

# Image Management Service

## Best Practices

**Issue** 01  
**Date** 2025-05-08



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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 Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property 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 Cloud 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.

# Contents

<b>1 Overview.....</b>	<b>1</b>
<b>2 Creating a Windows Image Using VirtualBox and an ISO File.....</b>	<b>3</b>
2.1 Introduction.....	3
2.2 Installing VirtualBox.....	5
2.3 Creating a VM and Installing an OS.....	8
2.4 Configuring the VM.....	16
2.5 Obtaining the Image File.....	22
2.6 Registering the Image File as a Private Image.....	23
<b>3 Creating a Linux Image Using VirtualBox and an ISO File.....</b>	<b>24</b>
3.1 Introduction.....	24
3.2 Installing VirtualBox.....	26
3.3 Creating a VM and Installing an OS.....	29
3.4 Configuring the VM.....	42
3.5 Obtaining the Image File.....	58
3.6 Registering the Image File as a Private Image.....	58
<b>4 Creating a Private Image Using Packer.....</b>	<b>60</b>
<b>5 Cleaning Up the Disk Space of a Windows ECS.....</b>	<b>66</b>
<b>6 Converting the Image Format.....</b>	<b>77</b>
6.1 Converting the Image Format Using qemu-img.....	77
6.2 Converting the Image Format Using qemu-img-hw.....	82
<b>7 Configuring an ISO File as a Local Image Source.....</b>	<b>86</b>
<b>8 Migrating ECSs Across Accounts and Regions.....</b>	<b>90</b>
<b>9 Creating a Data Disk Image to Migrate Service Data Across Accounts.....</b>	<b>98</b>
<b>10 IMS Security.....</b>	<b>104</b>

# 1 Overview

Common IMS practices are provided to help you use IMS easily.

**Table 1-1** IMS practices

Practice	Description
<a href="#">Creating a Windows Image Using VirtualBox and an ISO File</a>	Describes how to create a Windows image using VirtualBox. To do so, you need to install VirtualBox, use it to create a VM from an ISO file, configure the VM, and generate a VHD image using the configured VM.
<a href="#">Creating a Linux Image Using VirtualBox and an ISO File</a>	Describes how to create a Linux image using VirtualBox. To do so, you need to install VirtualBox, use it to create a VM from an ISO file, configure the VM, and generate a VHD image using the configured VM.
<a href="#">Creating a Private Image Using Packer</a>	Describes how to create an Ubuntu 22.04 Server 64-bit private image from a CentOS 8.2 ECS using Packer and upload it to the cloud platform.
<a href="#">Cleaning Up the Disk Space of a Windows ECS</a>	Describes how to clean up the disk space of a Windows ECS.
<a href="#">Converting the Image Format</a>	Describes how to use qemu-img or Huawei qemu-img-hw to convert the image format. qemu-img can be used for mutual conversion of formats VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, and QED but cannot be used for the format conversion to ZVHD or ZVHD2. To convert an image file to any of the two formats, use qemu-img-hw.

Practice	Description
<a href="#">Configuring an ISO File as a Local Image Source</a>	Describes how to configure a local image source by using the yum, apt, and zypper package managers and provides configuration examples of Debian 10.1.0 and CentOS 8.0.
<a href="#">Migrating ECSs Across Accounts and Regions</a>	Describes how to migrate an ECS with a website deployed across regions and accounts.
<a href="#">Creating a Data Disk Image to Migrate Service Data Across Accounts</a>	Generally, service data is stored on data disks. To migrate service data across accounts, you need to create data disk images and share them with the target account.

# 2 Creating a Windows Image Using VirtualBox and an ISO File

---

## 2.1 Introduction

### VirtualBox

VirtualBox is free, open-source virtualization software. It was first offered by InnoTek GmbH from Germany and re-branded as Oracle VM VirtualBox when InnoTek was acquired by Oracle Corporation.

For more information about VirtualBox, visit the Oracle official website. Click [here](#) to see the guest OSs that can work with VirtualBox.

### Scenarios

You can use a 32-bit or 64-bit Windows guest OS provided by VirtualBox to create an image file in VHD format.

### Advantages

You can customize Windows image files.

### Tools and Costs

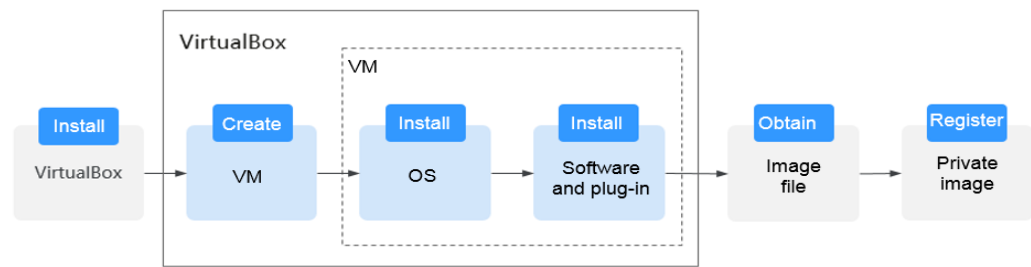
**Table 2-1** Tools and costs

Tool	Description	Costs
VirtualBox	VirtualBox is free, open-source virtualization software. Download it from: <a href="https://www.virtualbox.org/wiki/Downloads">https://www.virtualbox.org/wiki/Downloads</a>	Free

Tool	Description	Costs
VirtIO drivers	Before using an ECS or image file to create a private image, ensure that VirtIO drivers have been installed in the OS so that new ECSs created from this image can support KVM virtualization and the network performance can be improved.  Download the driver package from: <a href="https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/">https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/</a>	Free
ISO image file	It is used to install an OS on an empty VM. You need to prepare it.  File name: Windows_server_2008_r2.iso	-
(Optional) Cloudbase-Init	To ensure that you can inject custom information (for example, the login password) into ECSs created from the image, you are advised to install Cloudbase-Init on the VM that is used as the image source. If you do not install it, you can log in to the ECSs only with the password specified in the image.  Download it from: <a href="http://www.cloudbase.it/cloud-init-for-windows-instances/">http://www.cloudbase.it/cloud-init-for-windows-instances/</a>	Free
(Optional) One-click password reset plug-in	To ensure that you can reset the password of each ECS created from the image with a few clicks, you are advised to install the one-click password reset plug-in (CloudResetPwdAgent) on the VM that is used as the image source.  <a href="https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip">https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip</a>	Free

## Image Creation Process

The following figure shows how to use VirtualBox to create an image from an ISO file.

