xvda1** is contained, the root partition is in the device name format. Go to 5.
  - e. Identify the UUID of the root partition device based on **root=/dev/xvda1** (device name of the root partition) and the partition information obtained by running the **blkid** command.
  - f. Run the following command to open the **grub.cfg** file:
- g. Press **i** to enter editing mode and change the root partition to the UUID format, for example, from **root=/dev/xvda1** to **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34**.
  - h. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the configuration and exits the vi editor.
  - i. Run the following command to verify the change:

```
cat /boot/grub/grub.cfg
```

The change is successful if information similar to the following is displayed:

```
.....menuentry 'Ubuntu Linux, with Linux 3.13.0-24-generic' --class ubuntu --class gnu-linux --class gnu --class os --unrestricted $menuentry_id_option 'gnulinuz-3.13.0-24-generic-advanced-ec51d860-34bf-4374-ad46-a0c3e337fd34' {
recordfail
load_video
gfxmode $linux_gfx_mode
insmod gzio
insmod part_msdos
insmod ext2
if [x$feature_platform_search_hint = xy]; then
search --no-floppy --fs-uuid --set=root ec51d860-34bf-4374-ad46-a0c3e337fd34
else
search --no-floppy --fs-uuid --set=root ec51d860-34bf-4374-ad46-a0c3e337fd34
fi
echo 'Loading Linux 3.13.0-24-generic ...'
linux /boot/vmlinuz-3.13.0-24-generic root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34 ro
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-3.13.0-24-generic
}
```

- CentOS 6.5: Run **blkid** to obtain the UUID of the root partition. Modify the **/boot/grub/grub.conf** file and use the UUID of the root partition to configure the boot item. If the root partition already uses UUID, no modification is required. The procedure is as follows:

- a. Log in to the ECS as user **root**.
- b. Run the following command to query all types of mounted file systems and device UUIDs:

**blkid**

The following information is displayed:

```
/dev/xvda1: UUID="749d6c0c-990a-4661-bed1-46769388365a" TYPE="swap"
/dev/xvda2: UUID="f382872b-eda6-43df-9516-5a687fecdc6" TYPE="ext4"
```

- c. Run the following command to query the **grub.conf** file:

**cat /boot/grub/grub.conf**

The following information is displayed:

```
default=0
timeout=5
splashimage=(hd0,1)/boot/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.32-573.8.1.el6.x86_64)
root (hd0,1)
kernel /boot/vmlinuz-2.6.32-573.8.1.el6.x86_64 ro root=/dev/xvda2 rd_NO_LUKS rd_NO_LVM
LANG=en_US.UTF-8 rd_NO_MD SYSFONT=latarcyrheb-sun16
crashkernel=autoKEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb quiet
initrd /boot/initramfs-2.6.32-573.8.1.el6.x86_64.img
```

- d. Check whether the root partition in the **/boot/grub/grub.conf** configuration file contains **root=/dev/xvda2** or **root=UUID=f382872b-eda6-43df-9516-5a687fecdc6**.
  - If **root=UUID=f382872b-eda6-43df-9516-5a687fecdc6** is contained, the root partition is in the UUID format and requires no change.
  - If **root=/dev/xvda2** is contained, the root partition is in the device name format. Go to [5](#).
- e. Identify the UUID of the root partition device based on **root=/dev/xvda2** (device name of the root partition) and the partition information obtained by running the **blkid** command.
- f. Run the following command to open the **grub.conf** file:

**vi /boot/grub/grub.conf**

- g. Press **i** to enter editing mode and change the root partition to the UUID format, for example, from **root=/dev/xvda2** to **root=UUID=f382872b-eda6-43df-9516-5a687fecdc6**.
- h. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the configuration and exits the vi editor.
- i. Run the following command to verify the change:

**cat /boot/grub/grub.conf**

The change is successful if information similar to the following is displayed:

```
default=0
timeout=5
splashimage=(hd0,1)/boot/grub/splash.xpm.gz
```



```
hiddenmenu
title CentOS (2.6.32-573.8.1.el6.x86_64)
root (hd0,1)
kernel /boot/vmlinuz-2.6.32-573.8.1.el6.x86_64 ro root=UUID=f382872b-
eda6-43df-9516-5a687fecdc66 rd_NO_LUKS rd_NO_LVM LANG=en_US.UTF-8 rd_NO_MD
SYSEFONT=latacyrheb-sun16 crashkernel=autoKEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM
rhgb quiet
initrd /boot/initramfs-2.6.32-573.8.1.el6.x86_64.img
```

- CentOS 7.0: Run **blkid** to obtain the UUID of the root partition. Modify the **/boot/grub2/grub.cfg** file and use the UUID of the root partition to configure the boot item. If the root partition already uses UUID, no modification is required.

- a. Log in to the ECS as user **root**.
- b. Run the following command to query all types of mounted file systems and device UUIDs:

#### **blkid**

The following information is displayed:

```
/dev/xvda2: UUID="4eb40294-4c6f-4384-bbb6-b8795bbb1130" TYPE="xfs"
/dev/xvda1: UUID="2de37c6b-2648-43b4-a4f5-40162154e135" TYPE="swap"
```

- c. Run the following command to query the **grub.cfg** file:

#### **cat /boot/grub2/grub.cfg**

The following information is displayed:

```
.....
menuentry 'CentOS Linux (3.10.0-229.el7.x86_64) 7 (Core)' --class fedora --class gnu-linux --
class gnu --class os --unrestricted $menuentry_id_option 'gnulinux-3.10.0-229.el7.x86_64-
advanced-4eb40294-4c6f-4384-bbb6-b8795bbb1130' {
load_video
set gfxpayload=keep
insmod gzio
insmod part_msdos
insmod xfs
set root='hd0,msdos2'
if [x$feature_platform_search_hint = xy]; then
search --no-floppy --fs-uuid --set=root --hint='hd0,msdos2'4eb40294-4c6f-4384-bbb6-
b8795bbb1130
else
search --no-floppy --fs-uuid --set=root 4eb40294-4c6f-4384-bbb6-b8795bbb1130
fi
linux16 /boot/vmlinuz-3.10.0-229.el7.x86_64 root=/dev/xvda2 ro crashkernel=auto rhgb quiet
LANG=en_US.UTF-8
initrd16 /boot/initramfs-3.10.0-229.el7.x86_64.img
}
```

- d. Check whether the root partition in the **/boot/grub2/grub.cfg** configuration file contains **root=/dev/xvda2** or **root=UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130**.
  - If **root=UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130** is contained, the root partition is in the UUID format and requires no change.
  - If **root=/dev/xvda2** is contained, the root partition is in the device name format. Go to [5](#).
- e. Identify the UUID of the root partition device based on **root=/dev/xvda2** (device name of the root partition) and the partition information obtained by running the **blkid** command.
- f. Run the following command to open the **grub.cfg** file:

**vi /boot/grub2/grub.cfg**

- g. Press **i** to enter editing mode and change the root partition to the UUID format, for example, from **root=/dev/xvda2** to **root=UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130**.
- h. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the configuration and exits the vi editor.
- i. Run the following command to verify the change:

**cat /boot/grub2/grub.cfg**

The change is successful if information similar to the following is displayed:

```
.....
menuentry 'CentOS Linux (3.10.0-229.el7.x86_64) 7 (Core)' --class fedora --class gnu-linux --
class gnu --class os --unrestricted $menuentry_id_option 'gnulinux-3.10.0-229.el7.x86_64-
advanced-4eb40294-4c6f-4384-bbb6-b8795bbb1130' {
load_video
set gfxpayload=keep
insmod gzio
insmod part_msdos
insmod xfs
set root='hd0,msdos2'
if [x$feature_platform_search_hint = xy]; then
search --no-floppy --fs-uuid --set=root --hint='hd0,msdos2'4eb40294-4c6f-4384-bbb6-
b8795bbb1130
else
search --no-floppy --fs-uuid --set=root 4eb40294-4c6f-4384-bbb6-b8795bbb1130
fi
linux16 /boot/vmlinuz-3.10.0-229.el7.x86_64 root=UUID=4eb40294-4c6f-4384-bbb6-
b8795bbb1130 ro crashkernel=auto rhgb quiet LANG=en_US.UTF-8
initrd16 /boot/initramfs-3.10.0-229.el7.x86_64.img
}
```

## 3.9.5 Changing the Disk Identifier in the fstab File to UUID

### Scenarios

When optimizing a Linux private image, you need to change the disk identifier to UUID in the fstab configuration file of the ECS.

### Procedure

- Take CentOS 7.0 as an example. Run **blkid** to obtain the UUIDs of all partitions. Modify the **/etc/fstab** file and use the partition UUIDs to configure automatic partition mounting.
1. Log in to the ECS as user **root**.
  2. Run the following command to query all types of mounted file systems and device UUIDs:

**blkid**

The following information is displayed:

```
/dev/xvda2: UUID="4eb40294-4c6f-4384-bbb6-b8795bbb1130" TYPE="xfs"
/dev/xvda1: UUID="2de37c6b-2648-43b4-a4f5-40162154e135" TYPE="swap"
```

3. Run the following command to query the **fstab** file:

**cat /etc/fstab**

The following information is displayed:

```
[root@CTU1000028010 ~]# cat /etc/fstab
/dev/xvda2 / xfs defaults 0 0
/dev/xvda1 swap swap defaults 0 0
```

4. Check whether the disk identifier in the **fstab** file is the device name.
    - If the disk is represented by UUID, no further operation is required.
    - If the disk is represented by the device name, go to **5**.
  5. Run the following command to open the **fstab** file:
1. Log in to the ECS as user **root**.
  2. Run the following command to query all types of mounted file systems and device UUIDs:

```
vi /etc/fstab
```

6. Press **i** to enter editing mode and change the disk identifier in the **fstab** file to UUID.

- Take CentOS 7.1 as an example. Run **blkid** to obtain the UUIDs of all partitions. Modify the **/etc/fstab** file and use the partition UUIDs to configure automatic partition mounting.

```
blkid
```

```
/dev/xvda2: UUID="4eb40294-4c6f-4384-bbb6-b8795bbb1130" TYPE="xfs"
/dev/xvda1: UUID="2de37c6b-2648-43b4-a4f5-40162154e135" TYPE="swap"
```

Before the change:

```
[root@CTU1000028010 ~]# cat /etc/fstab
/dev/xvda2 / xfs defaults 0 0
/dev/xvda1 swap swap defaults 0 0
```

After the change:

```
[root@CTU1000028010 ~]# cat /etc/fstab
UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130 / xfs defaults 0 0
UUID=2de37c6b-2648-43b4-a4f5-40162154e135 swap swap defaults 0 0
```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the configuration and exits the vi editor.
4. Run the following command to verify the change:

```
cat /etc/fstab
```

The change is successful if information similar to the following is displayed:

```
[root@CTU1000028010 ~]# cat /etc/fstab
UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130 / xfs defaults 0 0
UUID=2de37c6b-2648-43b4-a4f5-40162154e135 swap swap defaults 0 0
```

## 3.9.6 Installing Native Xen and KVM Drivers

### Scenarios

When optimizing a Linux private image with Xen virtualization, you need to install native Xen and KVM drivers on the source ECS of the image.

This section describes how to install native Xen and KVM drivers.

 CAUTION

If an ECS has no Xen drivers installed, the network performance of the ECS will be poor, and the security groups and firewall configured for the ECS will not take effect.

If an ECS has no KVM drivers installed, the NICs of the ECS may not be detected and the ECS will be unable to communicate with other resources.

## Prerequisites

- The virtualization type of the ECS is Xen.
- The kernel version must be later than 2.6.24.
- Disable your antivirus and intrusion detection software. You can enable them after the driver installation is complete.

## Procedure

Modify the configuration file depending on the OS.

- CentOS, EulerOS  
Take CentOS 7.0 as an example. Modify the `/etc/dracut.conf` file. Add the Xen PV and VirtIO drivers to **add\_drivers**. Xen PV drivers include `xen-blkfront` and `xen-netfront`. VirtIO drivers include `virtio_blk`, `virtio_scsi`, `virtio_net`, `virtio_pci`, `virtio_ring`, and `virtio`. Separate driver names with spaces. Save and exit the `/etc/dracut.conf` file. Run the **dracut -f** command to regenerate `initrd`.  
For details, see [CentOS and EulerOS](#).
- Ubuntu and Debian  
Modify the `/etc/initramfs-tools/modules` file. Add the Xen PV and VirtIO drivers. Xen PV drivers include `xen-blkfront` and `xen-netfront`. VirtIO drivers include `virtio_blk`, `virtio_scsi`, `virtio_net`, `virtio_pci`, `virtio_ring`, and `virtio`. Separate driver names with spaces. Save and exit the `/etc/initramfs-tools/modules` file. Run the **update-initramfs -u** command to regenerate `initrd`.  
For details, see [Ubuntu and Debian](#).
- SUSE and openSUSE
  - If the OS version is earlier than SUSE 12 SP1 or openSUSE 13, modify the `/etc/sysconfig/kernel` file and add Xen PV and VirtIO drivers to **INITRD\_MODULES=""**. Xen PV drivers include `xen_vnif`, `xen_vbd`, and `xen_platform_pci`. VirtIO drivers include `virtio_blk`, `virtio_scsi`, `virtio_net`, `virtio_pci`, `virtio_ring`, and `virtio`. Separate driver names with spaces. Run the **mkinitrd** command to regenerate `initrd`.
  - If the OS version is SUSE 12 SP1, modify the `/etc/dracut.conf` file and add Xen PV and VirtIO drivers to **add\_drivers**. Xen PV drivers include `xen_vnif`, `xen_vbd`, and `xen_platform_pci`. VirtIO drivers include `virtio_blk`, `virtio_scsi`, `virtio_net`, `virtio_pci`, `virtio_ring`, and `virtio`. Separate driver names with spaces. Run the **dracut -f** command to regenerate `initrd`.
  - If the OS version is later than SUSE 12 SP1 or openSUSE 13, modify the `/etc/dracut.conf` file and add Xen PV and VirtIO drivers to **add\_drivers**. Xen PV drivers include `xen-blkfront` and `xen-netfront`. VirtIO drivers include `virtio_blk`, `virtio_scsi`, `virtio_net`, `virtio_pci`, `virtio_ring`, and

virtio. Separate driver names with spaces. Save and exit the `/etc/dracut.conf` file. Run the `dracut -f` command to regenerate `initrd`.

For details, see [SUSE and openSUSE](#).

#### NOTE

For SUSE, run the following command to check whether `xen-kmp` (driver package for Xen PV) is installed:

```
rpm -qa |grep xen-kmp
```

If information similar to the following is displayed, `xen-kmp` is installed in the OS:

```
xen-kmp-default-4.2.2_04_3.0.76_0.11-0.7.5
```

If `xen-kmp` is not installed, obtain it from the ISO file and install it.

If you add built-in drivers to the `initrd` or `initramfs` file by mistake, the ECS will not be affected.

## CentOS and EulerOS

1. Run the following command to open the `/etc/dracut.conf` file:

```
vi /etc/dracut.conf
```

2. Press `i` to enter editing mode and add Xen PV and VirtIO drivers to **add\_drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxx ~]# vi /etc/dracut.conf
additional kernel modules to the default
add_drivers+="xen-blkfront xen-netfront virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring virtio"
.....
```

3. Press `Esc`, enter `:wq`, and press `Enter`. The system saves the change and exits the `/etc/dracut.conf` file.
4. Run the following command to regenerate `initrd`:

```
dracut -f /boot/initramfs-2.6.32-573.8.1.el6.x86_64.img
```

If the virtual file system is not the default `initramfs`, run `dracut -f Name of the initramfs or initrd file actually used`. You can obtain the actual `initramfs` or `initrd` file name from the `grub.cfg` file, which can be `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, or `/boot/grub/grub.conf` depending on the OS.

5. Check whether native Xen and KVM drivers have been installed. If the 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 virtual file system is `initrd`, run the following commands:

```
lsinitrd /boot/initrd-`uname -r` | grep xen
```

```
lsinitrd /boot/initrd-`uname -r` | grep virtio
```

Assume that the virtual file system is `initramfs`. The command output will be:

```
[root@CTU10000xxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep xen
-rwxr--r-- 1 root root 54888 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/block/xen-blkfront.ko
-rwxr--r-- 1 root root 45664 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/net/xen-netfront.ko

[root@CTU10000xxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep virtio
-rwxr--r-- 1 root root 23448 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/block/virtio_blk.ko
-rwxr--r-- 1 root root 50704 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/net/virtio_net.ko
```

```
-rwxr--r-- 1 root root 28424 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
scsi/virtio_scsi.ko
drwxr-xr-x 2 root root 0 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio
-rwxr--r-- 1 root root 14544 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio.ko
-rwxr--r-- 1 root root 21040 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_pci.ko
-rwxr--r-- 1 root root 18016 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_ring.ko
```

#### NOTE

If you add built-in drivers to the `initrd` or `initramfs` file by mistake, the ECS will not be affected. The drivers cannot be found by running the `lsinitrd` command. You can run the following commands to check whether built-in drivers are in the kernel:

```
cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y
```

```
cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y
```

## Ubuntu and Debian

1. Run the following command to open the `modules` file:

```
vi /etc/initramfs-tools/modules
```

2. Press `i` to enter editing mode and add Xen PV and VirtIO drivers to the `/etc/initramfs-tools/modules` file (the format varies depending on the OS).

```
[root@CTU10000xxxx ~]#vi /etc/initramfs-tools/modules
```

```
.....
Examples:
#
raid1
sd_mOd
xen-blkfront
xen-netfront
virtio_blk
virtio_scsi
virtio_net
virtio_pci
virtio_ring
virtio
```

3. Press `Esc`, enter `:wq`, and press `Enter`. The system saves the change and exits the `/etc/initramfs-tools/modules` file.
4. Run the following command to regenerate `initrd`:

```
update-initramfs -u
```

5. Run the following commands to check whether native Xen and KVM drivers have been installed:

```
lsinitramfs /boot/initrd.img-`uname -r` |grep xen
```

```
lsinitramfs /boot/initrd.img-`uname -r` |grep virtio
```

```
[root@CTU10000xxxx home]# lsinitramfs /boot/initrd.img-`uname -r` |grep xen
lib/modules/3.5.0-23-generic/kernel/drivers/net/ethernet/qlogic/netxen
lib/modules/3.5.0-23-generic/kernel/drivers/net/ethernet/qlogic/netxen/netxen_nic.ko
lib/modules/3.5.0-23-generic/kernel/drivers/net/xen-netback
lib/modules/3.5.0-23-generic/kernel/drivers/net/xen-netback/xen-netback.ko
lib/modules/3.5.0-23-generic/kernel/drivers/block/xen-blkback
lib/modules/3.5.0-23-generic/kernel/drivers/block/xen-blkback/xen-blkback.ko
```

```
[root@CTU10000xxxx home]# lsinitramfs /boot/initrd.img-`uname -r` |grep virtio
lib/modules/3.5.0-23-generic/kernel/drivers/scsi/virtio_scsi.ko
```

 NOTE

If you add built-in drivers to the `initrd` or `initramfs` file by mistake, the ECS will not be affected. The drivers cannot be found by running the `lsinitrd` command. You can run the following commands to check whether built-in drivers are in the kernel:

```
[root@ CTU10000xxxxx home]# cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y
CONFIG_VIRTIO_BLK=y
CONFIG_VIRTIO_NET=y
CONFIG_VIRTIO=y
CONFIG_VIRTIO_RING=y
CONFIG_VIRTIO_PCI=y
CONFIG_VIRTIO_MMIO_CMDLINE_DEVICES=y
[root@ CTU10000xxxxx home]# cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y
CONFIG_XEN_BLKDEV_FRONTEND=y
CONFIG_XEN_NETDEV_FRONTEND=y
```

## SUSE and openSUSE

If the OS version is earlier than SUSE 12 SP1 or openSUSE 13, modify the `/etc/sysconfig/kernel` file to install the drivers. For details, see [scenario 1](#).

If the OS version is SUSE 12 SP1, modify the `/etc/dracut.conf` file to install the drivers. For details, see [scenario 2](#).

If the OS version is later than SUSE 12 SP1 or openSUSE 13, modify the `/etc/dracut.conf` file to install the drivers. For details, see [scenario 3](#).

- Earlier than SUSE 12 SP1 or openSUSE 13:

 NOTE

Before installing the drivers, run the following command to check whether `xen-kmp` (driver package for Xen PV) is installed:

```
rpm -qa |grep xen-kmp
```

If information similar to the following is displayed, `xen-kmp` is installed:

```
xen-kmp-default-4.2.2_04_3.0.76_0.11-0.7.5
```

If `xen-kmp` is not installed, obtain it from the ISO package and install it first.

- a. Run the following command to open the `/etc/sysconfig/kernel` file:

```
vi /etc/sysconfig/kernel
```

- b. Add Xen PV and VirtIO drivers after `INITRD_MODULES=` (the format varies depending on the OS).

```
SIA10000xxxxx:~ # vi /etc/sysconfig/kernel
(like drivers for scsi-controllers, for lvm or reiserfs)
#
INITRD_MODULES="ata_piix ata_generic xen_vnif xen_vbd xen_platform_pci virtio_blk
virtio_scsi virtio_net virtio_pci virtio_ring virtio"
```

- c. Run the `dracut -f` command to regenerate `initrd`.

 NOTE

If the virtual file system is not the default `initramfs` or `initrd`, run `dracut -f Name of the initramfs or initrd file actually used`. The actual `initramfs` or `initrd` file name can be obtained from the `menu.lst` or `grub.cfg` file (`/boot/grub/menu.lst`, `/boot/grub/grub.cfg`, or `/boot/grub2/grub.cfg`).

The following is an example `initrd` file of SUSE 11 SP4:

```
default 0
timeout 10
gfxmenu (hd0,0)/boot/message
title sles11sp4_001_[_VMX_]
```

```

root (hd0,0)
kernel /boot/linux.vmx vga=0x314 splash=silent console=ttyS0,115200n8 console=tty0
net.ifnames=0 NON_PERSISTENT_DEVICE_NAMES=1 showopts
initrd /boot/initrd.vmx
title Failsafe_sles11sp4_001_[_VMX_]
root (hd0,0)
kernel /boot/linux.vmx vga=0x314 splash=silent ide=nodma apm=off noresume edd=off
powersaved=off nohz=off highres=off processor.max+cstate=1 nomodeset x11failsafe
console=ttyS0,115200n8 console=tty0 net.ifnames=0 NON_PERSISTENT_DEVICE_NAMES=1
showopts
initrd /boot/initrd.vmx

```

**/boot/initrd.vmx** is the **initrd** file actually used. If **/boot** is missing in the **initrd** file path, you need to add it when you run the **dracut -f** command. In this case, the command should be **dracut -f /boot/initramfs-XXX**.

- d. Run the following commands to check whether Xen PVOPS and KVM VirtIO drivers have been installed:

```
lsinitrd /boot/initrd-`uname -r` | grep xen
```

```
lsinitrd /boot/initrd-`uname -r` | grep virtio
```

```

SIA10000xxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rwxr--r-- 1 root root 42400 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
xen-blkfront.ko
-rwxr--r-- 1 root root 44200 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
xen-netfront.ko

```

```

SIA10000xxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/
virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
virtio_net.ko

```

- e. Restart the ECS.
- f. Modify the **/boot/grub/menu.lst** file to add **xen\_platform\_pci.dev\_unplug=all** and change the root settings.

Before the modification:

```

###Don't change this comment -YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11SP4 - 3.0.76-0.11 (default)
root (hd0,0)
kernel /boot/vmlinuz-3.0.76-0.11-default root=UUID=4eb40294-4c6f-4384-bbb6-
b8795bbb1130 splash=silentcrashkernel=256M-:128M showopts vga=0x314
initrd /boot/initrd-3.0.76-0.11-default

```

After the modification:

```

###Don't change this comment -YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11SP4 - 3.0.76-0.11 (default)
root (hd0,0)
kernel /boot/vmlinuz-3.0.76-0.11-default root=UUID=4eb40294-4c6f-4384-bbb6-
b8795bbb1130 splash=silentcrashkernel=256M-:128M showopts vga=0x314
xen_platform_pci.dev_unplug=all
initrd /boot/initrd-3.0.76-0.11-default

```



 NOTE

- Ensure that the root partition is in UUID format.
- **xen\_platform\_pci.dev\_unplug=all** is used to shield QEMU devices.
- For SUSE 11 SP1 64bit to SUSE 11 SP4 64bit, add **xen\_platform\_pci.dev\_unplug=all** to the **menu.lst** file. For SUSE 12 or later, QEMU device shield is enabled by default, and you do not need to configure it.

- g. Run the following commands to check whether Xen drivers exist in `initrd`:

```
lsinitrd /boot/initrd-`uname -r` | grep xen
```

```
lsinitrd /boot/initrd-`uname -r` | grep virtio
```

```
SIA10000xxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rwxr--r-- 1 root root 42400 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
xen-blkfront.ko
-rwxr--r-- 1 root root 44200 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
xen-netfront.ko

SIA10000xxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/
virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
virtio_net.ko
```

 NOTE

If you add built-in drivers to the `initrd` or `initramfs` file by mistake, the ECS will not be affected. The drivers cannot be found by running the `lsinitrd` command. You can run the following commands to check whether built-in drivers are in the kernel:

```
cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y
```

```
cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y
```

- SUSE 12 SP1:

- a. Run the following command to open the `/etc/dracut.conf` file:

```
vi /etc/dracut.conf
```

- b. Press **i** to enter editing mode and add Xen PV and VirtIO drivers to **add-drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxx ~]# vi /etc/dracut.conf
additional kernel modules to the default
add_drivers+="ata_piix ata_generic xen_vnif xen_vbd xen_platform_pci virtio_blk virtio_scsi
virtio_net virtio_pci virtio_ring virtio"
```

- c. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the `/etc/dracut.conf` file.

- d. Run the following command to regenerate `initrd`:

```
dracut -f /boot/initramfs-File name
```

If the virtual file system is not the default `initramfs`, run the **dracut -f *Name of the initramfs or initrd file actually used*** command. The actual `initramfs` or `initrd` file name can be obtained from the **grub.cfg** file, which

can be `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, or `/boot/grub/grub.conf` depending on the OS.

- e. Check whether native Xen and KVM drivers have been installed. If the 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 virtual file system is `initrd`, run the following commands:

```
lsinitrd /boot/initrd-`uname -r` | grep xen
```

```
lsinitrd /boot/initrd-`uname -r` | grep virtio
```

- Later than SUSE 12 SP1 or openSUSE 13:

Take SUSE Linux Enterprise Server 12 SP2 (x86\_64) as an example.

- a. Run the following command to open the `/etc/dracut.conf` file:

```
vi /etc/dracut.conf
```

- b. Press `i` to enter editing mode and add Xen PV and VirtIO drivers to `add_drivers` (the format varies depending on the OS).

```
[root@CTU10000xxxx ~]# vi /etc/dracut.conf
additional kernel modules to the default
add_drivers+="ata_piix ata_generic xen-blkfront xen-netfront virtio_blk virtio_scsi
virtio_net virtio_pci virtio_ring virtio"
```

- c. Press `Esc`, enter `:wq`, and press `Enter`. The system saves the change and exits the `/etc/dracut.conf` file.

- d. Run the following command to regenerate `initrd`:

```
dracut -f /boot/initramfs-File name
```

If the virtual file system is not the default `initramfs`, run the `dracut -f Name of the initramfs or initrd file actually used` command. The actual `initramfs` or `initrd` file name can be obtained from the `grub.cfg` file, which can be `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, or `/boot/grub/grub.conf` depending on the OS.

- e. Check whether native Xen and KVM drivers have been installed. If the 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 virtual file system is `initrd`, run the following commands:

```
lsinitrd /boot/initrd-`uname -r` | grep xen
```

```
lsinitrd /boot/initrd-`uname -r` | grep virtio
```

Assume that the virtual file system is `initrd`. The command output will be:

```
sluo-ecs-30dc:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rw-r--r-- 1 root root 69575 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/block/xen-
blkfront.ko
-rw-r--r-- 1 root root 53415 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/net/xen-
netfront.ko
drwxr-xr-x 2 root root 0 Sep 28 10:21 lib/modules/4.4.21-69-default/updates/pvdriver/xen-hcall
-rwxr-xr-x 1 root root 8320 Sep 28 10:21 lib/modules/4.4.21-69-default/updates/pvdriver/xen-
hcall/xen-hcall.ko

sluo-ecs-30dc:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rw-r--r-- 1 root root 29335 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/block/
virtio_blk.ko
-rw-r--r-- 1 root root 57007 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/net/
virtio_net.ko
```

```
-rw-r--r-- 1 root root 32415 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/scsi/
virtio_scsi.ko
drwxr-xr-x 2 root root 0 Sep 28 10:21 lib/modules/4.4.21-69-default/kernel/drivers/virtio
-rw-r--r-- 1 root root 19623 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/
virtio.ko
-rw-r--r-- 1 root root 38943 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/
virtio_pci.ko
-rw-r--r-- 1 root root 24431 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/
virtio_ring.ko
```

#### NOTE

If you add built-in drivers to the `initrd` or `initramfs` file by mistake, the ECS will not be affected. The drivers cannot be found by running the `lsinitrd` command. You can run the following commands to check whether built-in drivers are in the kernel:

```
cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y
cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y
```

## 3.9.7 Installing Native KVM Drivers

### Scenarios

When optimizing a Linux private image, you need to install native KVM drivers on the ECS. If the drivers have been installed, skip this section.

---

#### CAUTION

If you do not install KVM drivers, NICs of the ECS may not be detected and the ECS cannot communicate with other resources.

---

### Prerequisites

- The ECS needs to be optimized. For details, see [Checking Whether a Private Image Needs to be Optimized](#).
- The ECS kernel must be later than 2.6.24.
- Disable your antivirus and intrusion detection software. You can enable the software after KVM drivers are installed.

### Procedure

Modify the configuration file based on the OS version.

**Table 3-2** Modifying configuration files for different OSs

| OS                | Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Reference                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| CentOS/EulerOS    | <p>Take CentOS 7.0 as an example.</p> <ol style="list-style-type: none"> <li>In the <code>/etc/dracut.conf</code> file, add VirtIO drivers to <b>add_drivers</b>, including <code>virtio_blk</code>, <code>virtio_scsi</code>, <code>virtio_net</code>, <code>virtio_pci</code>, <code>virtio_ring</code>, and <code>virtio</code>. Separate driver names with spaces.</li> <li>Save and exit the <code>/etc/dracut.conf</code> file and run the <code>dracut -f</code> command to generate <b>initrd</b> again.</li> </ol> | <a href="#">CentOS and EulerOS</a>                                          |
| Ubuntu/Debian     | <ol style="list-style-type: none"> <li>In the <code>/etc/initramfs-tools/modules</code> file, add VirtIO drivers, including <code>virtio_blk</code>, <code>virtio_scsi</code>, <code>virtio_net</code>, <code>virtio_pci</code>, <code>virtio_ring</code>, and <code>virtio</code>. Separate driver names with spaces.</li> <li>Save and exit the <code>/etc/initramfs-tools/modules</code> file and run the <code>update-initramfs -u</code> command to generate <b>initrd</b> again.</li> </ol>                           | <a href="#">Ubuntu and Debian</a>                                           |
| SUSE and openSUSE | <p>If the OS version is earlier than SUSE 12 SP1 or openSUSE 13:</p> <ol style="list-style-type: none"> <li>In the <code>/etc/sysconfig/kernel</code> file, add VirtIO drivers to <b>INITRD_MODULES=""</b>. VirtIO drivers include <code>virtio_blk</code>, <code>virtio_scsi</code>, <code>virtio_net</code>, <code>virtio_pci</code>, <code>virtio_ring</code>, and <code>virtio</code>. Separate driver names with spaces.</li> <li>Run the <code>mkinitrd</code> command to generate <b>initrd</b> again.</li> </ol>    | <a href="#">SUSE and openSUSE (Earlier than SUSE 12 SP1 or openSUSE 13)</a> |
|                   | <p>If the OS version is SUSE 12 SP1:</p> <ol style="list-style-type: none"> <li>In the <code>/etc/dracut.conf</code> file, add VirtIO drivers to <b>add_drivers</b>. VirtIO drivers include <code>virtio_blk</code>, <code>virtio_scsi</code>, <code>virtio_net</code>, <code>virtio_pci</code>, <code>virtio_ring</code>, and <code>virtio</code>. Separate driver names with spaces.</li> <li>Run the <code>dracut -f</code> command to generate <b>initrd</b> again.</li> </ol>                                          | <a href="#">SUSE and openSUSE (SUSE 12 SP1)</a>                             |

| OS | Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Reference                                                                 |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
|    | <p>If the OS version is later than SUSE 12 SP1 or openSUSE 13:</p> <ol style="list-style-type: none"> <li>In the <code>/etc/dracut.conf</code> file, add VirtIO drivers to <b>add_drivers</b>, including <code>virtio_blk</code>, <code>virtio_scsi</code>, <code>virtio_net</code>, <code>virtio_pci</code>, <code>virtio_ring</code>, and <code>virtio</code>. Separate driver names with spaces.</li> <li>Save and exit the <code>/etc/dracut.conf</code> file and run the <b>dracut -f</b> command to generate <b>initrd</b> again.</li> </ol> | <a href="#">SUSE and openSUSE (Later than SUSE 12 SP1 or openSUSE 13)</a> |

## CentOS and EulerOS

- Run the following command to open the `/etc/dracut.conf` file:  
**vi /etc/dracut.conf**
- Press **i** to enter the editing mode and add VirtIO drivers to **add\_drivers** (the format varies depending on the OS).  

```
[root@CTU10000xxxx ~]# vi /etc/dracut.conf
additional kernel modules to the default
add_drivers+="virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring virtio"
....
```
- Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the `/etc/dracut.conf` file.