**Figure 2-1** Image creation process

1. Install VirtualBox: Prepare a host (64-bit Windows is recommended) and install VirtualBox on the host. For details, see [Installing VirtualBox](#).
2. Create a VM: Use VirtualBox to create an empty VM from which an image will be created. For details, see [Creating an Empty VM](#).
3. Install an OS on the VM: Mount an ISO file to install an OS for the VM. The ISO file determines the OS of the image you want to create. For details, see [Installing Windows on the VM](#).
4. Install software and plug-ins on the VM: To ensure that ECSs created from this image can run properly, install the required software and plug-ins on the VM, including VirtIO drivers, Cloudbase-Init, and one-click password reset plug-in. For details, see [Configuring the VM](#).
5. Obtain the image file: Export an image file in VHD format from VirtualBox. For details, see [Obtaining the Image File](#).
6. Register a private image: Upload the exported VHD image file to an OBS bucket and register it as a private image. Then, you can use the private image to create ECSs. For details, see [Registering the Image File as a Private Image](#).

## 2.2 Installing VirtualBox

### Preparations

The host where VirtualBox is to be installed must meet the following requirements:

- A 64-bit Windows OS (recommended).
- At least 4 GB of memory and a dual-core processor. For example, the host specifications can be 8U16G.
- At least 20 GB of available disk space.
- CPU hardware virtualization (Intel VT-x or AMD-V) enabled. For how to enable it, see [Host CPU Settings \(Hardware Virtualization\)](#).

#### NOTE

For details about how to install VirtualBox, see the VirtualBox user guide at <https://www.virtualbox.org/manual/UserManual.html>.

## Host CPU Settings (Hardware Virtualization)

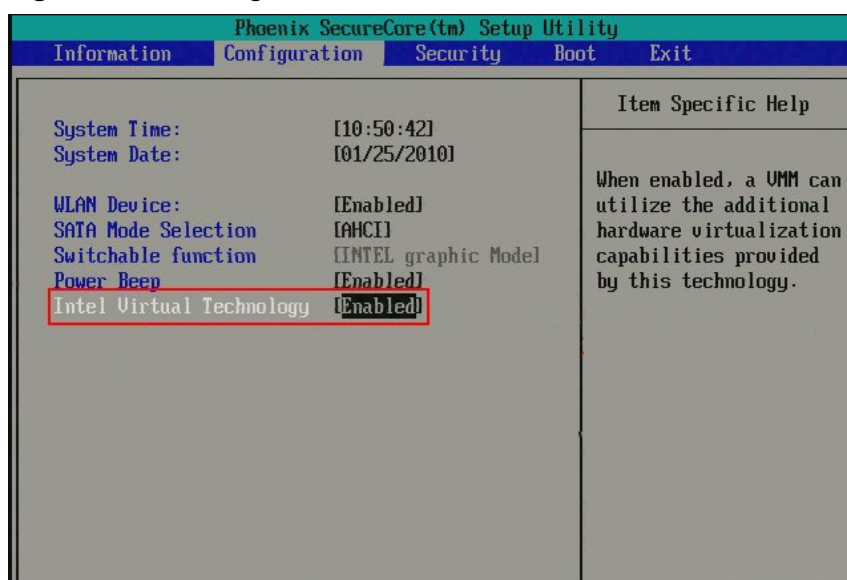
For an Intel host, perform the following operations to enable hardware virtualization:

### NOTE

The operations may differ depending on the CPU type. You can do it as prompted.

1. During the host startup, press the BIOS key set by the manufacturer to access the BIOS.
2. Choose **Configuration > Intel Virtual Technology**, and press **Enter**.
3. Select **Enabled** and press **Enter**. The value of **Intel Virtual Technology** will become **Enabled**.
4. Press **F10** to save the settings and exit.

**Figure 2-2** Enabling hardware virtualization



## Procedure

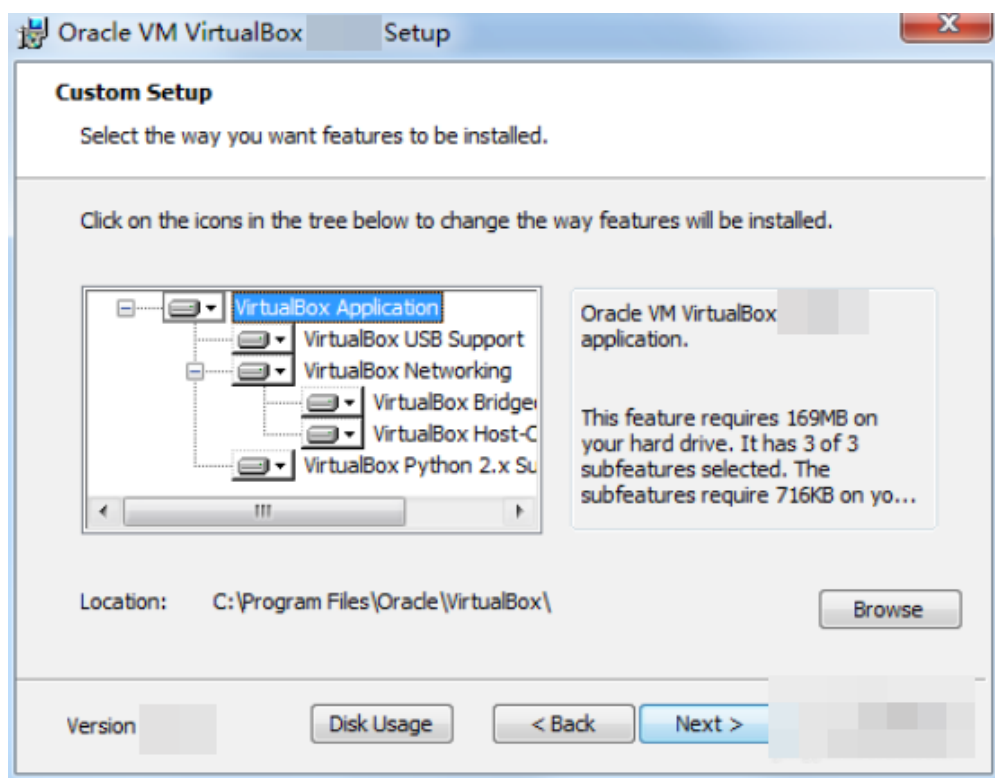
1. Download a VirtualBox package. VirtualBox-5.2.0 is used as an example. Download it from <https://www.virtualbox.org/wiki/Downloads>.
2. Decompress the package. Right-click **VirtualBox-5.2.0-118431-Win.exe**, choose **Run as administrator**, and click **Next**.

**Figure 2-3** Installing VirtualBox



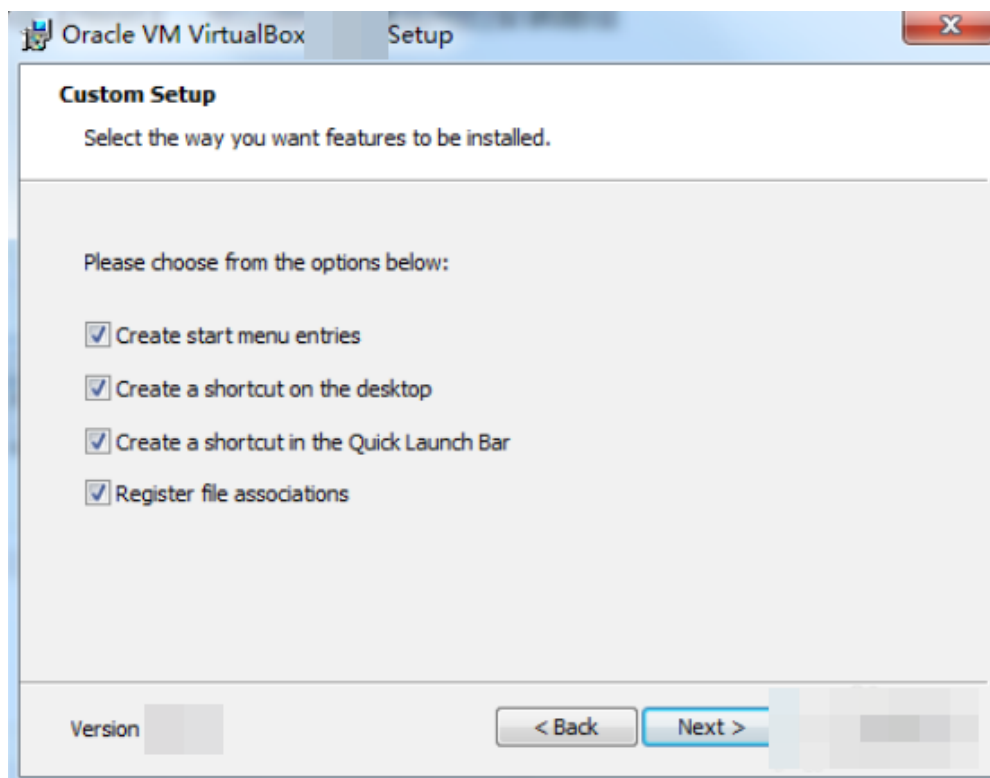
3. Select a VirtualBox installation path and click **Next**.

**Figure 2-4** Selecting an installation path



4. Personalize the settings and click **Next**.

**Figure 2-5** Personalized settings



5. Click **Finish**.

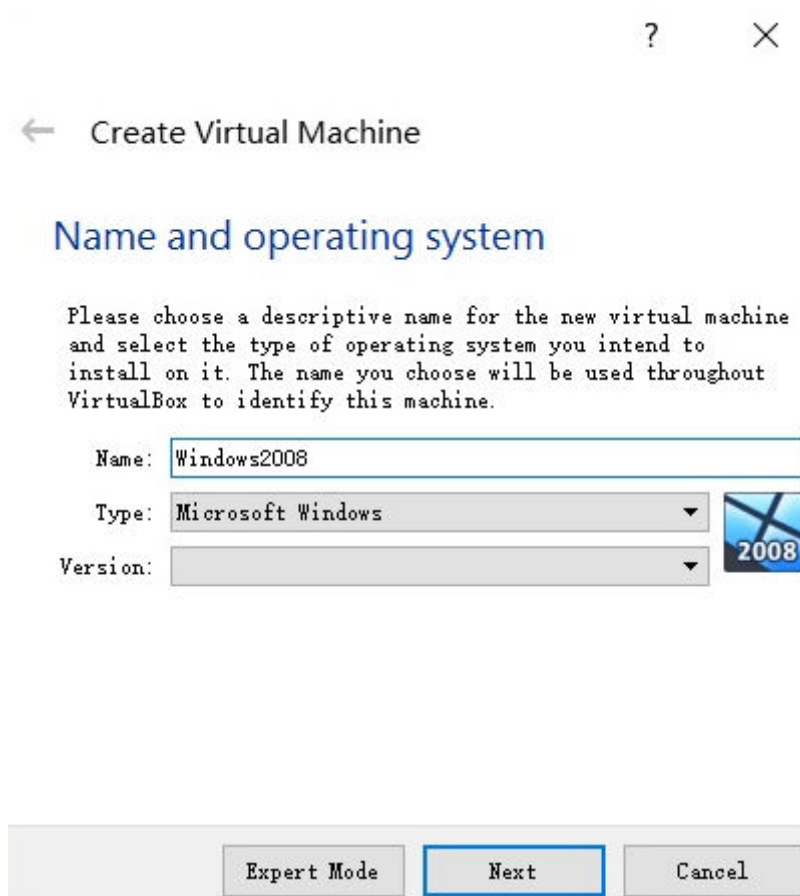
## 2.3 Creating a VM and Installing an OS

### Prerequisites

VirtualBox has been installed.

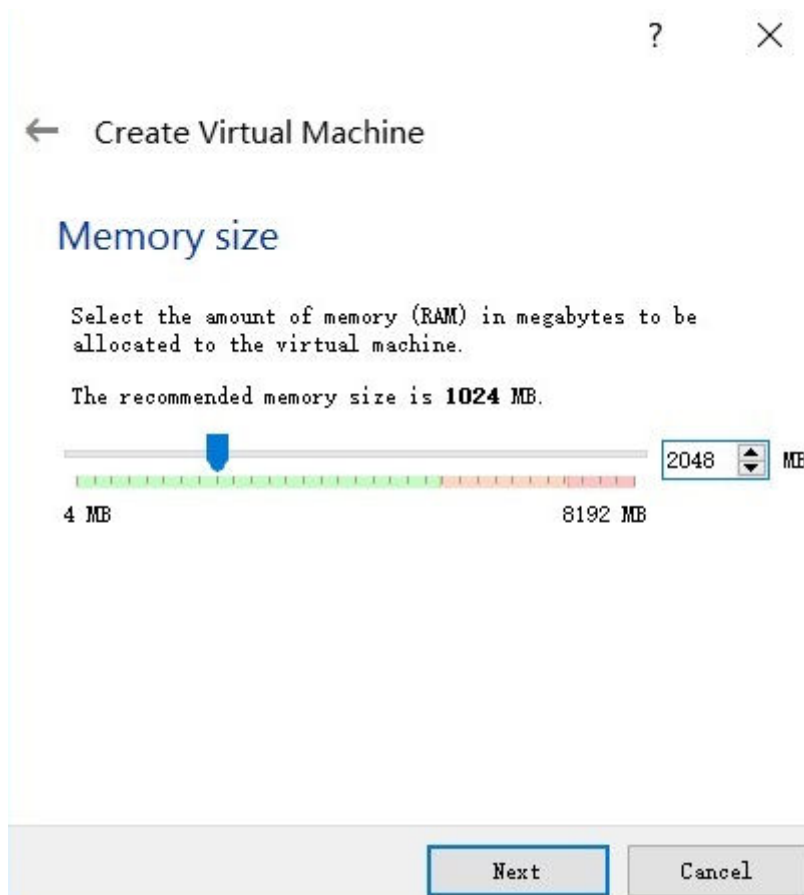
### Creating an Empty VM

1. Open VirtualBox and click **New**. In the displayed **Create Virtual Machine** dialog box, enter a VM name, select an OS type and version, and click **Next**. Take Windows 2008 64-bit as an example. The OS type must be **Microsoft Windows**.  
Ensure that the selected version is the same as that of the OS you want to install on the VM.