- Run the following command to regenerate `initrd`:

```
dracut -f /boot/initramfs-2.6.32-573.8.1.el6.x86_64.img
```

If the virtual file system is not the default `initramfs`, run the **dracut -f Name of the initramfs or initrd file actually used** command. The actual `initramfs` or `initrd` file name can be obtained from the **grub.cfg** file, which can be `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, or `/boot/grub/grub.conf` depending on the OS.

- If the virtual file system is `initramfs`, run the following command to check whether native KVM drivers have been installed:

```
lsinitrd /boot/initramfs-`uname -r`.img | grep virtio
```

If the virtual file system is `initrd`, run the following command to check whether native KVM drivers have been installed:

```
lsinitrd /boot/initrd-`uname -r` | grep virtio
```

Assume that the virtual file system is `initramfs`. The following command output will be displayed:

```
[root@CTU10000xxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep virtio
-rwxr--r-- 1 root root 23448 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
block/virtio_blk.ko
-rwxr--r-- 1 root root 50704 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/
drivers/net/virtio_net.ko
-rwxr--r-- 1 root root 28424 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
scsi/virtio_scsi.ko
drwxr-xr-x 2 root root 0 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio
```

```
-rwxr--r-- 1 root root 14544 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/virtio/virtio.ko
-rwxr--r-- 1 root root 21040 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/virtio/virtio_pci.ko
-rwxr--r-- 1 root root 18016 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/virtio/virtio_ring.ko
```

#### NOTE

If you add built-in drivers to the `initrd` or `initramfs` file, the ECS will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the `lsinitrd` command. You can run the following command to check whether the drivers are built-in ones in the kernel:

```
cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y
```

## Ubuntu and Debian

1. Run the following command to open the `modules` file:  
**vi /etc/initramfs-tools/modules**
2. Press **i** to enter the editing mode and add VirtIO drivers to the `/etc/initramfs-tools/modules` file (the format varies depending on the OS).

```
[root@CTU10000xxxx ~]#vi /etc/initramfs-tools/modules
...
Examples:
#
raid1
sd_mOd
virtio_blk
virtio_scsi
virtio_net
virtio_pci
virtio_ring
virtio
```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the `/etc/initramfs-tools/modules` file.
4. Run the following command to regenerate `initrd`:  
**update-initramfs -u**
5. Run the following command to check whether native KVM drivers have been installed:

```
lsinitramfs /boot/initrd.img-`uname -r` |grep virtio
```

```
[root@ CTU10000xxxx home]# lsinitramfs /boot/initrd.img-`uname -r` |grep virtio
lib/modules/3.5.0-23-generic/kernel/drivers/scsi/virtio_scsi.ko
```

#### NOTE

If you add built-in drivers to the `initrd` or `initramfs` file, the ECS will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the `lsinitrd` command. You can run the following command to check whether the drivers are built-in ones in the kernel:

```
[root@ CTU10000xxxx home]# cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y
CONFIG_VIRTIO_BLK=y
CONFIG_VIRTIO_NET=y
CONFIG_VIRTIO=y
CONFIG_VIRTIO_RING=y
CONFIG_VIRTIO_PCI=y
CONFIG_VIRTIO_MMIO_CMDLINE_DEVICES=y
```

## SUSE and openSUSE (Earlier than SUSE 12 SP1 or openSUSE 13)

Modify the `/etc/sysconfig/kernel` file.

1. Run the following command to modify the `/etc/sysconfig/kernel` file:  
**vi /etc/sysconfig/kernel**
2. Add VirtIO drivers to `INITRD_MODULES=""` (the format of drivers depends on the OS).

```
SIA10000xxxxx:~ # vi /etc/sysconfig/kernel
(like drivers for scsi-controllers, for lvm or reiserfs)
#
INITRD_MODULES="ata_piix ata_generic virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring
virtio"
```

3. Run the `mkinitrd` command to generate `initrd` again.

#### NOTE

If the virtual file system is not the default `initramfs` or `initrd`, run the `dracut -f Name of the initramfs or initrd file actually used` command. The actual `initramfs` or `initrd` file name can be obtained from the `menu.lst` or `grub.cfg` file (`/boot/grub/menu.lst`, `/boot/grub/grub.cfg`, or `/boot/grub2/grub.cfg`).

The following is an example `initrd` file of SUSE 11 SP4:

```
default 0
timeout 10
gfxmenu (hd0,0)/boot/message
title sles11sp4_001_[_VMX_]
root (hd0,0)
kernel /boot/linux.vmx vga=0x314 splash=silent console=ttyS0,115200n8 console=tty0 net.ifnames=0
NON_PERSISTENT_DEVICE_NAMES=1 showopts
initrd /boot/initrd.vmx
title Failsafe_sles11sp4_001_[_VMX_]
root (hd0,0)
kernel /boot/linux.vmx vga=0x314 splash=silent ide=nodma apm=off noresume edd=off
powersaved=off nohz=off highres=off processor.max+cstate=1 nomodeset x11failsafe
console=ttyS0,115200n8 console=tty0 net.ifnames=0 NON_PERSISTENT_DEVICE_NAMES=1 showopts
initrd /boot/initrd.vmx
```

`/boot/initrd.vmx` in the `initrd` line is the `initrd` file actually used. Run the `dracut -f /boot/initrd.vmx` command. If the `initrd` file does not contain the `/boot` directory, such as `/initramfs-xxx`, run the `dracut -f /boot/initramfs-xxx` command.

4. Run the following command to check whether KVM VirtIO drivers have been installed:

#### **lsinitrd /boot/initrd-`uname -r` | grep virtio**

```
SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/
virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
virtio_net.ko
```

5. Restart the ECS.
6. Run the following command to check whether KVM drivers exist in `initrd`:

#### **lsinitrd /boot/initrd-`uname -r` | grep virtio**

```
SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/
virtio_scsi.ko
```

```
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
virtio_net.ko
```

#### NOTE

If you add built-in drivers to the `initrd` or `initramfs` file, the ECS will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the `lsinitrd` command. You can run the following command to check whether the drivers are built-in ones in the kernel:

```
cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y
```

## SUSE and openSUSE (SUSE 12 SP1)

Modify the `/etc/dracut.conf` file.

1. Run the following command to open the `/etc/dracut.conf` file:

```
vi /etc/dracut.conf
```

2. Press `i` to enter the editing mode and add VirtIO drivers to **add-drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxx ~]# vi /etc/dracut.conf
additional kernel modules to the default
add_drivers+="ata_piix ata_generic virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring virtio"
```

3. Press `Esc`, enter `:wq`, and press `Enter`. The system saves the change and exits the `/etc/dracut.conf` file.
4. Run the following command to regenerate `initrd`:

```
dracut -f /boot/initramfs-File name
```

If the virtual file system is not the default `initramfs`, run the `dracut -f Name of the initramfs or initrd file actually used` command. The actual `initramfs` or `initrd` file name can be obtained from the `grub.cfg` file, which can be `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, or `/boot/grub/grub.conf` depending on the OS.

5. If the virtual file system is `initramfs`, run the following command to check whether native KVM drivers have been installed:

```
lsinitrd /boot/initramfs-`uname -r`.img | grep virtio
```

If the virtual file system is `initrd`, run the following command to check whether native KVM drivers have been installed:

```
lsinitrd /boot/initrd-`uname -r` | grep virtio
```

## SUSE and openSUSE (Later than SUSE 12 SP1 or openSUSE 13)

Modify the `/etc/dracut.conf` file.

Take SUSE Linux Enterprise Server 12 SP2 (x86\_64) as an example.

1. Run the following command to open the `/etc/dracut.conf` file:

```
vi /etc/dracut.conf
```



2. Press **i** to enter the editing mode and add VirtIO drivers to **add\_drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxx ~]# vi /etc/dracut.conf
additional kernel modules to the default
add_drivers+="ata_piix ata_generic virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring virtio"
```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

4. Run the following command to regenerate initrd:

```
dracut -f /boot/initramfs-File name
```

If the virtual file system is not the default initramfs, run the **dracut -f Name of the initramfs or initrd file actually used** command. The actual initramfs or initrd file name can be obtained from the **grub.cfg** file, which can be **/boot/grub/grub.cfg**, **/boot/grub2/grub.cfg**, or **/boot/grub/grub.conf** depending on the OS.

5. If the virtual file system is initramfs, run the following command to check whether native KVM drivers have been installed:

```
lsinitrd /boot/initramfs-`uname -r`.img | grep virtio
```

If the virtual file system is initrd, run the following command to check whether native KVM drivers have been installed:

```
lsinitrd /boot/initrd-`uname -r` | grep virtio
```

Assume that the virtual file system is initrd. The following command output will be displayed:

```
sluo-ecs-30dc:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rw-r--r-- 1 root root 29335 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/block/
virtio_blk.ko
-rw-r--r-- 1 root root 57007 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/net/
virtio_net.ko
-rw-r--r-- 1 root root 32415 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/scsi/
virtio_scsi.ko
drwxr-xr-x 2 root root 0 Sep 28 10:21 lib/modules/4.4.21-69-default/kernel/drivers/virtio
-rw-r--r-- 1 root root 19623 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio.ko
-rw-r--r-- 1 root root 38943 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/
virtio_pci.ko
-rw-r--r-- 1 root root 24431 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/
virtio_ring.ko
```

#### NOTE

If you add built-in drivers to the initrd or initramfs file, the ECS will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the **lsinitrd** command. You can run the following command to check whether the drivers are built-in ones in the kernel:

```
cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y
```

## 3.9.8 Clearing System Logs

Delete log files and historical records, and stop the ECS.

1. Run the following commands to delete redundant key files:

```
echo > /$path/$to/$root/.ssh/authorized_keys
```

An example command is **echo > /root/.ssh/authorized\_keys**.

```
echo > /$path/$to/$none-root/.ssh/authorized_keys
```

An example command is **echo > /home/linux/.ssh/authorized\_keys**.

2. Run the following command to clear log files in the `/var/log` directory:

```
rm -rf /var/log/*
```

 NOTE

Before deleting log files, back up log directories and log files required by application startup. For example, if the default Nginx log directory `/var/log/nginx` is deleted, Nginx may fail to be started.

3. Run the following commands to delete historical records:

```
echo > /root/.bash_history
```

```
history -c
```

## 3.10 Encrypting Images

### 3.10.1 Overview

IMS allows you to create encrypted images to ensure data security.

 NOTE

To use the image encryption function, you must apply for KMS Administrator permissions.

#### Constraints

- DEW must be enabled.
- Encrypted images cannot be shared with others.
- Encrypted images cannot be published in KooGallery.
- The system disk of an ECS created from an encrypted image is also encrypted, and its key is the same as the image key.
- If an ECS has an encrypted system disk, private images created from the ECS are also encrypted.
- The key used for encrypting an image cannot be changed.
- If the key used for encrypting an image is disabled or deleted, the image is unavailable.

### 3.10.2 Creating Encrypted Images

You can create an encrypted image using an external image file or an encrypted ECS.

- Create an encrypted image using an external image file.

When you register the external image file as a private image, select **KMS encryption** and select a key. For details, see [Creating a Windows System Disk Image from an External Image File](#) and [Creating a Linux System Disk Image from an External Image File](#).

- Create an encrypted image using an encrypted ECS.

When you use an ECS to create a private image, if the system disk of the ECS is encrypted, the private image created using the ECS is also encrypted. The key used for encrypting the image must be the same as that used for

encrypting the system disk. For details, see [Creating a System Disk Image from a Linux ECS](#).

## 3.11 Replicating Images Within a Region

### Scenarios

You can convert encrypted and unencrypted images into each other or enable some advanced features (such as fast ECS creation from an image) using in-region image replication. You may need to replicate an image to:

- Replicate an encrypted image to an unencrypted one.  
Encrypted images cannot be shared with other tenants. If you want to share an encrypted image, you can replicate it to an unencrypted one.
- Replicate an encrypted image to an encrypted one.  
Keys for encrypting the images cannot be changed. If you want to change the key of an encrypted image, you can replicate this image to a new one and encrypt the new image using an encryption key.
- Replicate an unencrypted image to an encrypted one.  
If you want to store an unencrypted image in an encrypted way, you can replicate this image as a new one and encrypt the new image using a key.
- Optimize a system disk image so that it can be used to quickly create ECSs.  
Fast Create greatly reduces the time required for creating ECSs from a system disk image. Currently, this feature is supported by all newly created system disk images by default. Existing system disk images may not support this function. You can optimize the images through in-region image replication. For example, if image A does not support fast ECS creation, you can replicate it to generate image copy\_A that supports fast ECS creation.

### Constraints

- Full-ECS images cannot be replicated within the same region.
- Private images created using ISO files do not support in-region replication.

### Prerequisites

The images to be replicated are in the **Normal** state.

### Procedure

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Locate the row that contains the image to be replicated, click **More** in the **Operation** column, and select **Replicate**.
3. In the displayed **Replicate Image** dialog box, set the following parameters:
  - **Name**: Enter a name that is easy to identify.

- **Enterprise Project:** Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. To enable this function, contact your customer manager.
  - **Description:** This parameter is optional. Enter description of the replication.
  - **Encryption:** If you want to encrypt the image or change a key, select **KMS encryption** and select the key you want to use from the drop-down list.
4. Click **OK**.
- On the **Private Images** page, view the replication progress. If the status of the new image becomes **Normal**, the image replication is successful.

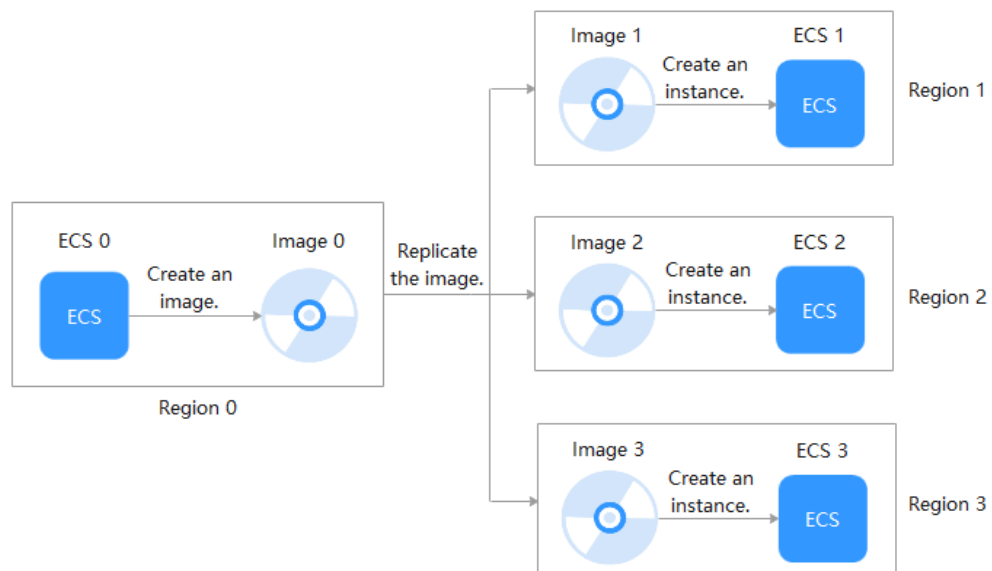
## 3.12 Replicating Images Across Regions

### Scenarios

An image is a regional resource. If you want to use a private image in another region, you can replicate it to the target region.

Cross-region image replication is required for system HA typically when your system is deployed in multiple regions. In most cases, ECSs are deployed in multiple regions (including regions outside China). If you want to clone an ECS across regions, you can replicate its image across the regions and then use the image to create the identical ECSs in the target region.

**Figure 3-22** Typical cross-region replication



### Background

- Cross-region replication is applicable to cross-region server deployment or data backup. It is often used together with image sharing for cross-region,

cross-account image replication. The following table describes image replication in different scenarios.

| Scenario                                        | Description                                                                                                                                                                                                      | Procedure                                                       |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Cross-region replication under the same account | After the replication is complete, a new image is generated in the target region. The new image has an ID that is different from the source image ID.                                                            | See this section.                                               |
| Cross-region, cross-account replication         | Replicate the image to the target region and share it with other accounts.                                                                                                                                       | See this section and <a href="#">Sharing Specified Images</a> . |
| Cross-account replication in the same region    | After the replication is complete, the image is shared with the target tenant. The target tenant can use the image (with the same ID as the source image) but the image owner is still the tenant who shared it. | See <a href="#">Sharing Specified Images</a> .                  |

- When a full-ECS image is replicated across regions, the associated CSBS or CBR backups will also be replicated. Therefore, you will be charged for these backups in the target region.
- The time required for replicating an image across regions depends on the network speed, image size, and the number of concurrent tasks.
- You can select multiple images for cross-region replication at a time. However, you are not allowed to select an ISO image, encrypted image, full-ECS image, frozen image, or the image that is being created.
- An agency is required for cross-region image replication. This agency has the permissions of IMS Administrator, allowing you to perform operations on the projects in the destination region.

For example, if you want to replicate an image from region A to region B, the agency must have the permissions of IMS Administrator in region B. For how to create an agency, see [Create an Agency](#).

## Constraints

- Cross-region replication of full-ECS images is only available for certain regions. You can see on the console if it is available for a given region.  
If a full-ECS image cannot be replicated to a different region, you can use it to create an ECS, use the ECS to create a system disk image and a data disk image, and replicate the images to the destination region.  
A full-ECS image created using an ECS backup can be replicated from the region where they reside to another region, but the replicated full-ECS image cannot be replicated across regions again.
- You can replicate only private images across regions. If you want to replicate an image of another type (for example, a public image) across regions, you

can use the image to create an ECS, use the ECS to create a private image, and then replicate the private image across regions.

 **NOTE**

A private image cannot be replicated across regions after it is published in KooGallery.

- To perform cross-region replication, IAM users must have the IAM `ReadOnlyAccess` permission and the IMS `FullAccess` permission in both the source and destination regions.
- The size of each image to be replicated across regions cannot be larger than 128 GB.
- You can replicate only five images across regions at a time.
- ISO images and encrypted images cannot be replicated across regions.

## Procedure

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
3. Locate the row that contains the image to be replicated, click **More** in the **Operation** column, and select **Replicate**.
4. In the displayed **Replicate Image** dialog box, set the following parameters.

 **NOTE**

If the current region does not support cross-region replication, set the parameters by referring to [Replicating Images Within a Region](#).

**Figure 3-23** Replicating an image across regions

**Replicate Image** [X]

Image Size: 9.7 GB

OS Type: Windows

OS: Windows-Server-2012-R2-Datacenter-64bit

Created: Dec 02, 2020 11:22:41 GMT+08:00

Replication Mode:  Within Region  Across Regions

\* Name:

\* Destination Region:

\* Destination Project:

\* IAM Agency:  [View Agency](#) [?](#)

- **Replication Mode:** Select **Across Regions**.
- **Name:** Enter a name that is easy to identify. The image name is in the following format: **copy\_Name of the source region where the image is located\_Source image name**.
- **Destination Region:** Select the region where you want to use the image.
- **Destination Project:** Select a project in the destination region. After you select the destination region, the system automatically displays available projects.
- **Target Server Backup Vault:** This parameter is available only for full-ECS images created using CBR backups. Select a vault for storing backups. If no CBR backup vault is available in the destination region, click **Create Server Backup Vault** to create one. Ensure that you select **Replication** for **Protection Type**. For other parameters, see [Purchasing a Server Backup Vault](#). After the vault is created, click [Refresh](#) to refresh the page and select the vault from the drop-down list box.
- **IAM Agency:** Select an IAM agency.
- **Description:** This parameter is optional. Enter description of the replication.

5. Click **OK**.

Switch to the destination region. If the image status becomes **Normal**, the image replication is successful.

 **NOTE**

The time required for replicating an image across regions depends on the network speed, image size, and the number of concurrent tasks.

## Create an Agency

1. Log in to the management console.
2. In the upper right corner of the page, click the username and select **Identity and Access Management**.
3. In the navigation pane, choose **Agencies**.
4. Click **Create Agency**.
5. On the **Create Agency** page, set the following parameters:
  - **Agency Name**: Enter an agency name, such as **ims\_admin\_agency**.
  - **Agency Type**: Select **Cloud service**.
  - **Cloud Service**: This parameter is available only if you select **Cloud service** for **Agency Type**. Select **Image Management Service (IMS)** from the drop-down list.
  - **Validity Period**: Select **Unlimited**.
  - **Description**: This parameter is optional. You can enter **Agency with IMS Administrator privileges**.
6. Click **Next**.
  - Select **Region-specific projects** for **Scope** and select one or more projects from the drop-down list.

---

 **CAUTION**

Do not select **All projects**, or the created agency will be invalid.

---

- Select **IMS Administrator** for **Permissions**.
7. Click **OK**.

## 3.13 Tagging an Image

### Scenarios

You can use tags to classify images. You can add, modify, or delete image tags, or search for required images by tag in the image list.

 **NOTE**

- When adding predefined tags to an image or searching for an image using predefined tags, you must have permission to access the Tag Management Service (TMS).



## Constraints

An image can have a maximum of 10 tags.

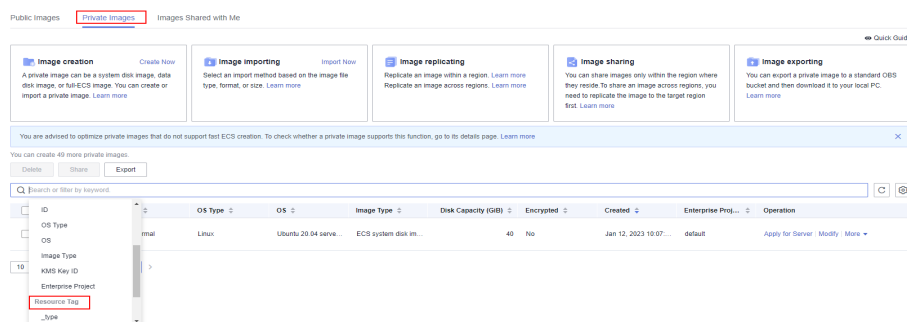
## Add, Delete, and Modify Image Tags

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Private Images** tab and click the image name to display the image details.
  - To modify an image tag, go to **3**.
  - To delete an image tag, go to **4**.
  - To add an image tag, go to **5**.
3. Click the **Tags** tab, locate the target tag, and click **Edit** in the **Operation** column. In the displayed dialog box, modify the tag.
4. Click the **Tags** tab, locate the target tag, and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.
5. Click the **Tags** tab and then **Add Tag**. In the displayed dialog box, add a tag.

## Search for Private Images by Tag

1. Access the IMS console.
  - a. Log in to the management console.
  - b. Under **Compute**, click **Image Management Service**.  
The IMS console is displayed.
2. Click the **Private Images** tab and click the search box above the private image list. Specify tag keys and values under **Resource Tag** to search for private images.

**Figure 3-24** Searching for images by tag



### NOTE

- Neither the tag key nor tag value can be empty. When the tag key and tag value are matched, the system automatically shows your desired private images.
- You can add multiple tags to search for shared images. The system will display private images that match all tags.

## 3.14 Auditing Key Operations

### 3.14.1 IMS Operations Recorded by CTS

#### Scenarios

Cloud Trace Service (CTS) is a log audit service provided by Huawei Cloud and intended for cloud security. It allows you to collect, store, and query cloud resource operation records and use these records for security analysis, compliance auditing, resource tracking, and fault locating.

You can use CTS to record IMS operations for later querying, auditing, and backtracking.

#### Prerequisites

You need to enable CTS before using it. If it is not enabled, IMS operations cannot be recorded. After being enabled, CTS automatically creates a tracker to record all your operations. The tracker stores only the operations of the last seven days. To store the operations for a longer time, store trace files in OBS buckets.

#### IMS Operations Recorded by CTS

**Table 3-3** IMS operations that can be recorded by CTS

| Operation                                                                | Resource Type | Trace Name    |
|--------------------------------------------------------------------------|---------------|---------------|
| Creating an Image                                                        | ims           | createImage   |
| Modifying an image                                                       | ims           | updateImage   |
| Deleting images in a batch                                               | ims           | deleteImage   |
| Replicating an image                                                     | ims           | copyImage     |
| Exporting an image                                                       | ims           | exportImage   |
| Adding a tenant that can use a shared image                              | ims           | addMember     |
| Modifying tenants that can use a shared image                            | ims           | updateMember  |
| Deleting tenants from the group where the members can use a shared image | ims           | deleteMemeber |

**Table 3-4** Relationship between IMS operations and native OpenStack APIs

| Operation                                                                 | Trace Name   | Service Type | Resource Type | OpenStack Component |
|---------------------------------------------------------------------------|--------------|--------------|---------------|---------------------|
| Creating an Image                                                         | createImage  | IMS          | image         | glance              |
| Modifying/<br>Uploading an image                                          | updateImage  | IMS          | image         | glance              |
| Deleting an image                                                         | deleteImage  | IMS          | image         | glance              |
| Tagging an image                                                          | addTag       | IMS          | image         | glance              |
| Deleting an image tag                                                     | deleteTag    | IMS          | image         | glance              |
| Adding a tenant that can use a shared image                               | addMember    | IMS          | image         | glance              |
| Modifying information about a tenant that can use a shared image          | updateMember | IMS          | image         | glance              |
| Deleting a tenant from the group where the members can use a shared image | deleteMember | IMS          | image         | glance              |

## 3.14.2 Viewing Traces




### Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

- [Viewing Real-Time Traces in the Trace List](#)

## Viewing Real-Time Traces in the Trace List

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment > Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Set filters to search for your desired traces. The following filters are available:
  - **Trace Type, Trace Source, Resource Type, and Search By:** Select a filter from the drop-down list.
    - If you select **Resource ID** for **Search By**, specify a resource ID.
    - If you select **Trace name** for **Search By**, specify a trace name.
    - If you select **Resource name** for **Search By**, specify a resource name.
  - **Operator:** Select a user.
  - **Trace Status:** Select **All trace statuses, Normal, Warning, or Incident**.
  - **Time range:** You can query traces generated during any time range in the last seven days.
  - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
5. Click **Query**.
6. On the **Trace List** page, you can also export and refresh the trace list.
  - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
  - Click  to view the latest information about traces.
7. Click  on the left of a trace to expand its details.

| Trace Name         | Resource Type  | Trace Source | Resource ID | Resource Name  | Trace Status | Operator | Operation Time                  | Operation                  |
|--------------------|----------------|--------------|-------------|----------------|--------------|----------|---------------------------------|----------------------------|
| createDockerConfig | dockerlogincmd | SWR          | -           | dockerlogincmd | normal       |          | Nov 16, 2023 10:54:04 GMT+08:00 | <a href="#">View Trace</a> |

|               |                                                                           |
|---------------|---------------------------------------------------------------------------|
| request       |                                                                           |
| trace_id      |                                                                           |
| code          | 200                                                                       |
| trace_name    | createDockerConfig                                                        |
| resource_type | dockerlogincmd                                                            |
| trace_rating  | normal                                                                    |
| api_version   |                                                                           |
| message       | createDockerConfig, Method: POST URI=/v2/management/ulits/secret, Reason: |
| source_ip     |                                                                           |
| domain_id     |                                                                           |
| trace_type    | ApiCall                                                                   |

8. Click **View Trace** in the **Operation** column. The trace details are displayed.

View Trace

```
{
 "request": "",
 "trace_id": " ",
 "code": "200",
 "trace_name": "createDockerConfig",
 "resource_type": "dockerlogincmd",
 "trace_rating": "normal",
 "api_version": "",
 "message": "createDockerConfig, Method: POST Url=/v2/management/Utils/secret. Reason:",
 "source_ip": " ",
 "domain_id": " ",
 "trace_type": "ApiCall",
 "service_type": "SWR",
 "event_type": "system",
 "project_id": " ",
 "response": "",
 "resource_id": "",
 "tracker_name": "system",
 "time": "Nov 16, 2023 10:54:04 GMT+08:00",
 "resource_name": "dockerlogincmd",
 "user": {
 "domain": {
 "name": " ",
 "id": " "
 }
 }
}
```

- 9. For details about key fields in the trace structure, see section "Trace References" > "Trace Structure" and section "Trace References" > "Example Traces" in the *CTS User Guide*.

# 4 Windows Operations

---

## 4.1 Setting the NIC to DHCP

### Scenarios

If a private image is created from an ECS or external image file and the VM where the ECS or external image file is located is configured with a static IP address, you need to change the NIC attribute to DHCP so that the new ECSs created from the private image can dynamically obtain an IP address.

This section uses Windows Server 2008 R2 as an example to describe how to configure DHCP. For details about how to configure DHCP on ECSs running other OSs, see the relevant OS documentation.

#### NOTE

When registering an external image file as a private image, configure DHCP on the VM where the external image file is located. You are advised to configure DHCP on the VM and then export the image file.

### Prerequisites

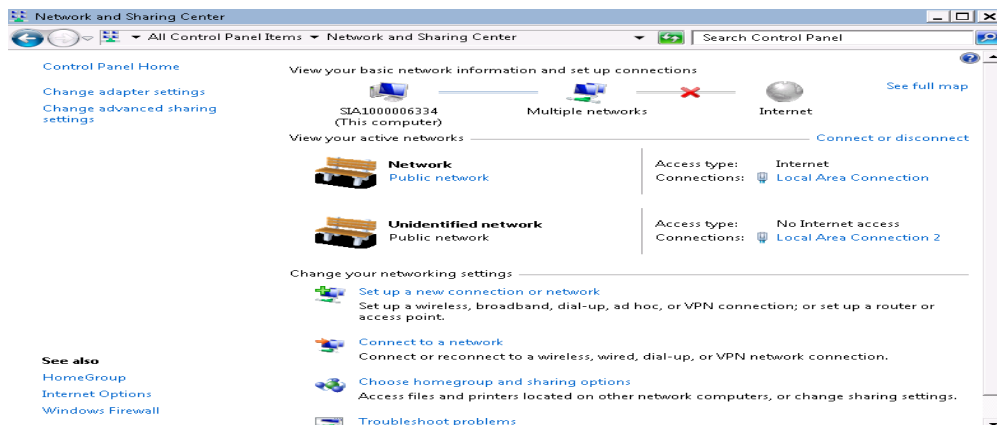
You have logged in to the ECS used to create a Windows private image.

For details about how to log in to an ECS, see *Elastic Cloud Server User Guide*.

### Procedure

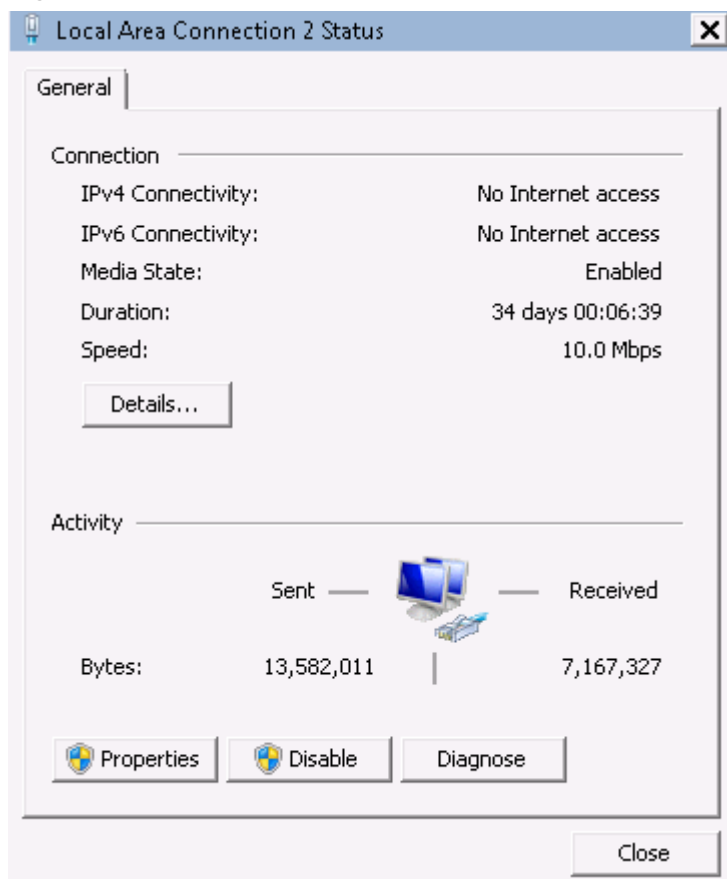
1. On the ECS, choose **Start > Control Panel**.
2. Click **Network and Internet Connections**.
3. Click **Network and Sharing Center**.