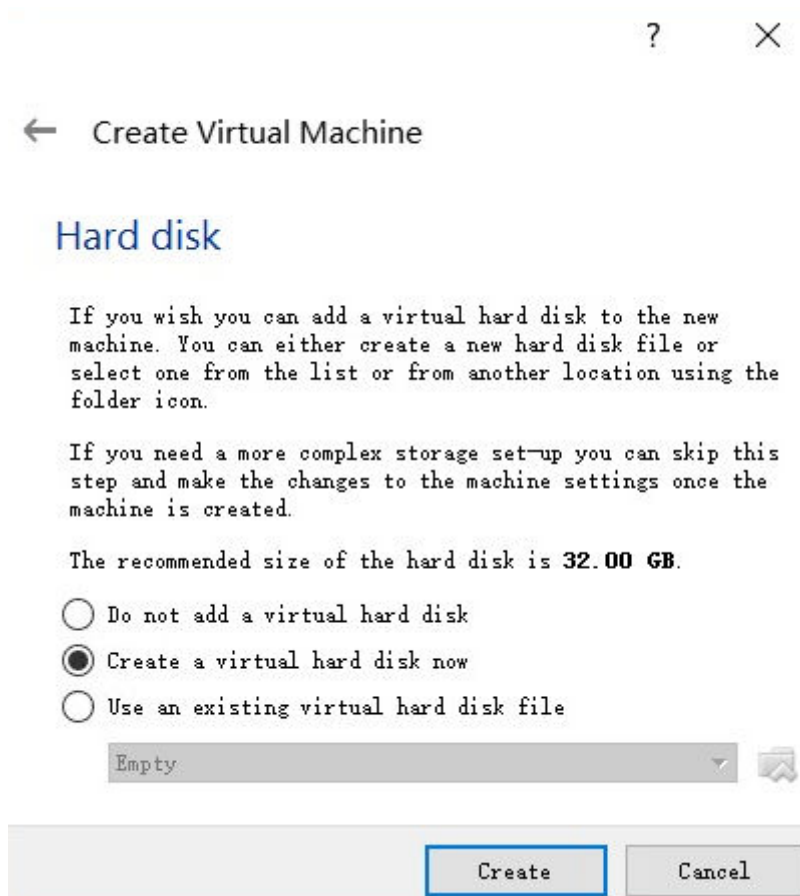
**Figure 2-6** Creating a VM

2. In the **Memory size** dialog box, set a value and click **Next**.  
You can reference the VM specifications or official OS requirements. For example, set the memory size to 2,048 MB.