**Figure 4-1** Network and Sharing Center



4. Select the connection configured with the static IP address. For example, click **Local Area Connection 2**.

**Figure 4-2** Local Area Connection 2 Status

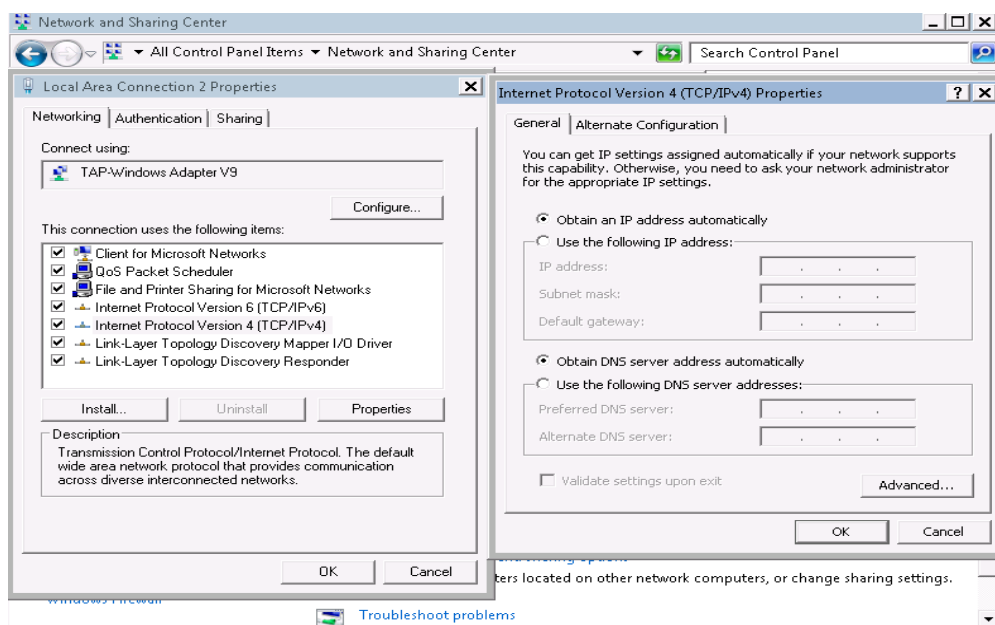


5. Click **Properties** and select the configured Internet protocol version.
6. On the **General** tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**, as shown in [Figure 4-3](#). The system will automatically obtain an IP address.

**NOTE**

You are advised to record the original network information so that you can restore the network if necessary.

Figure 4-3 Configuring DHCP



## 4.2 Enabling Remote Desktop Connection

### Scenarios

If you want to remotely access an ECS, enable remote desktop connection for the source ECS when creating a private image. This function must be enabled for GPU-accelerated ECSs.

#### NOTE

When registering an external image file as a private image, enable remote desktop connection on the VM where the external image file is located. You are advised to enable this function on the VM and then export the image file.

### Prerequisites

You have logged in to the ECS used to create a Windows private image.

For details about how to log in to an ECS, see *Elastic Cloud Server User Guide*.

### Procedure

1. Before enabling this function, you are advised to set the resolution of the ECS to 1920×1080.

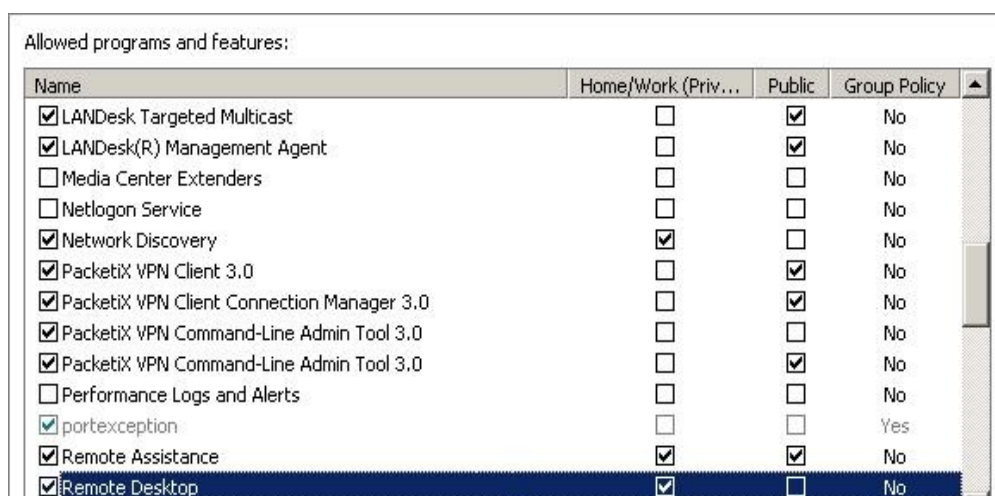
On the ECS, choose **Start > Control Panel**. Under **Appearance and Personalization**, click **Adjust screen resolution**. Then select a proper value from the **Resolution** drop-down list box.

2. Choose **Start**, right-click **Computer**, and choose **Properties** from the shortcut menu.



3. Click **Remote settings**.
4. In the **Remote** tab, select **Allow connections from computers running any version of Remote Desktop (less secure)**.
5. Click **OK**.
6. Choose **Start > Control Panel** and navigate to **Windows Firewall**.
7. Choose **Allow a program or feature through Windows Firewall** in the left pane.
8. Select programs and features that are allowed by the Windows firewall for **Remote Desktop** based on your network requirements and click **OK** in the lower part.

**Figure 4-4** Configuring remote desktop



## 4.3 Installing and Configuring Cloudbase-Init

### Scenarios

To ensure that you can use the user data injection function to inject initial custom information into ECSs created from a private image (such as setting the ECS login password), install Cloudbase-Init on the ECS used to create the image.

- If Cloudbase-Init is not installed, you cannot configure an ECS. As a result, you can only use the password in the image file to log in to the ECS.
- By default, ECSs created from a public image have Cloudbase-Init installed. You do not need to install or configure Cloudbase-Init on such ECSs.
- For ECSs created from external image files, install and configure Cloudbase-Init by performing the operations in this section.

#### NOTE

Cloudbase-Init is open-source software. If the installed version has security vulnerabilities, you are advised to upgrade it to the latest version.

## Prerequisites

- An EIP has been bound to the ECS.
- You have logged in to the ECS.
- The IP address obtaining mode of the ECS is DHCP.

## Install Cloudbase-Init

1. On the Windows **Start** menu, choose **Control Panel > Programs > Programs and Features** and check whether Cloudbase-Init 1.1.2 is installed.
  - If Cloudbase-Init 1.1.2 is installed, skip the subsequent steps and go to [Configure Cloudbase-Init](#).
  - If Cloudbase-Init is installed but the version is not 1.1.2, uninstall Cloudbase-Init and go to the next step.
  - If Cloudbase-Init is not installed, go to the next step.
2. Check whether the version of the OS is Windows desktop.
  - If yes, go to [3](#).
  - If the OS is Windows Server, go to [4](#).
3. Enable the administrator account (Windows 7 is used as an example).
  - a. Click **Start** and choose **Control Panel > System and Security > Administrative Tools**.
  - b. Double-click **Computer Management**.
  - c. Choose **System Tools > Local Users and Groups > Users**.
  - d. Right-click **Administrator** and select **Properties**.
  - e. Deselect **Account is disabled**.
4. Download the Cloudbase-Init installation package.

Download the Cloudbase-Init installation package of the appropriate version based on the OS architecture from the Cloudbase-Init official website (<http://www.cloudbase.it/cloud-init-for-windows-instances/>).

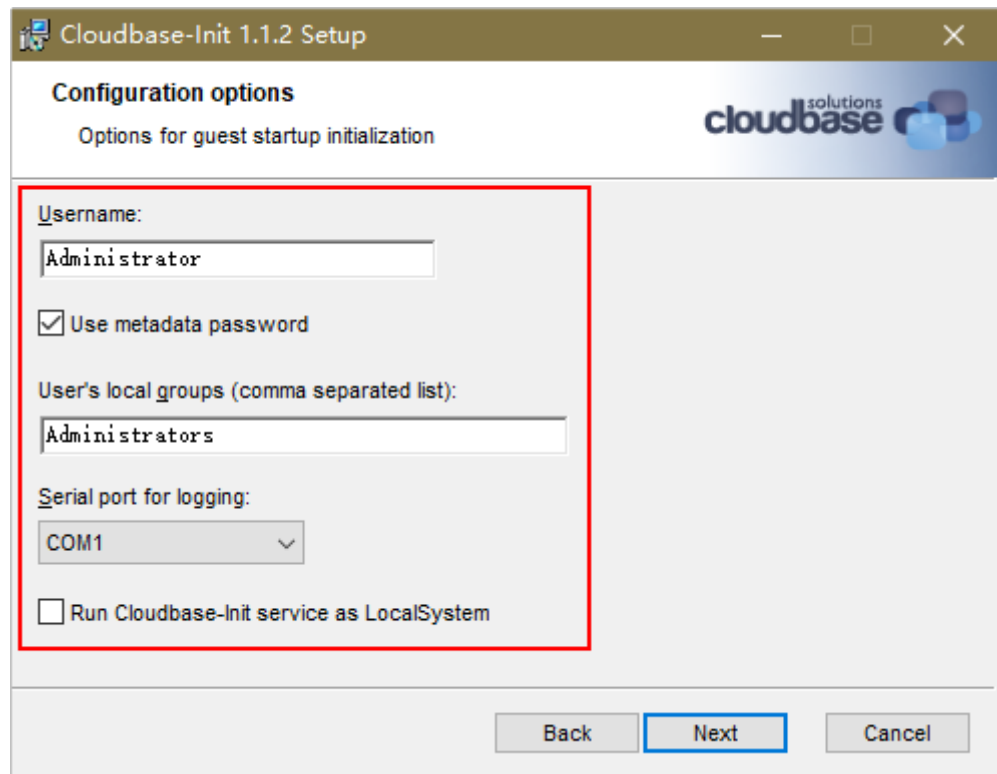
To obtain the stable version, visit the following paths:

  - 64-bit: [https://www.cloudbase.it/downloads/CloudbaseInitSetup\\_Stable\\_x64.msi](https://www.cloudbase.it/downloads/CloudbaseInitSetup_Stable_x64.msi)
  - 32-bit: [https://www.cloudbase.it/downloads/CloudbaseInitSetup\\_Stable\\_x86.msi](https://www.cloudbase.it/downloads/CloudbaseInitSetup_Stable_x86.msi)
5. Double-click the Cloudbase-Init installation package.
6. Click **Next**.
7. Select **I accept the terms in the License Agreement** and click **Next**.
8. Retain the default path and click **Next**.
9. In the **Configuration options** window, enter **Administrator** for **Username**, select **COM1** for **Serial port for logging**, and ensure that **Run Cloudbase-Init service as LocalSystem** is not selected.

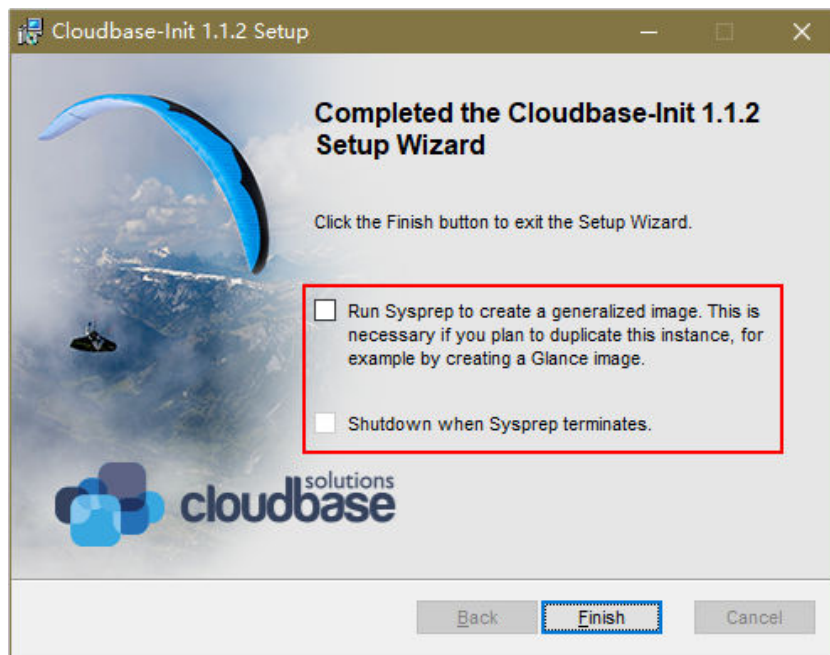
### NOTE

The version number shown in the figure is for reference only.

**Figure 4-5** Configuring parameters



10. Click **Next**.
11. Click **Install**.
12. In the **Files in Use** dialog box, select **Close the application and attempt to restart them** and click **OK**.
13. Check whether the version of the OS is Windows desktop.
  - If yes, go to **15**.
  - If no, go to **14**.
14. In the **Completed the Cloudbase-Init Setup Wizard** window, ensure that neither option is selected.

**Figure 4-6** Completing the Cloudbase-Init installation**NOTE**

The version number shown in the figure is for reference only.

15. Click **Finish**.

## Configure Cloudbase-Init

1. Edit the configuration file **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf** in the Cloudbase-Init installation path.

- a. Add **netbios\_host\_name\_compatibility=false** to the last line of the file so that the hostname supports a maximum of 63 characters.

**NOTE**

NetBIOS contains no more than 15 characters due to Windows system restrictions.

- b. Add **metadata\_services=cloudbaseinit.metadata.services.httpservice.HttpService** to enable the agent to access the IaaS OpenStack data source.
- c. Add **plugins** to configure the plugins that will be loaded. Separate different plugins with commas (,). The information in bold is the keyword of each plugin.

- The following plugins are loaded by default. You can keep all or some of them as needed.

```
plugins=cloudbaseinit.plugins.common.localscripts.LocalScriptsPlugin,cloudbaseinit.plugins.common.mtu.MTUPlugin,cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,cloudbaseinit.plugins.common.setuserpassword.SetUserPasswordPlugin,cloudbaseinit.plugins.common.sshpublickeys.SetUserSSHPublicKeysPlugin,cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin,cloudbaseinit.plugins.windows.extendvolumes.ExtendVolumesPlugin,cloudbaseinit.plugins.common.userdata.UserDataPlugin,cloudbaseinit.plugins.windows.licensing.WindowsLicensingPlugin
```

Plugin functions:

- **LocalScriptsPlugin** configures scripts.
- **MTUPlugin** configures MTU network interfaces.
- **CreateUserPlugin** creates a user.
- **SetUserPasswordPlugin** configures a password.
- **SetUserSSHPublicKeysPlugin** configures a key.
- **SetHostNamePlugin** configures a hostname.
- **ExtendVolumesPlugin** expands disk space.
- **UserDataPlugin** injects user data.
- **WindowsLicensingPlugin** activates Windows instances.

 **NOTE**

If you may change the hostname of ECSs after they are created from this image and services on the ECSs are sensitive to hostname changes, you are not advised to configure the **SetHostNamePlugin** here.

■ **Optional plugins:**

```
plugins=cloudbaseinit.plugins.windows.winrmlistener.ConfigWinRMListenerPlugin,cloudbaseinit.plugins.windows.winrmcertificateauth.ConfigWinRMCertificateAuthPlugin
```

Plugin functions:

- **ConfigWinRMListenerPlugin** configures listening to remote logins.
- **ConfigWinRMCertificateAuthPlugin** configures remote logins without password authentication.

---

 **CAUTION**

The WinRM plug-ins use weak cryptographic algorithm, which may cause security risks. So, you are advised not to load the plug-ins.

---

- d. (Optional) Add the following configuration items to configure the number of retry times and interval for obtaining metadata:

```
retry_count=40
retry_count_interval=5
```
- e. (Optional) Add the following configuration item to prevent metadata network disconnections caused by the default route added by Windows:

```
[openstack]
add_metadata_private_ip_route=False
```
- f. (Optional) If the Cloudbase-Init version is 0.9.12 or later, you can customize the length of the password.  
Change the value of **user\_password\_length** to customize the password length.
- g. (Optional) Add the following configuration item to disable password changing upon first login:  
**first\_logon\_behaviour=no**
- h. (Optional) Add the following configuration item to ensure that time synchronization from BIOS persists through system restarts:  
**real\_time\_clock\_utc=true**

 NOTE

The registry entry **RealTimeIsUniversal=1** allows the system to synchronize time from BIOS. If **real\_time\_clock\_utc=true** is not configured, Cloudbase-Init will revert **RealTimeIsUniversal** back to **0**. As a result, the system cannot synchronize time from BIOS after a restart.

2. Release the current DHCP address so that the created ECSs can obtain correct addresses.

In the Windows command line, run the following command to release the current DHCP address:

**ipconfig /release**

 NOTE

This operation will interrupt network connection and adversely affect ECS use. The network will automatically recover after the ECSs are started again.

3. When creating an image using a Windows ECS, you need to change the SAN policy of the ECS to **OnlineAll**. Otherwise, EVS disks attached to the ECSs created from the image may be offline.

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

**Table 4-1** SAN policies

| Type            | Description                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------|
| OnlineAll       | All newly detected disks are automatically brought online.                                                                         |
| OfflineShared   | All disks on sharable buses, such as iSCSI and FC, are left offline by default, while disks on non-sharable buses are kept online. |
| OfflineInternal | All newly detected disks are left offline.                                                                                         |

- a. Execute **cmd.exe** and run the following command to query the current SAN policy of the ECS using DiskPart:

**diskpart**

- b. Run the following command to view the SAN policy of 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 [3.c](#).
- c. Run the following command to change the SAN policy of the ECS to **OnlineAll**:  
**san policy=onlineall**

## 4.4 Running Sysprep

### Scenarios

Running Sysprep ensures that an ECS has a unique SID after it is added to a domain.

After installing Cloudbase-Init on an ECS, you need to decide whether the ECS needs to be added to a domain or whether it must have a unique SID. If yes, run Sysprep as instructed in this section.

### Prerequisites

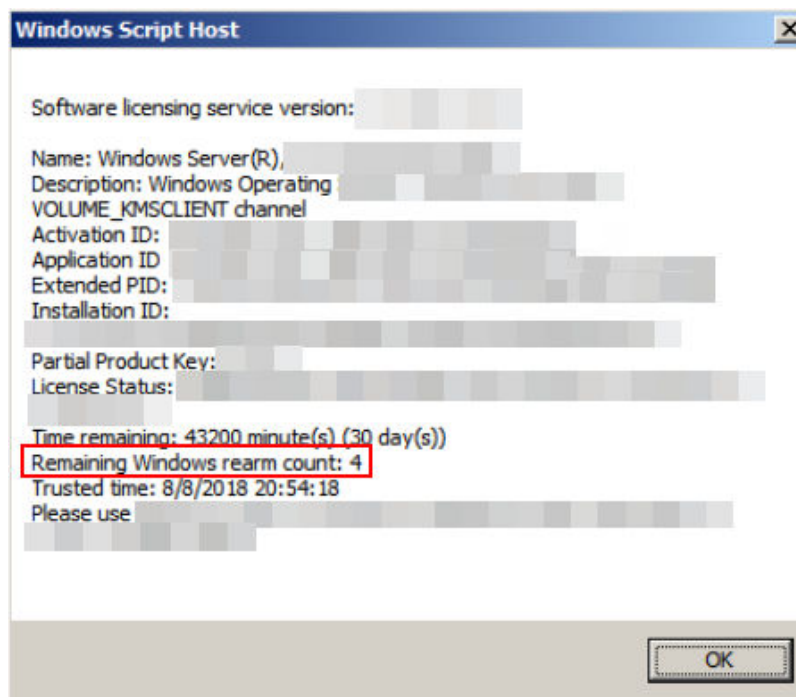
- Run Sysprep as the administrator.
- For a newly activated Windows ECS, you can run Sysprep only once at a time.
- If an ECS is created from an image file, only Sysprep provided by the image file can be used. In addition, Sysprep must always reside in the **%WINDIR%\system32\sysprep** directory.
- Windows must be in the activated state, and the remaining Windows rearm count must be greater than or equal to 1. Otherwise, the Sysprep encapsulation cannot be executed.

Run the following command in the Windows command line and check how many times you can run Sysprep in the displayed **Windows Script Host** dialog box:

```
slmgr.vbs /dlv
```

If the value of **Remaining Windows rearm count** is 0, you cannot run Sysprep.

**Figure 4-7** Windows Script Host



## Procedure

1. Enter the Cloudbase-Init installation directory.  
**C:\Program Files\Cloudbase Solutions\** is used as an example of the Cloudbase-Init installation directory. Switch to the root directory of drive C and run the following command to enter the installation directory:  
**cd C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf**
2. Run the following command to encapsulate Windows:  
**C:\Windows\System32\sysprep\sysprep.exe /generalize /oobe /unattend:Unattend.xml**

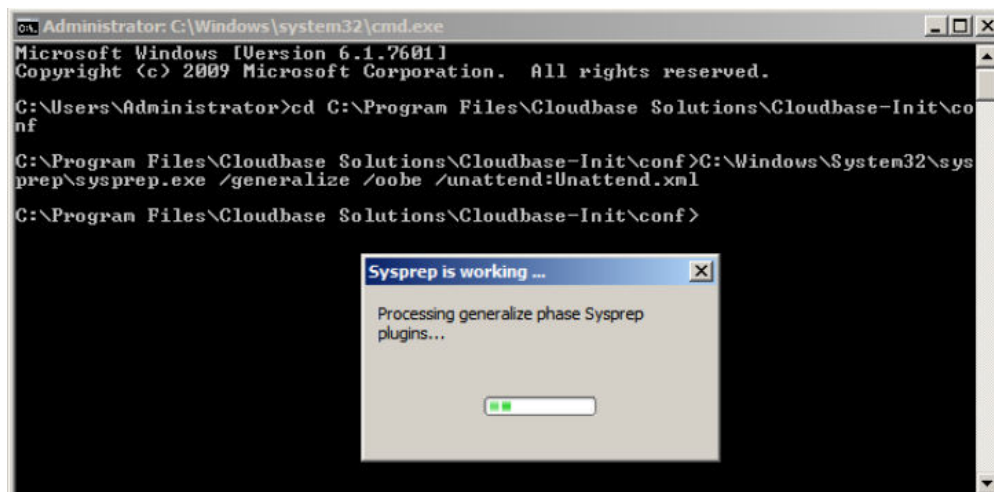
---

### CAUTION

- Ensure that **/unattend:Unattend.xml** is contained in the preceding command. Otherwise, the username, password, and other important configuration information of the ECS will be reset, and you must configure the OS manually when you use ECSs created from the Windows private image.
  - After this command is executed, the ECS will be automatically stopped. After the ECS is stopped, use the ECS to create an image. ECSs created using the image have unique SIDs. If you restart a Windows ECS on which Sysprep has been executed, Sysprep takes effect only for the current ECS. Before creating an image using the ECS, you must run Sysprep again.
  - For Windows Server 2012 and Windows Server 2012 R2, the administrator password of the ECS will be deleted after Sysprep is executed on the ECS. You need to log in to the ECS and reset the administrator password. In this case, the administrator password set on the management console will be invalid. Keep the password you set secure.
  - If a domain account is required for logins, run Sysprep on the ECS before using it to create a private image. For details about the impact of running Sysprep, see [Why Is Sysprep Required for Creating Private Images Using a Windows ECS?](#)
  - The Cloudbase-Init account of a Windows ECS is an internal account of the Cloudbase-Init agent. This account is used for obtaining metadata and completing relevant configuration when the Windows ECS starts. If you modify or delete this account, or uninstall the Cloudbase-Init agent, you will be unable to inject initial custom information into an ECS created from a Windows private image. Therefore, you are not advised to modify or delete the Cloudbase-Init account.
-



Figure 4-8 Running Sysprep



## Follow-up Procedure

1. Create a private image from the ECS on which Sysprep is executed. For details, see [Creating a System Disk Image from a Windows ECS](#).
2. You can use the image to create ECSs. Each ECS has a unique SID.

Run the following command to query the ECS SID:

```
whoami /user
```

Figure 4-9 ECS SID before Sysprep is executed

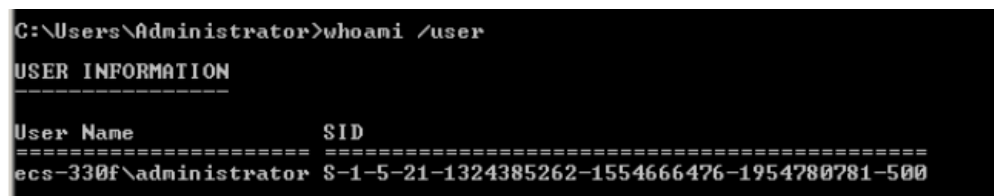
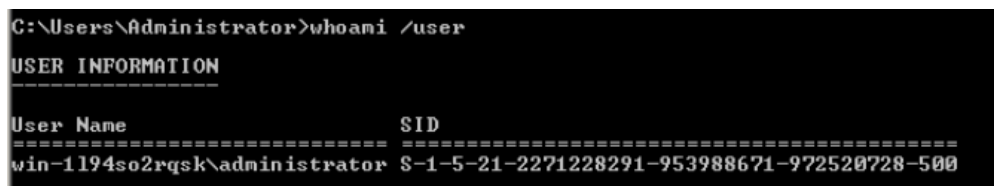


Figure 4-10 ECS SID after Sysprep is executed



## 4.5 Installing Special Windows Drivers

### Scenarios

Before using some types of ECSs to create private images, you need to install special drivers on the ECSs.

## GPU Driver

If you want to use the created private image to create GPU-accelerated ECSs, install a proper GPU driver for the image to enable GPU acceleration. There are two types of NVIDIA Tesla GPU drivers for GPU-accelerated ECSs, Tesla and GRID/vGPU drivers.

- To use graphics acceleration, such as OpenGL, DirectX, or Vulkan, install the GRID/vGPU driver and separately configure a GRID license. The GRID/vGPU driver with a vDWS license also supports CUDA for both computing and graphics acceleration.
- To use NVIDIA CUDA computing acceleration, install the Tesla driver.

# 5 Linux Operations

## 5.1 Setting the NIC to DHCP

### Scenarios

If a private image is created from an ECS or external image file and the VM where the ECS or external image file is located is configured with a static IP address, you need to change the NIC attribute to DHCP so that the new ECSs created from the private image can dynamically obtain an IP address.

The configuration method varies depending on OSs.

#### NOTE

When registering an external image file as a private image, configure DHCP on the VM where the external image file is located. You are advised to configure DHCP on the VM and then export the image file.

### Prerequisites

You have logged in to the ECS used to create a Windows private image.

For details about how to log in to an ECS, see [Login Overview](#).

### Ubuntu 18 or Later

1. Run `vi /etc/netplan/01-netcfg.yaml` on the ECS to open the `/etc/netplan/01-netcfg.yaml` file, and check whether the value of `dhcp4` is `true`.

- If `dhcp4` is set to `true`, enter `:q` to exit the editor. No further action will be required.

```
network:
 version:2
 renderer:NetworkManager
 ethernets:
 eth0:
 dhcp4: true
```

- If `dhcp4` is set to `no` and a static IP address is configured, go to the next step.

```
network:
 version:2
 renderer:NetworkManager
 ethernets:
 eth0:
 dhcp4: no
 addresses: [192.168.1.109/24]
 gateway4: 192.168.1.1
 nameservers:
 addresses: [8.8.8.8,114.114.114.114]
```

2. Press **i** to enter the editing mode.

Delete the static IP address settings and set **dhcp4** to **true**. You can also use a number sign (**#**) to comment out the static IP address settings.

```
network:
 version:2
 renderer:NetworkManager
 ethernets:
 eth0:
 dhcp4: true # Set dhcp4 to true.
 #dhcp4: no # Delete or comment out the static IP address settings.
 #addresses: [192.168.1.109]
 #gateway4: 192.168.1.1
 #nameservers:
 # addresses: [8.8.8.8,114.114.114.114]
```

3. If your ECS has more than one NIC, configure DHCP for all of them.

```
network:
 version:2
 renderer:NetworkManager
 ethernets:
 eth0:
 dhcp4: true
 eth1:
 dhcp4: true
 eth2:
 dhcp4: true
 eth3:
 dhcp4: true
```

4. Press **Esc**, enter **:wq**, and press **Enter** to save the settings and exit the vi editor.
5. Run the **netplan apply** command to make the settings take effect.

## Ubuntu 16.04

1. Run the following command on the ECS to open the **/etc/network/interfaces** file:

### **vi /etc/network/interfaces**

- If DHCP has been configured for all NICs, enter **:q** to exit the vi editor.

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet dhcp
```

- If static IP addresses are set on the NICs, go to **2**.

```
auto lo
iface lo inet loopback
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.109
```

```
netmask 255.255.255.0
gateway 192.168.1.1
```

2. Press **i** to enter the editing mode.
3. Delete the static IP address settings and configure DHCP for the NICs.

You can also use a number sign (**#**) to comment out the static IP address settings.

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
```

If the ECS has multiple NICs, you must configure DHCP for all the NICs.

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
auto eth1
iface eth1 inet dhcp
```

4. Press **Esc**, enter **:wq**, and press **Enter**.  
The system saves the settings and exits the vi editor.

## Related Operations

Configure DHCP to enable the ECS to obtain IP addresses continuously.

- For CentOS and EulerOS, use the vi editor to add **PERSISTENT\_DHCLIENT="y"** to configuration file **/etc/sysconfig/network-scripts/ifcfg-ethX**.
- For SUSE Linux Enterprise, use the vi editor to set **DHCLIENT\_USE\_LAST\_LEASE** to **no** in the configuration file **/etc/sysconfig/network/dhcp**.
- For Ubuntu 12.04 or later, upgrade dhclient to ISC dhclient 4.2.4 so that the NIC can consistently obtain IP addresses from the DHCP server. To perform the upgrade, you need to install isc-dhcp-server first.

## 5.2 Deleting Files from the Network Rule Directory

### Scenarios

To prevent NIC name drift when you use a private image to create ECSs, you need to delete files from the network rule directory of the VM where the ECS or image file is located during the private image creation.

#### NOTE

When registering an external image file as a private image, delete files from the network rule directory on the VM where the external image file is located. You are advised to delete the files on the VM and then export the image file.

### Prerequisites

An OS and VirtIO drivers have been installed on the ECS.

## Procedure

1. Run the following command to query files in the network rule directory:

```
ls -l /etc/udev/rules.d
```

2. Run the following commands to delete the files whose names contain **persistent** and **net** from the network rule directory:

Example:

```
rm /etc/udev/rules.d/30-net_persistent-names.rules
```

```
rm /etc/udev/rules.d/70-persistent-net.rules
```

The italic content in the commands varies depending on your environment.

### NOTE

For CentOS 6 images, to prevent NIC name drift, you need to create an empty rules configuration file.

Example:

```
touch /etc/udev/rules.d/75-persistent-net-generator.rules //Replace 75 with the actual value in the environment.
```

3. Delete network rules.
  - If the OS uses the initrd system image, perform the following operations:
    - i. Run the following command to check whether the initrd image file whose name starts with **initrd** and ends with **default** contains the **persistent** and **net** network device rule files (replace the italic content in the following command with the actual OS version):

```
lsinitrd /boot/initrd-2.6.32.12-0.7-default |grep persistent|grep net
```

      - o If no, no further action is required.
      - o If yes, go to [3.ii](#).
    - ii. Run the following command to back up the initrd image files (replace the italic part in the following command with the actual OS version):

```
cp /boot/initrd-2.6.32.12-0.7-default /boot/initrd-2.6.32.12-0.7-default_bak
```
    - iii. Run the following command to generate the initrd file again:

```
mkinitrd
```
  - If the OS uses the initramfs system image (such as Ubuntu), perform the following operations:
    - i. Run the following command to check whether the initramfs image file whose name starts with **initrd** and ends with **generic** contains persistent and net rule files.