Figure 2-7 Setting the memory size

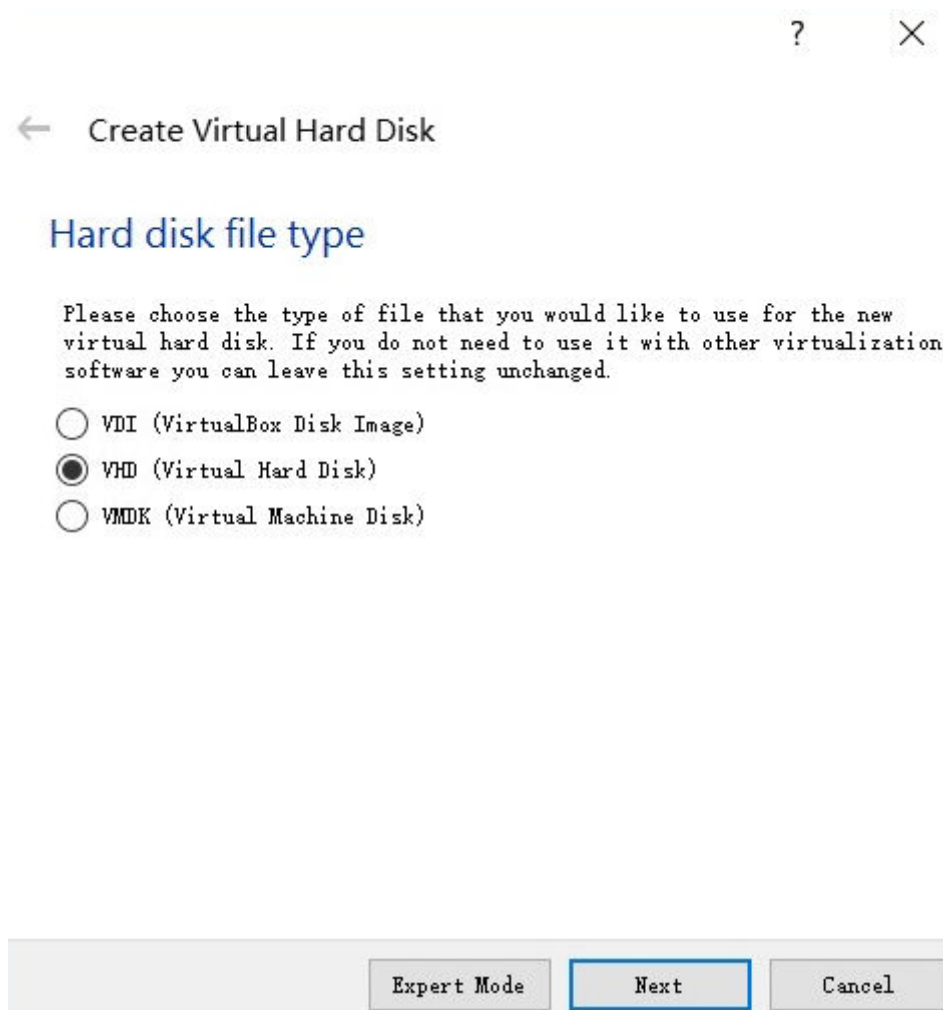


3. In the **Hard disk** dialog box, select **Create a virtual hard disk now** and click **Create**.

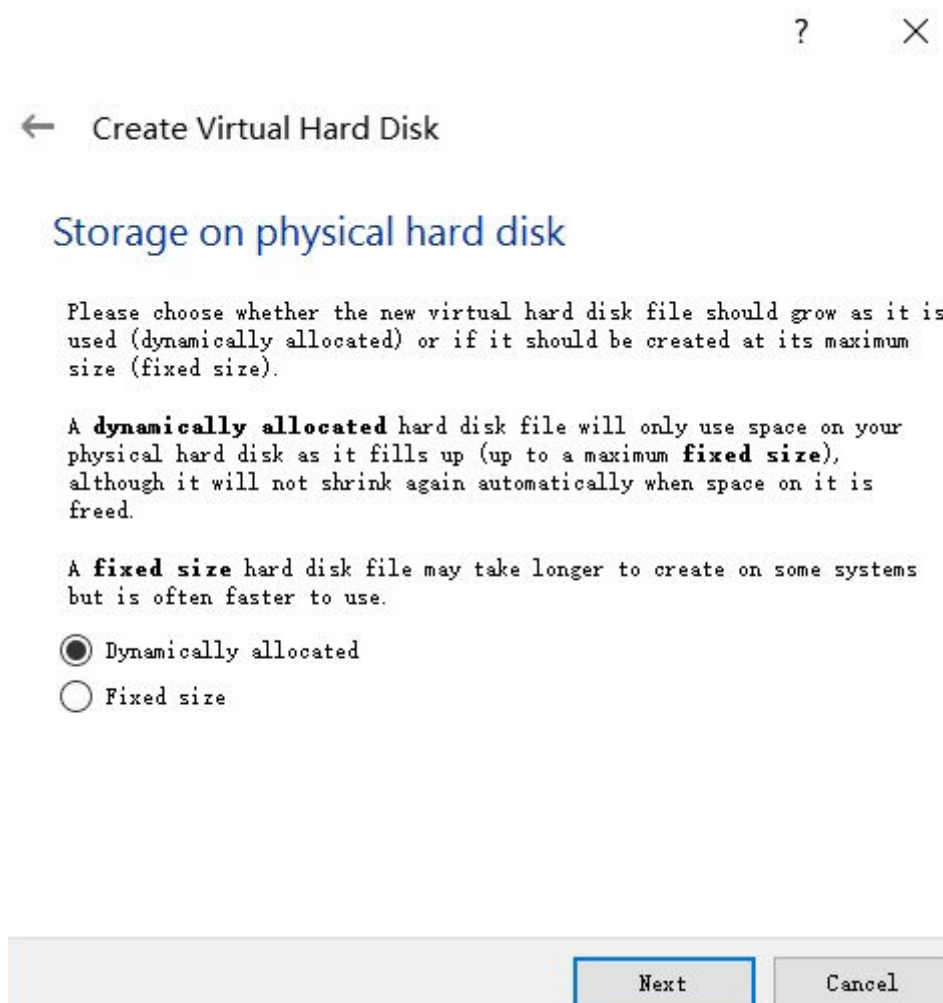
**Figure 2-8** Creating a virtual hard disk

4. In the **Hard disk file type** dialog box, select **VHD** and click **Next**.

**Figure 2-9** Setting the hard disk file type

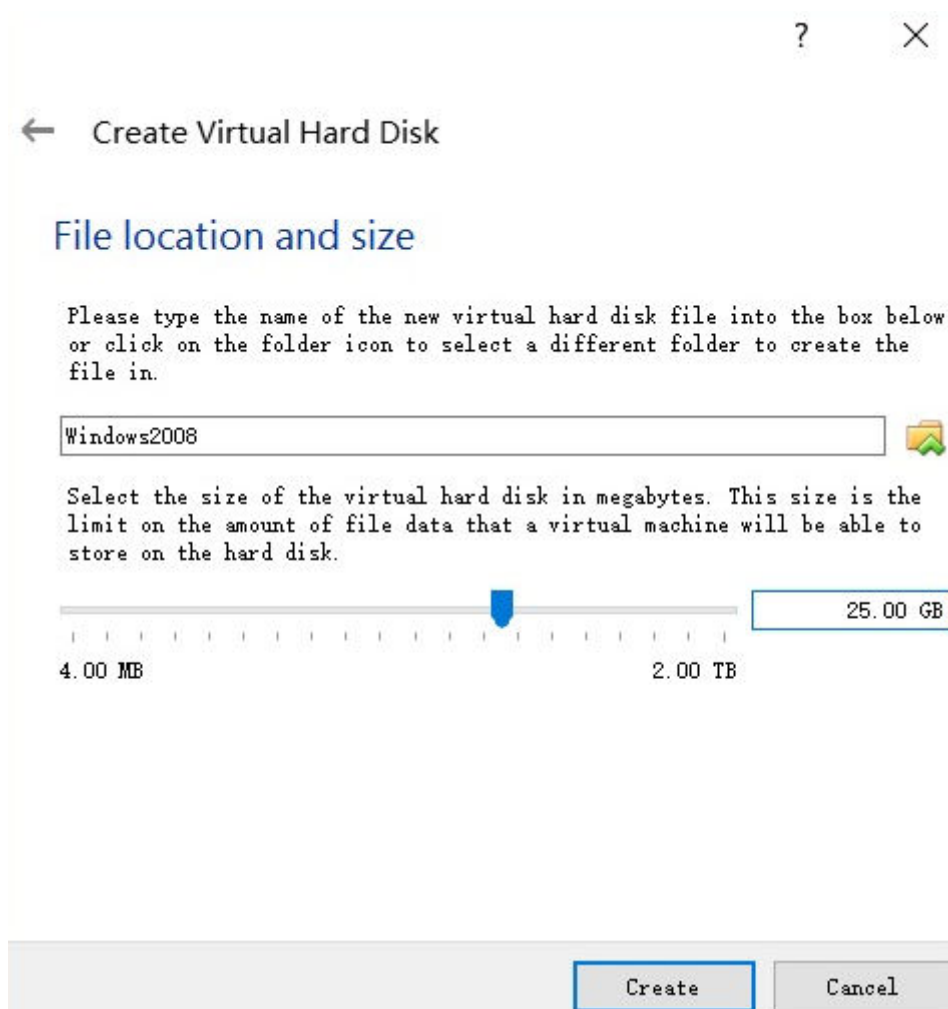


5. In the **Storage on physical hard disk** dialog box, select **Dynamically allocated** and click **Next**.

**Figure 2-10** Selecting the disk allocation mode

6. In the **File location and size** dialog box, set the disk size and storage location.

For example, you can set the disk size to 25 GB.

**Figure 2-11** Setting the disk location and size

7. Click **Create**.

## Installing Windows on the VM

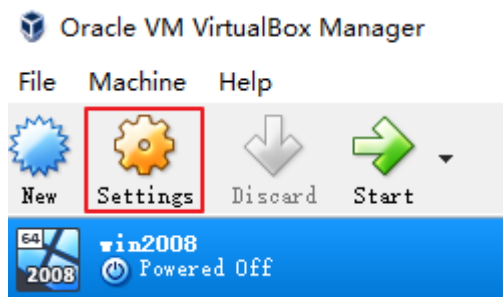
The procedure varies depending on the image file you use. This section uses Windows Server 2008 R2 as an example.


### NOTE

After the OS is installed, you need to activate it.

Use an ISO file to install Windows for the empty VM. Assume that the ISO image file is **Windows\_server\_2008\_r2.iso**.

1. In VirtualBox Manager, select the new VM and click **Settings**.

**Figure 2-12** Setting the VM

2. Choose **Storage > Empty**, click  in the **Attributes** area, and select the ISO image file **Windows\_server\_2008\_r2.iso**.

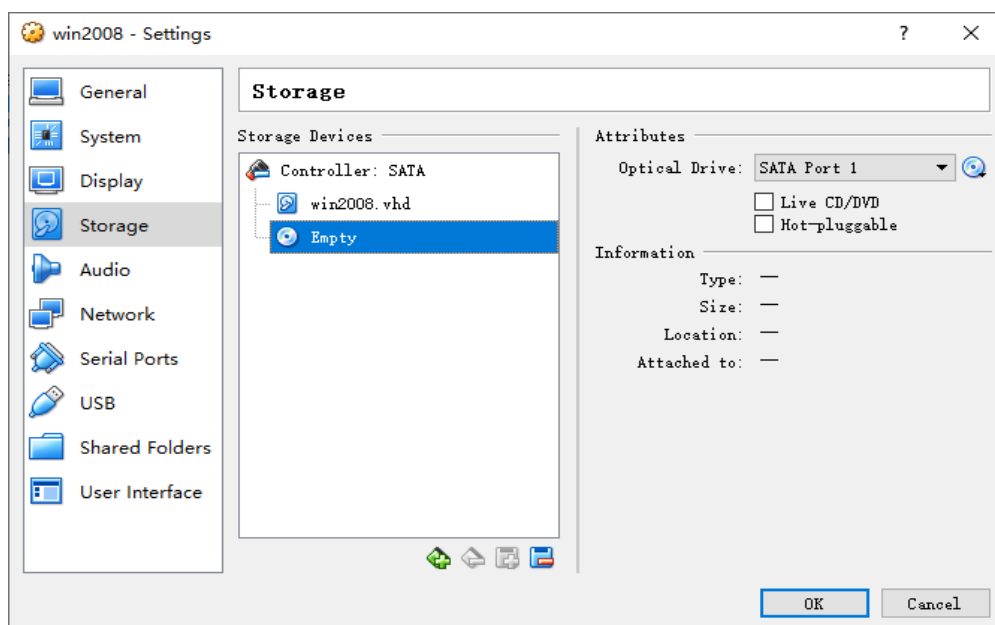
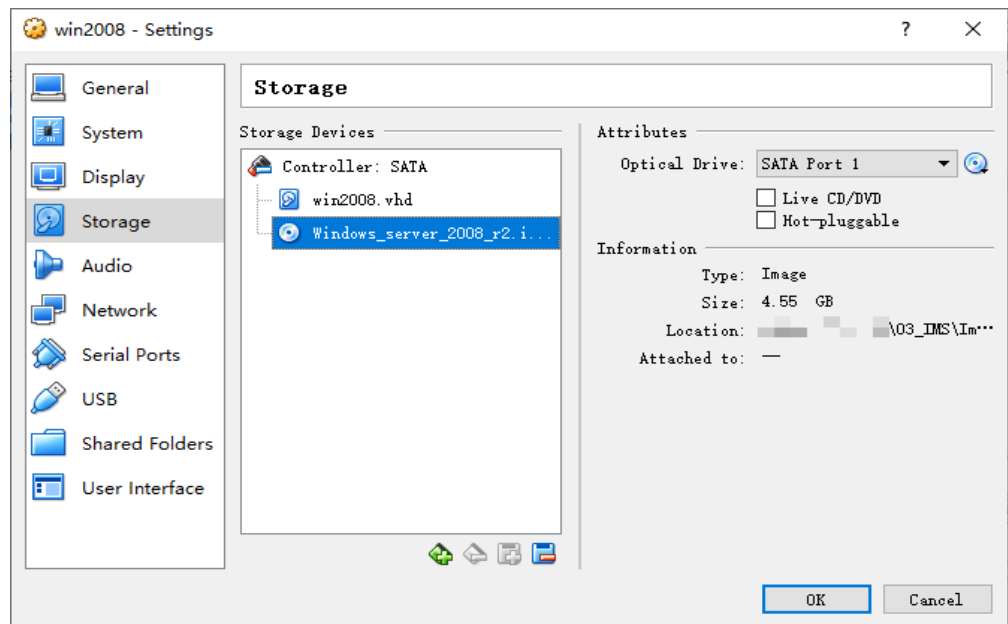
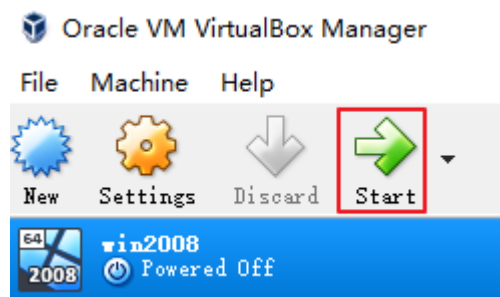
**Figure 2-13** Selecting the ISO file to be mounted

Figure 2-14 Mounted ISO file



3. In VirtualBox Manager, select the new VM and click **Start**.

Figure 2-15 Starting the VM



4. Install the OS as prompted.

## 2.4 Configuring the VM

### Install VirtIO Drivers

If VirtIO drivers are not installed, the image you create will be unavailable.