```
lsinitramfs /boot/initrd.img-3.19.0-25-generic|grep persistent|grep net
```

      - o If no, no further action is required.
      - o If yes, go to [3.ii](#).
    - ii. Run the following command to back up the initrd image files:

```
cp /boot/initrd.img-3.19.0-25-generic /boot/initrd.img-3.19.0-25-generic_bak
```

- iii. Run the following command to generate the initramfs image files again:

```
update-initramfs -u
```

## 5.3 Installing Cloud-Init

### Scenarios

To ensure that you can use the user data injection function to inject initial custom information into ECSs created from a private image (such as setting the ECS login password), install Cloud-Init on the ECS used to create the image.

- You need to download Cloud-Init from its official website. Therefore, you must bind an EIP to the ECS.
- If Cloud-Init is not installed, you cannot configure an ECS. As a result, you can only use the password in the image file to log in to the created ECSs.
- By default, ECSs created from a public image have Cloud-Init installed. You do not need to install or configure Cloud-Init on such ECSs.
- For ECSs created using an external image file, install and configure Cloud-Init by performing the operations in this section. For how to configure Cloud-Init, see [Configuring Cloud-Init](#).

#### NOTE

Cloud-Init is open-source software. If the installed version has security vulnerabilities, you are advised to upgrade it to the latest version.

### Prerequisites

- An EIP has been bound to the ECS.
- You have logged in to the ECS.
- The IP address obtaining mode of the ECS is DHCP.

### Procedure

1. Check whether Cloud-Init has been installed.  
For details, see [Check Whether Cloud-Init Has Been Installed](#).
2. Install Cloud-Init.  
You can install Cloud-Init in any of the following ways: [\(Recommended\) Install Cloud-Init Using the Official Installation Package](#), [Install Cloud-Init Using the Official Source Code Package and pip](#), and [Install Cloud-Init Using the Official GitHub Source Code](#).

### Check Whether Cloud-Init Has Been Installed

Perform the operations provided here to check whether Cloud-Init has been installed. The methods of checking whether Cloud-Init is installed vary depending on the OSs.

- If you are in a Python 3 environment, run the following command to check whether Cloud-Init is installed (Ubuntu 22.0.4 is used as an example):

**which cloud-init**

- If information similar to the following is displayed, Cloud-Init has been installed:

```
/usr/bin/cloud-init
```

- If information similar to the following is displayed, Cloud-Init is not installed:

```
/usr/bin/which: no cloud-init in (/usr/local/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin)
```

- If you are in a Python 2 environment, run the following command to check whether Cloud-Init is installed (CentOS 6 is used as an example):

**which cloud-init**

- If information similar to the following is displayed, Cloud-Init has been installed:

```
cloud-init-0.7.5-10.el6.centos.2.x86_64
```

- If no information is returned, Cloud-Init is not installed.

 **NOTE**

To confirm Cloud-Init is really not installed, you are advised to run **rpm -qa |grep cloud-init** to check again. If either of **which cloud-init** and **rpm -qa |grep cloud-init** shows that Cloud-Init has been installed, Cloud-Init is installed.

If Cloud-Init has been installed, perform the following operations:

- Check whether to use the SSH certificate in the ECS OS. If the certificate is no longer used, delete it.
  - If the certificate is stored in a directory of user **root**, for example, `/$path/$to/$root/.ssh/authorized_keys`, run the following commands:  
**cd /root/.ssh**  
**rm authorized\_keys**
  - If the certificate is not stored in a directory of user **root**, for example, `/$path/$to/$none-root/.ssh/authorized_keys`, run the following commands:  
**cd /home/centos/.ssh**  
**rm authorized\_keys**
- Run the following command to delete the cache generated by Cloud-Init and ensure that the ECS created from the private image can be logged in by using the certificate:  
**sudo rm -rf /var/lib/cloud/\***

 **NOTE**

Do not restart the ECS after performing the configuration. Otherwise, you need to configure it again.

## (Recommended) Install Cloud-Init Using the Official Installation Package

The method of installing Cloud-Init on an ECS varies depending on the OS. Perform the installation operations as user **root**.

The following describes how to install Cloud-Init on an ECS running SUSE Linux, CentOS, Fedora, Debian, and Ubuntu. For other OS types, install the required type of Cloud-Init. For example, you need to install `coreos-cloudinit` on ECSs running CoreOS.



- SUSE Linux

Paths for obtaining the Cloud-Init installation package for SUSE Linux

<https://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/>

<http://download.opensuse.org/repositories/Cloud:/Tools/>

 NOTE

Select the required repo installation package in the provided paths.

Take SUSE Enterprise Linux Server 12 as an example. Perform the following steps to install Cloud-Init:

- a. Log in to the ECS used to create a Linux private image.
- b. Run the following command to install the network installation source for SUSE Enterprise Linux Server 12:

```
zypper ar https://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/SLE_12_SP3/Cloud:Tools.repo
```

- c. Run the following command to update the network installation source:

```
zypper refresh
```

- d. Run the following command to install Cloud-Init:

```
zypper install cloud-init
```

- e. Run the following commands to enable Cloud-Init to automatically start upon system boot:

- SUSE 11

```
chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config on; chkconfig cloud-final on
```

```
service cloud-init-local status; service cloud-init status; service cloud-config status; service cloud-final status
```

- SUSE 12 and openSUSE 12/13/42

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

---

 CAUTION

For SUSE and openSUSE, perform the following steps to disable dynamic change of the ECS name:

1. Run the following command to open the **dhcp** file using the vi editor:

```
vi etc/sysconfig/network/dhcp
```

2. Change the value of **DHCLIENT\_SET\_HOSTNAME** in the **dhcp** file to **no**.

---

- CentOS

**Table 5-1** lists the Cloud-Init installation paths for CentOS. Select the required installation package from the following addresses.

**Table 5-1** Cloud-Init installation package addresses

| OS Type | Version  | How to Obtain                                                                                                                                                   |
|---------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CentOS  | 6 32-bit | <a href="https://archives.fedoraproject.org/pub/archive/epel/6/i386/">https://archives.fedoraproject.org/pub/archive/epel/6/i386/</a>                           |
|         | 6 64-bit | <a href="https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/">https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/</a>                       |
|         | 7 64-bit | <a href="https://archives.fedoraproject.org/pub/archive/epel/7/x86_64/Packages/e/">https://archives.fedoraproject.org/pub/archive/epel/7/x86_64/Packages/e/</a> |

- a. Run the following commands to install Cloud-Init:

```
yum install Cloud-Init installation package address/epel-release-x-y.noarch.rpm
```

```
yum install cloud-init
```

 **NOTE**

*Cloud-Init installation package address* indicates the address of the Cloud-Init epel-release installation package, and *x-y* indicates the version of the Cloud-Init epel-release required by the current OS. Replace them with the actual values according to [Table 5-1](#).

- Take CentOS 6 64-bit as an example. If the version is 6.8, the command is as follows:  

```
yum install https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/epel-release-6-8.noarch.rpm
```
- Take CentOS 7 64-bit as an example. If the version is 7.14, the command is as follows:  

```
yum install https://archives.fedoraproject.org/pub/archive/epel/7/x86_64/Packages/e/epel-release-7-14.noarch.rpm
```

- b. Run the following commands to enable Cloud-Init to automatically start upon system boot:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

- Fedora

Before installing Cloud-Init, ensure that the network installation source address has been configured for the OS by checking whether the `/etc/yum.repo.d/fedora.repo` file contains the installation source address of the software package. If the file does not contain the address, configure the address by following the instructions on the Fedora official website.

- a. Run the following command to install Cloud-Init:

```
yum install cloud-init
```

- b. Run the following commands to enable Cloud-Init to automatically start upon system boot:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

- Debian and Ubuntu

Before installing Cloud-Init, ensure that the network installation source address has been configured for the OS by checking whether the `/etc/apt/sources.list` file contains the installation source address of the software package. If the file does not contain the address, configure the address by following the instructions on the Debian or Ubuntu official website.

- a. Run the following commands to install Cloud-Init:

```
apt-get update
```

```
apt-get install cloud-init
```

- b. Run the following commands to enable Cloud-Init to automatically start upon system boot:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

Cloud-Init-23.2.2 is used as an example to describe how to install Cloud-Init on CentOS, Fedora, Ubuntu, Debian, and SUSE.

Download the `cloud-init-23.2.2.tar.gz` source code package from <https://launchpad.net/cloud-init/trunk/23.2.2/+download/cloud-init-23.2.2.tar.gz>.

- Centos 7/Fedora Server 36

---

#### NOTICE

Ensure that Python 3 has been installed.

- a. Check whether Cloud-Init has been installed. If any command output is displayed, Cloud-Init has been installed.

```
cloud-init -v
```

- b. Delete the cache directory of Cloud-Init.

```
rm -rf /var/lib/cloud/*
```

- c. Install dependency packages of Cloud-Init.

```
yum install python3-pip -y
yum install python3-devel
```

- d. Download the Cloud-Init package.

```
wget https://launchpad.net/cloud-init/trunk/23.2.2/+download/cloud-init-23.2.2.tar.gz
```

- e. Decompress the Cloud-Init package.

```
tar -zxvf cloud-init-23.2.2.tar.gz
```

- f. Go to the `cloud-init-23.2.2` directory and install dependent libraries:

```
cd cloud-init-23.2.2
pip3 install -r requirements.txt
```

- g. Install Cloud-Init.

```
python3 setup.py build
python3 setup.py install --init-system systemd
```

- h. (Optional) Disable Cloud-Init's network configuration capability by modifying the `/etc/cloud/cloud.cfg` file.

```
vi /etc/cloud/cloud.cfg
```

Add the following content to the file:

```
network:
 config: disabled
```

- i. Restart Cloud-Init and check its status.  

```
systemctl restart cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

```
Searching for six==1.16.0
Best match: six 1.16.0
Adding six 1.16.0 to easy-install.pth file

Using /usr/local/lib/python3.6/site-packages
Searching for typing-extensions==4.1.1
Best match: typing-extensions 4.1.1
Adding typing-extensions 4.1.1 to easy-install.pth file

Using /usr/local/lib/python3.6/site-packages
Searching for zipp==3.6.0
Best match: zipp 3.6.0
Adding zipp 3.6.0 to easy-install.pth file

Using /usr/local/lib/python3.6/site-packages
Finished processing dependencies for cloud-init==23.2.2
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]# cloud-init -v
/usr/local/bin/cloud-init 23.2.2
[root@localhost cloud-init-23.2.2]#
```

- j. Enable Cloud-Init related services to automatically start upon system boot.  

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```
- k. Check whether Cloud-Init is running properly.  

```
cloud-init -v
cloud-init init --local
```

```
Using /usr/local/lib/python3.6/site-packages
Finished processing dependencies for cloud-init==23.2.2
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]# cloud-init -v
/usr/local/bin/cloud-init 23.2.2
[root@localhost cloud-init-23.2.2]#
```

- **Ubuntu 22.0.4/Debian 11**

### NOTICE

Ensure that Python 3 has been installed.

- a. Check and delete redundant Cloud-Init configuration files.  

```
rm -rf /var/lib/cloud/*
rm -f /var/log/cloud-init*
```

Delete all files except log-related configuration files from the **/etc/cloud/cloud.cfg.d/** directory.
- b. Update your package list and check whether Wget is installed. If it is not, install it.  

```
sudo apt update
sudo apt install wget
```
- c. Install dependency packages.  

```
apt-get install cloud-guest-utils -y
apt-get install python3-pip -y
apt-get install python3-devel
```
- d. Download the Cloud-Init package.  

```
wget https://launchpad.net/cloud-init/trunk/23.2.2/+download/cloud-init-23.2.2.tar.gz
```
- e. Decompress the Cloud-Init package.  

```
tar -zxvf cloud-init-23.2.2.tar.gz
```
- f. Go to the **cloud-init** directory.  

```
cd cloud-init-23.2.2
```

- g. Install dependent libraries.  
`pip3 install -r requirements.txt`
- h. Install Cloud-Init.  
`python3 setup.py install`
- i. (Optional) Disable Cloud-Init's network configuration capability.  
You need to do so when the Cloud-Init version is 0.7.9 or later and you want to configure the network.

**NOTE**

1. Open the `/etc/cloud/cloud.cfg` file.

```
vi /etc/cloud/cloud.cfg
```

2. Enter `i` and configure **network**. (If there is no such a configuration item, add it.)

```
network:
 config: disabled
```

- j. Restart Cloud-Init and check its status.  
`systemctl restart cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service`  
`systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service`
- k. Enable Cloud-Init related services to automatically start upon system boot.  
`systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service`
- l. Check whether Cloud-Init is running properly.  
`cloud-init -v`  
`cloud-init init --local`

- **SUSE Enterprise Linux Server 15**

**NOTICE**

Ensure that Python 3 has been installed.

- a. View existing SUSE repositories.  
`zypper lr`
- b. Delete the SUSE repositories.  
`zypper rr No. of repositories listed in 1`
- c. Configure a SUSE repository.  
`zypper ar https://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/SLE\_15\_SP4/Cloud:Tools.repo`
- d. Refresh the SUSE repository.  
`zypper refresh`
- e. Install Cloud-Init.  
`zypper install cloud-init`
- f. Run `cloud-init -v`. If error messages similar to the following are displayed, install the dependency packages.

```
.bash_history .config .esd_auth .local .ssh .xauthxxyalg .xsession-errors-:0 bin
linux-1941:~ # cloud-init -v
Traceback (most recent call last):
 File "/usr/bin/cloud-init", line 5, in <module>
 from pkg_resources import load_entry_point
 File "/etc/zypp/repos.d/distribute-0.7.3/pkg_resources.py", line 2989, in <module>
 working_set.require(_requires_)
 File "/etc/zypp/repos.d/distribute-0.7.3/pkg_resources.py", line 726, in require
 needed = self.resolve(parse_requirements(requirements))
 File "/etc/zypp/repos.d/distribute-0.7.3/pkg_resources.py", line 624, in resolve
 raise DistributionNotFound(req)
pkg_resources.DistributionNotFound: requests
linux-1941:~ # ll /usr/bin/
```

```

100% | ██████████ | 1.3MB 60kB/s
Collecting wheel
 Downloading https://files.pythonhosted.org/packages/1b/d2/22cde5ea9af055f81814
 f9f2545f5ed8a053eb749c08d186b369959189a8/wheel-0.31.0-py2.py3-none-any.whl (41kB
)
100% | ██████████ | 51kB 65kB/s
cloud-init 18.1 requires configobj, which is not installed.
cloud-init 18.1 requires jinja2, which is not installed.
cloud-init 18.1 requires jsonpatch, which is not installed.
cloud-init 18.1 requires jsonschema, which is not installed.
cloud-init 18.1 requires oauthlib, which is not installed.
cloud-init 18.1 requires pyyaml, which is not installed.
cloud-init 18.1 requires requests, which is not installed.
Installing collected packages: pip, wheel
Successfully installed pip-10.0.1 wheel-0.31.0
linux-1941:~ # pip -V
pip 10.0.1 from /usr/lib/python2.7/site-packages/pip (python 2.7)
linux-1941:~ # █

```

```
pip install requests pyyaml oauthlib jsonschema jsonpatch jinja2 configobj
```

- g. Check whether Cloud-Init is successfully installed. If the following error message is displayed, configure `datasource_list` in `/etc/cloud/cloud.cfg`.

```

host-192-168-0-123:~ # cloud-init init --local
Cloud-init v. 23.1-150400.9.3 running 'init-local' at Sat, 19 Aug 2023 08:00:22 +0000. Up 3580.28 seconds.
2023-08-19 08:00:22.259 - util.py[WARNING]: Getting data from <class 'cloudinit.sources.DataSourceGCE.DataSourceGCELocal'> failed
2023-08-19 08:00:22.296 - DataSourceWare.py[ERROR]: failed to find a valid data access method
host-192-168-0-123:~ # █

```

```

datasource_list: [OpenStack]
datasource:
 OpenStack:
 metadata_urls: ['http://169.254.169.254']
 max_wait: 120
 timeout: 5
 apply_network_config: false

```

- h. Modify the configuration file, restart Cloud-Init, and check the Cloud-Init status.
- ```
systemctl restart cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```
- ```
systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

- i. Enable Cloud-Init related services to automatically start upon system boot.

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

```

Aug 19 16:25:04 ecs-suse-cloud cloud-init[1543]: Cloud-init v. 23.1-150400.9.3 running 'modules:config' at Sat, 19 Aug 2023 08:25:04 +0000. Up 26.03 seconds.
Aug 19 16:25:04 ecs-suse-cloud systemd[1]: Finished Apply the settings specified in cloud-config.
● cloud-final.service - Execute cloud user/final scripts
 Loaded: loaded (/usr/lib/systemd/system/cloud-final.service; enabled; vendor preset: disabled)
 Active: active (exited) since Sat 2023-08-19 16:25:05 CST; 55s ago
 Process: 1544 ExecStart=/usr/bin/cloud-init modules --mode=final (code=exited, status=0/SUCCESS)
 Main PID: 1544
 -- Home --
ecs-suse-cloud:~ # cd /home/
ecs-suse-cloud:~ # ls
ecs-suse-cloud:~ # ls -l
-rw-r--r-- 1 user user 0 Aug 19 16:25 socket-tool user.txt
ecs-suse-cloud:~ #
ecs-suse-cloud:~ #
ecs-suse-cloud:~ #

```

- j. Check whether Cloud-Init is running properly.

```
cloud-init -v
cloud-init init --local
```

## Install Cloud-Init Using the Official Source Code Package and pip

The following operations use Cloud-Init 0.7.9 as an example to describe how to install Cloud-Init.

1. Download the **cloud-init-0.7.9.tar.gz** source code package (version 0.7.9 is recommended) and upload it to the `/home/` directory of the ECS.

Download **cloud-init-0.7.9.tar.gz** from the following path:

<https://launchpad.net/cloud-init/trunk/0.7.9/+download/cloud-init-0.7.9.tar.gz>

2. Create a **pip.conf** file in the **~/pip/** directory and edit the following content:

 **NOTE**

If the **~/pip/** directory does not exist, run the **mkdir ~/pip** command to create it.

```
[global]
index-url = https://<$mirror>/simple/
trusted-host = <$mirror>
```

 **NOTE**

Replace **<\$mirror>** with a public network PyPI source.

Public network PyPI source: <https://pypi.python.org/>

3. Run the following command to install the downloaded Cloud-Init source code package (select **--upgrade** as needed during installation):

```
pip install [--upgrade] /home/cloud-init-0.7.9.tar.gz
```

 **NOTE**

For details about how to install a Cloud-Init source code package, see [Cloud-Init Documentation](#)

4. Run the **cloud-init -v** command. Cloud-Init is installed successfully if the following information is displayed:

```
cloud-init 0.7.9
```

5. Enable Cloud-Init to automatically start upon system boot.

- If the OS uses SysVinit to manage automatic start of services, run the following commands:

```
chkconfig --add cloud-init-local; chkconfig --add cloud-init; chkconfig --add cloud-config; chkconfig --add cloud-final
```

```
chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config on; chkconfig cloud-final on
```

```
service cloud-init-local status; service cloud-init status; service cloud-config status; service cloud-final status
```

- If the OS uses Systemd to manage automatic start of services, run the following commands:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

**CAUTION**

If you install Cloud-Init using the official source code package and pip, pay attention to the following:

1. Add user **syslog** to the **adm** group during the installation. If user **syslog** exists, add it to the **adm** group. For some OSs (such as CentOS and SUSE), user **syslog** may not exist. Run the following commands to create user **syslog** and add it to the **adm** group:

```
useradd syslog
groupadd adm
usermod -g adm syslog
```

2. Change the value of **distro** in **system\_info** in the **/etc/cloud/cloud.cfg** file based on the OS release version, such as **distro: ubuntu**, **distro: sles**, **distro: debian**, and **distro: fedora**.