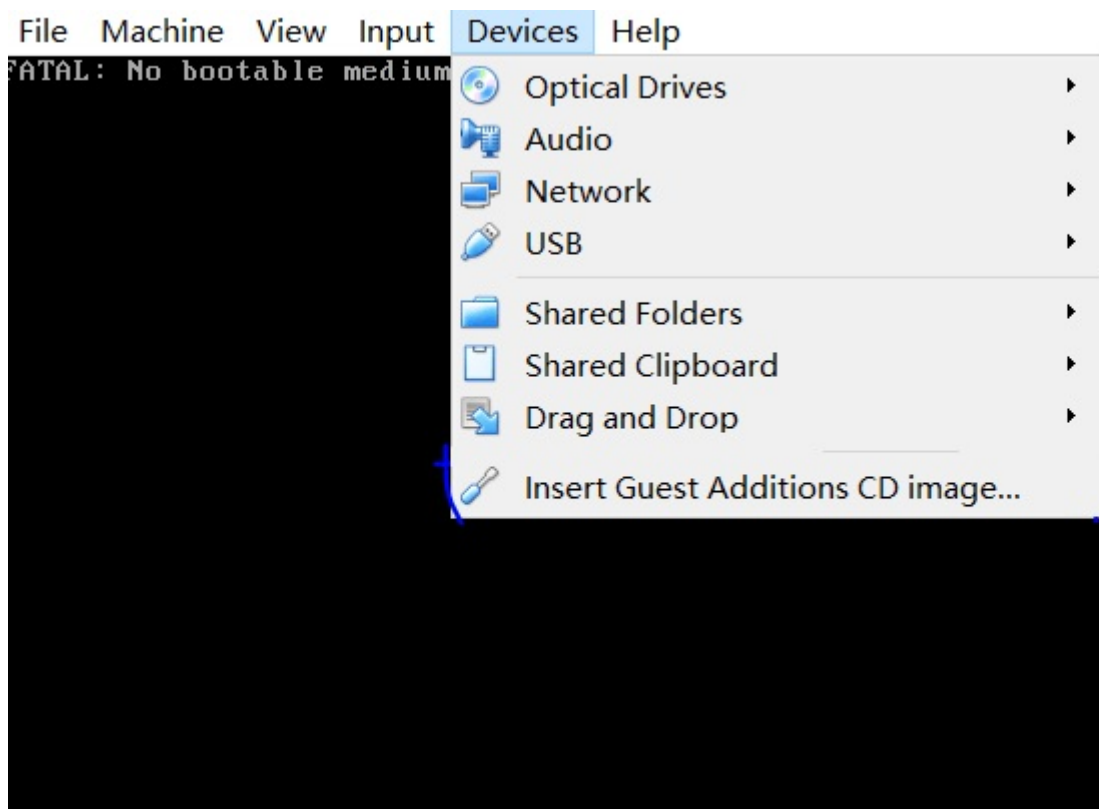
1. Download a VirtIO driver package.  
Download a **virtio-win.iso** driver package of the required version from:  
<https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/>
2. On the VirtualBox Windows VM, choose **Device > Allocate Drive > virtio-win.iso**.
3. Choose **Computer > CD Drive**.

## Install VirtualBox Guest Additions

After Guest Additions are installed on a Windows VM, files can be easily shared between the VM and host.

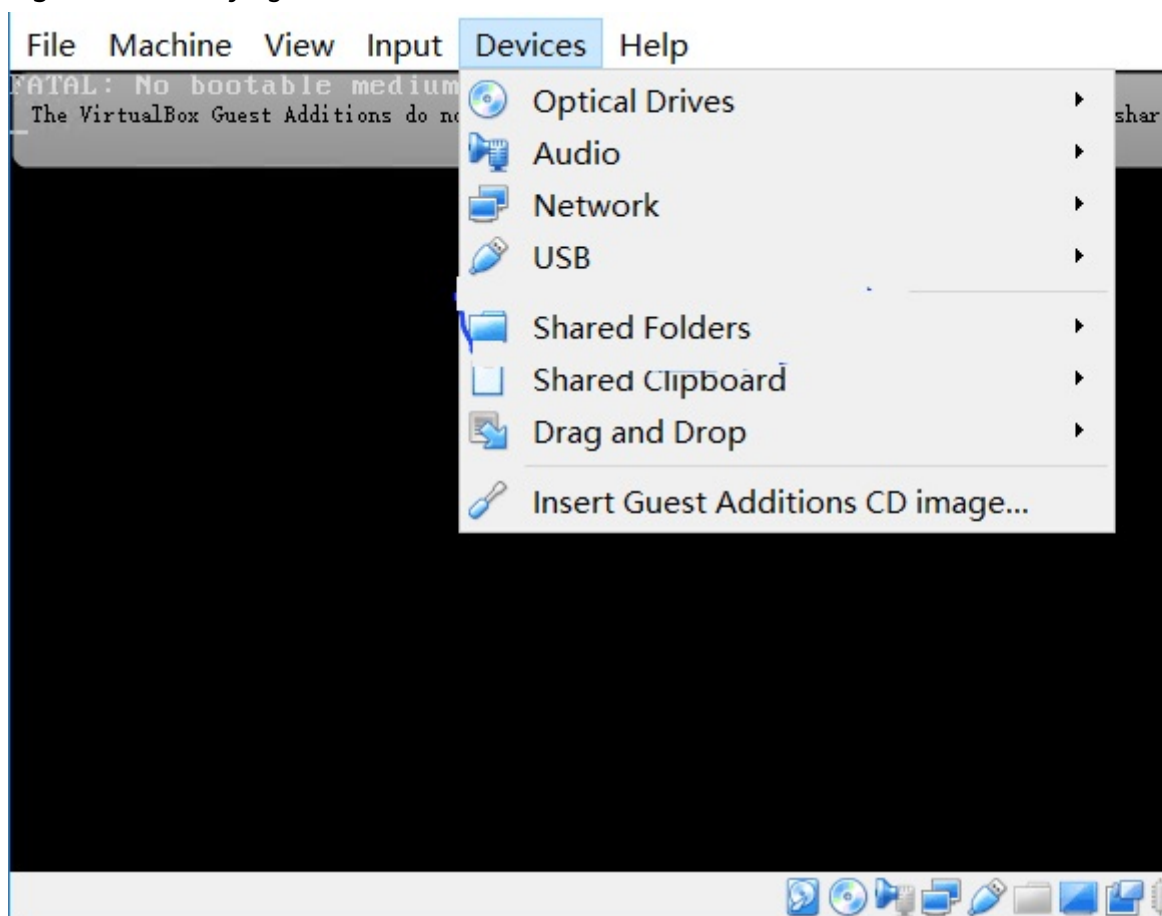
1. On the VirtualBox Windows VM, choose **Devices > Insert Guest Additions CD image**.

**Figure 2-16** Installing Guest Additions



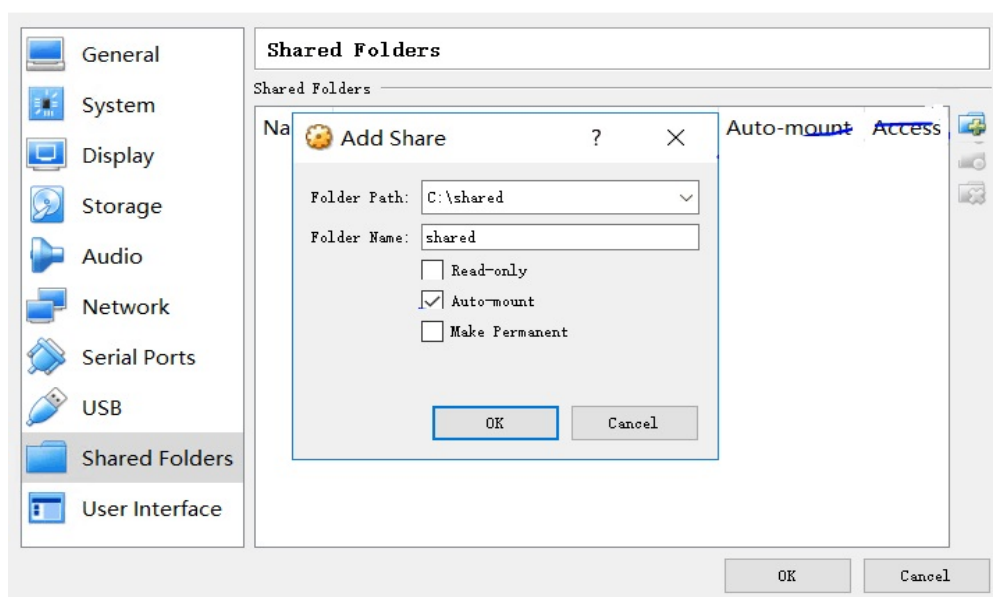
2. Choose **Computer > CD Drive**, double-click VirtualBox Guest, and complete the installation as prompted.
3. Verify the installation.  
After the installation is complete, click **Devices** to check whether a shared folder exists.