## Install Cloud-Init Using the Official GitHub Source Code

You can obtain the Cloud-Init source code from GitHub at <https://github.com/canonical/cloud-init/>

1. Run the following commands to download the source code package and copy it to the **/tmp/CLOUD-INIT** folder:

**NOTE**

Cloud-Init 0.7.6: <https://github.com/canonical/cloud-init/archive/refs/tags/0.7.6.zip>

Cloud-Init 0.7.9: <https://github.com/canonical/cloud-init/archive/refs/tags/0.7.9.zip>

All versions: <https://github.com/canonical/cloud-init/releases>

```
wget https://github.com/canonical/cloud-init/archive/refs/tags/0.7.6.zip
mkdir /tmp/CLOUD-INIT
cp cloud-init-0.7.6.zip /tmp/CLOUD-INIT
cd /tmp/CLOUD-INIT
```

2. Run the following command to decompress the package:

```
unzip cloud-init-0.7.6.zip
```

3. Run the following command to enter the **cloud-init-0.7.6** folder:

```
cd cloud-init-0.7.6
```

4. (Optional) If the Cloud-Init version is 18.3 to 22.3, run the following commands:

```
sed -i '/VALID_DMI_ASSET_TAGS =/a\VALID_DMI_ASSET_TAGS += ["HUAWEICLOUD"]' cloudinit/sources/DataSourceOpenStack.py
cat cloudinit/sources/DataSourceOpenStack.py | grep VALID_DMI_ASSET_TAGS
```

If the following information is displayed, the execution is successful.

```
root@ecs-cc9e cloud-init]# cat cloudinit/sources/DataSourceOpenStack.py | grep VALID_DMI_ASSET_TAGS
VALID_DMI_ASSET_TAGS = VALID_DMI_PRODUCT_NAMES
VALID_DMI_ASSET_TAGS += ["HUAWEICLOUD"]
VALID_DMI_ASSET_TAGS += [DMI_ASSET_TAG_OPENTELEKOM, DMI_ASSET_TAG_SAPCCLOUD]
 elif dmi.read_dmi_data("chassis-asset-tag") in VALID_DMI_ASSET_TAGS:
root@ecs-cc9e cloud-init]#
```



5. Install Cloud-Init. The commands vary depending on the OS type.
  - For CentOS 6.x or SUSE 11.x, run the following commands:  
**python setup.py build**  
**python setup.py install --init-system sysvinit**
  - For CentOS 7.x or SUSE 12.x, run the following commands:  
**python setup.py build**  
**python setup.py install --init-system systemd**

 NOTE

Add user **syslog** to the **adm** group during the installation. If user **syslog** exists, add it to the **adm** group. For some OSs (such as CentOS and SUSE), user **syslog** may not exist. Run the following commands to create user **syslog** and add it to the **adm** group:

```
useradd syslog
groupadd adm
usermod -g adm syslog
```

6. Enable Cloud-Init to automatically start upon system boot.
  - If the OS uses SysVinit to manage automatic start of services, run the following commands:  
**chkconfig --add cloud-init-local; chkconfig --add cloud-init; chkconfig --add cloud-config; chkconfig --add cloud-final**  
**chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config on; chkconfig cloud-final on**  
**service cloud-init-local status; service cloud-init status; service cloud-config status; service cloud-final status**
  - If the OS uses Systemd to manage automatic start of services, run the following commands:  
**systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service**  
**systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service**
7. Run the following commands to check whether Cloud-Init has been installed:  
**cloud-init -v**  
**cloud-init init --local**

Cloud-Init is successfully installed if the following information is displayed:

```
cloud-init 0.7.6
```

## 5.4 Configuring Cloud-Init

### Scenarios

You need to configure Cloud-Init after it is installed.

### Prerequisites

- Cloud-Init has been installed.

- An EIP has been bound to the ECS.
- You have logged in to the ECS.
- The ECS obtains its IP address using DHCP.

## Procedure

The following operations are required:

1. Configure Cloud-Init.  
For details, see [Configure Cloud-Init](#).
2. Check whether Cloud-Init is successfully configured.  
For details, see [Check the Cloud-Init Configuration](#).

## Configure Cloud-Init

1. Configure the user permissions for logging in to the ECS. If you select user **root**, enable the SSH permissions of user **root** and enable remote login to the ECS using a password.
  - If you inject a password, use it to log in to the ECS remotely using SSH or noVNC.
  - If you inject a key, use it to log in to the ECS remotely using SSH.
2. Enable remote login using the password of user **root** and enable the SSH permissions of user **root**.

Take CentOS 6.7 as an example. If the value of **disable\_root** in the **/etc/cloud/cloud.cfg** file is **0**, the permissions are enabled. (In some OSs, value **true** indicates that the permissions are disabled, and **false** indicates that the permissions are enabled). Set **ssh\_pwauth** to **1**, and **lock\_passwd** to **False** (indicating that user passwords are not locked).

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

disable_root: 0
ssh_pwauth: 1
```

3. Prevent Cloud-Init from taking over the network in **/etc/cloud/cloud.cfg**.  
If the Cloud-Init version is 0.7.9 or later, add the following content to **/etc/cloud/cloud.cfg**:

**Figure 5-1** Preventing Cloud-Init from taking over the network

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

disable_root: 0
ssh_pwauth: 1

datasource_list: ['OpenStack']

network:
 config: disabled
```

**NOTE**

The added content must be in the YAML format.

4. Enable the agent to access the IaaS OpenStack data source.

Add the following information to the last line of `/etc/cloud/cloud.cfg`:

```
datasource_list: [OpenStack]
datasource:
 OpenStack:
 metadata_urls: ['http://169.254.169.254']
 max_wait: 120
 timeout: 5
 apply_network_config: false
```

**NOTE**

- You can decide whether to set **max\_wait** and **timeout**. The values of **max\_wait** and **timeout** in the preceding command output are only for reference.
  - If the OS version is earlier than Debian 8 or CentOS 5, you cannot enable the agent to access the IaaS OpenStack data source.
  - The default zeroconf route must be disabled for CentOS and EulerOS ECSs for accurate access to the IaaS OpenStack data source.  
**echo "NOZEROCONF=yes" >> /etc/sysconfig/network**
  - **apply\_network\_config: false** is only required by users who use Cloud-Init 18.3 or later.
5. Add the following content to `/etc/cloud/cloud.cfg`:

**manage\_etc\_hosts: localhost**

This prevents the system from staying in the **Waiting for cloudResetPwdAgent** state for a long time during ECS startup.

Figure 5-2 Adding `manage_etc_hosts: localhost`

```
datasource_list: ['OpenStack']
manage_etc_hosts: localhost

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

6. Run the `vi /etc/ssh/sshd_config` command to open the `/etc/ssh/sshd_config` file using the vi editor.

Change the value of **PasswordAuthentication** in the `sshd_config` file to **yes**.

**NOTE**

For SUSE and openSUSE, change the values of the following parameters in the `sshd_config` file to **yes**:

- PasswordAuthentication
  - ChallengeResponseAuthentication
7. Modify **cloud\_init\_modules** in the `cloud.cfg` configuration file.
    - Move **ssh** from the bottom to the top to speed up the SSH login.

- Enable the hostname update. Do not comment out or delete the - **update\_hostname** statement.

```
cloud_init_modules:
```

```
- ssh
- migrator
- bootcmd
- write-files
- growpart
- resizefs
- set_hostname
- update_hostname
- update_etc_hosts
- rsyslog
- users-groups
```

8. Modify the configuration so that the hostname of the ECS created from the image does not contain the **.novalocal** suffix and can contain a dot (.).

- a. Run the following command to modify the **\_\_init\_\_.py** file:

```
vi /usr/lib/python*/site-packages/cloudinit/sources/__init__.py
```

The Python version varies depending on the OS.

Press **i** to enter editing mode. Modify the file content as follows based on the keyword **toks**:

```
if toks:
 toks = str(toks).split('.')
else:
 #toks = ["ip-%s" % lhost.replace(".", "-")] # Comment out this line.
 toks = lhost.split(".novalocal") # Add this line.

if len(toks) > 1:
 hostname = toks[0]
 #domain = ''.join(toks[1:]) # Comment out this line.
else:
 hostname = toks[0]

if fqdn and domain != defdomain:
 #return hostname # Comment out this line.
 return "%s.%s" % (hostname, domain) # Add this line.
else:
 return hostname
```

After the modification is complete, press **Esc** to exit the editing mode and enter **:wq!** to save the settings and exit.

- b. Run the following command to switch to the **cloudinit/sources** folder:

```
cd /usr/lib/python*/site-packages/cloudinit/sources/
```

The Python version varies depending on the OS.

- c. Run the following commands to delete the **\_\_init\_\_.pyc** file and the optimized **\_\_init\_\_.pyo** file:

```
rm -rf __init__.pyc
```

```
rm -rf __init__.pyo
```

- d. Run the following commands to clear the logs:

```
rm -rf /var/lib/cloud/*
```

```
rm -rf /var/log/cloud-init*
```

9. Run the following command to edit the **/etc/cloud/cloud.cfg.d/05\_logging.cfg** file to use cloudLogHandler to process logs:

```
vim /etc/cloud/cloud.cfg.d/05_logging.cfg
```

```
[logger_cloudinit]
level=DEBUG
```

```
qualname=cloudinit
handlers=cloudLogHandler
propagate=1
```

10. Delete user **linux** and the **/home/linux** directory from the image template.

```
userdel linux
```

```
rm -fr /home/linux
```

## Check the Cloud-Init Configuration

Run the following command to check whether Cloud-Init has been properly configured:

```
cloud-init init --local
```

If Cloud-Init has been properly installed, the version information is displayed and no error occurs. For example, messages indicating lack of files will not be displayed.

### NOTE

(Optional) Run the following command to set the password validity period to the maximum:

```
chage -M 99999 $user_name
```

*user\_name* is a system user, such as user **root**.

You are advised to set the password validity period to **99999**.

## 5.5 Detaching Data Disks from an ECS

### Scenarios

If multiple data disks are attached to the ECS used to create a private image, ECSs created from the image may be unavailable. Therefore, you need to detach all data disks from the ECS before using it to create a private image.

This section describes how to detach all data disks from an ECS.

### Prerequisites

You have logged in to the ECS used to create a Linux private image.

### Procedure

1. Check whether the ECS has data disks.

Run the following command to check the number of disks attached to the ECS:

```
fdisk -l
```

- If the number is greater than 1, the ECS has data disks. Go to **2**.
- If the number is equal to 1, no data disk is attached to the ECS. Go to **3**.

2. Run the following command to check the data disks attached to the ECS:

```
mount
```

- If the command output does not contain any EVS disk information, no EVS data disks need to be detached.  
`/dev/vda1 on / type ext4 (rw,relatime,data=ordered)`
  - If information similar to the following is displayed, go to **3**:  
`/dev/vda1 on / type ext4 (rw,relatime,data=ordered)`  
`/dev/vdb1 on /mnt/test type ext4 (rw,relatime,data=ordered)`
3. Delete the configuration information in the **fstab** file.
    - a. Run the following command to edit the **fstab** file:  
**vi /etc/fstab**
    - b. Delete the disk configuration from the **fstab** file.

The **/etc/fstab** file contains information about the file systems and storage devices automatically attached to the ECS when the ECS starts. The configuration about data disks automatically attached to the ECS needs to be deleted, for example, the last line shown in the following figure.

**Figure 5-3** EVS disk configuration in the **fstab** file

```
[root@ecs-bf78 ~]# cat /etc/fstab
#
/etc/fstab
Created by anaconda on Wed Feb 27 06:58:16 2019
#
Accessible filesystems, by reference, are maintained under '/dev/disk'
See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=4c2c090d-4228-49fc-9cbe-3920b3bf287c / ext4 defaults 1 1
UUID=9c29104b-31b8-4421-a207-102f86ec7ae5 /mnt/test ext4 defaults 1 1
```

4. Run the following command to detach data disks from the ECS:  
Run the following command to detach the disks:  
**umount /dev/vdb1**
5. Run the following command to check the data disks attached to the ECS:  
**mount**  
If the command output contains no information about the data disks, they have been detached from the ECS.

# 6 Permissions Management

---

## 6.1 Creating a User and Granting Permissions

### Scenarios

This section describes how to use [Identity and Access Management](#) (IAM) to implement fine-grained permissions control over your images. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own identity credentials for accessing images.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or cloud service to perform professional and efficient O&M on your images.

If your account does not need individual IAM users for permissions management, you can skip this section.

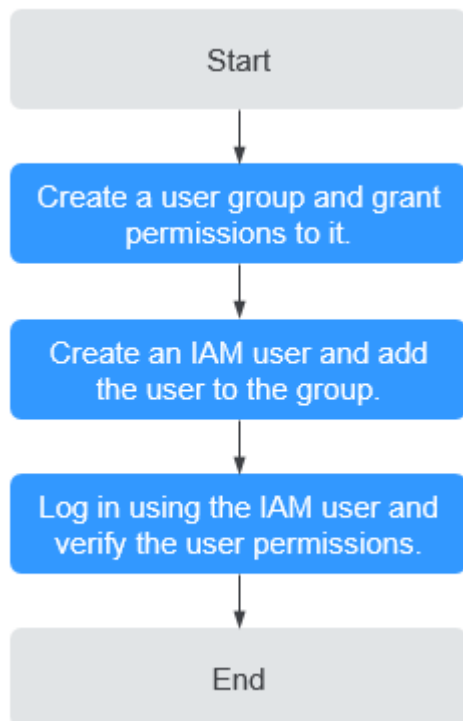
This section uses the **IMS ReadOnlyAccess** permission as an example to describe how to grant permissions to a user. [Figure 6-1](#) shows the process.

### Prerequisites

Learn about the permissions (see [IMS Permissions](#)) supported by IMS. For the system permissions of other services, see [System Permissions](#).

## Process Flow

Figure 6-1 Process for granting IMS permissions



1. **Create a user group and grant permissions to it.**

Create a user group on the IAM console, and grant the read-only permission to the group by assigning the **IMS ReadOnlyAccess** permission.

2. **Create an IAM user and add it to the user group.**

Create a user on the IAM console and add the user to the group created in 1.

3. **Log in** and verify permissions.

Log in to the management console using the IAM user, switch to a region where the permissions take effect, and verify the permissions (assume that the user has only the **IMS ReadOnlyAccess** permission).

- In the **Service List**, choose **Image Management Service**. On the IMS console, perform operations except querying images, such as creating, modifying, and deleting an image.

For example, click **Create Private Image** in the upper right corner. If you are prompted insufficient permissions, the **IMS ReadOnlyAccess** permission has taken effect.

- Choose any other service in the **Service List**, such as **Virtual Private Cloud**. If a message appears indicating insufficient permissions to access the service, the **IMS ReadOnlyAccess** permission has taken effect.



## 6.2 Creating a Custom Policy

### Scenarios

Custom policies can be created as a supplement to the system policies of IMS. For the actions supported by custom policies, see [Permission Policies and Supported Actions](#).

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see [Creating a Custom Policy](#). This section provides examples of common IMS custom policies.

### Example Policies

- Example 1: Allowing users to create images

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ims:serverImages:create"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "KMS:*:*"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "ecs:cloudServers:get",
 "ecs:servers:get",
 "ecs:serverVolumes:use",
 "ecs:cloudServers:list",
 "ecs:serverVolumeAttachments:list",
 "ecs:servers:list"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "bms:servers:list",
 "bms:servers:get",
 "bms:serverFlavors:get"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "evs:volumes:*"
]
 }
]
}
```

```
}
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "OBS:*:*"
]
 }
]
}
```

**NOTE**

The action required for creating an image is **ims:serverImages:create**. Others are dependent actions for creating an image.

- Example 2: Denying image deletion

A deny policy must be used in conjunction with other policies to take effect. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

The following method can be used if you need to assign the **IMS FullAccess** policy to a user but also forbid the user from deleting images. Create a custom policy for denying image deletion, and assign both the policies to the group the user belongs to. Then, the user can perform all operations on IMS except deleting images. The following is an example deny policy:

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": [
 "ims:images:delete"
]
 }
]
}
```