**Figure 2-17** Verifying the installation



4. Set the folder sharing mode.  
Select a folder path on the host where VirtualBox has been installed and set the sharing mode. After the folder is shared, you can access it from the VirtualBox VM.

**Figure 2-18** Setting the folder sharing mode



## (Optional) Install Cloudbase-Init

To ensure that you can inject custom information (for example, the login password) into ECSs created from the image, you are advised to install Cloudbase-Init on the VM that is used as the image source. If you do not install it, you can log in to the ECSs only with the password specified in the image.

### NOTE

Cloudbase-Init is open-source software. If the installed version has security vulnerabilities, you are advised to upgrade it to the latest version.

1. Download a Cloudbase-Init package.  
Download a Cloudbase-Init package of the required version based on the OS bit and save the package to a local shared folder.  
Cloudbase-Init official website: <http://www.cloudbase.it/cloud-init-for-windows-instances/>
2. On the VirtualBox Windows VM, choose **Computer > Network > VBOXSVR**.
3. Double-click the shared folder, copy the Cloudbase-Init package to the VM, and double-click the package to install Cloudbase-Init.

In this section, **CloudbaseInitSetup\_0\_9\_11\_x64** is used as an example.

## 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 can have a maximum of 63 characters.

### NOTE

If you are using NetBIOS in your network, the hostname cannot exceed 15 characters because NetBIOS has a 15 character limit.

- 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 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 need to 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 these 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 password length.

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 added, Cloudbase-Init will be set **RealTimeIsUniversal** back to **0**, causing the system to not 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 2-2** 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**

## (Optional) Install the One-Click Password Reset Plug-In

To ensure that you can reset the password of each ECS created from the image with a few clicks, you are advised to install the one-click password reset plug-in (CloudResetPwdAgent) on the VM that is used as the image source.

1. Download the one-click password reset plug-in CloudResetPwdAgent.  
Download the **CloudResetPwdAgent.zip** package from the following link and decompress it to a local shared folder:  
[https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/reset\\_pwd\\_agent/CloudResetPwdAgent.zip](https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip)
2. On the VirtualBox Windows VM, choose **Computer > Network > VBOXSVR**. Copy **CloudResetPwdAgent.zip** to the VM.
3. Install the one-click password reset plug-in.
  - a. Open the shared folder and double-click **setup.bat** in the **CloudResetPwdAgent.Windows** folder.
  - b. Open **Task Manager** and check whether the installation is successful.  
If you can find **cloudResetPwdAgent** in **Task Manager**, the installation is successful. Otherwise, the installation failed.

### NOTE

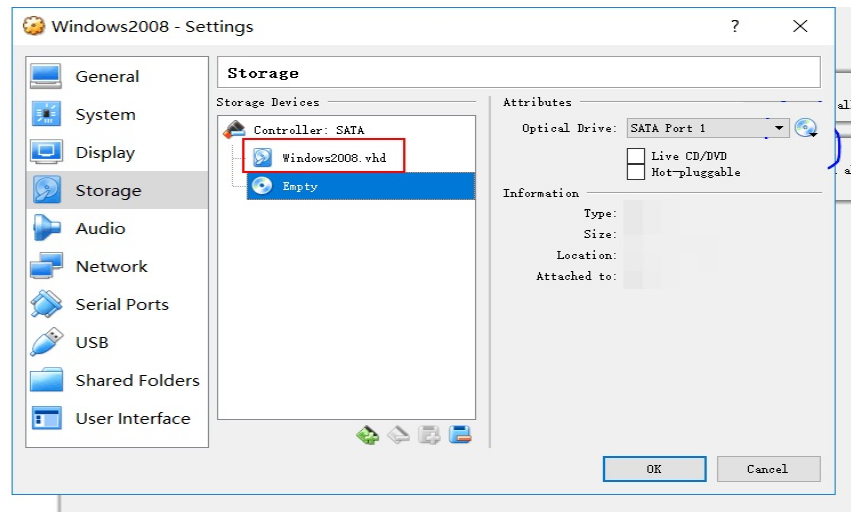
If the installation failed, check whether the installation environment meets the requirements and install the plug-in again.

## 2.5 Obtaining the Image File

After the VM is configured, perform the following operations to generate and export a Windows image file:

1. Open VirtualBox, select the VM, choose **Settings > Storage**, and select **win2008.vhd**.  
**win2008** is the VM name.
2. In the right pane, view the image file location.
3. Go to the location to obtain the generated **win2008.vhd** image file.

**Figure 2-19** Viewing the image file location



## 2.6 Registering the Image File as a Private Image

Upload the image file to an OBS bucket and register it as a private image.

### Constraints

- Only an unencrypted image file or an image file encrypted using SSE-KMS can be uploaded to an OBS bucket.
- When uploading an image file, you must select an OBS bucket with the storage class of Standard.

### Procedure

1. Use OBS Browser+ to upload the image file. For details, see [OBS Browser+ Best Practices](#).  
For how to download OBS Browser+, see [https://support.huaweicloud.com/intl/en-us/browsertg-obs/obs\\_03\\_1003.html](https://support.huaweicloud.com/intl/en-us/browsertg-obs/obs_03_1003.html).
2. Register the image file as a private image. For details, see [Registering an Image File as a Private Image](#).

# 3

## Creating a Linux Image Using VirtualBox and an ISO File

---

### 3.1 Introduction

#### VirtualBox

VirtualBox is free, open-source virtualization software. It was first offered by InnoTek GmbH from Germany and re-branded as Oracle VM VirtualBox when InnoTek was acquired by Oracle Corporation.

For more information about VirtualBox, visit the Oracle official website. Click [here](#) to see the guest OSs that can work with VirtualBox.

#### Scenarios

You can use a 32-bit or 64-bit Linux guest OS provided by VirtualBox to create an image file in VHD format.

#### Advantages

You can customize Linux image files.

#### Tools and Costs

**Table 3-1** Tools and costs

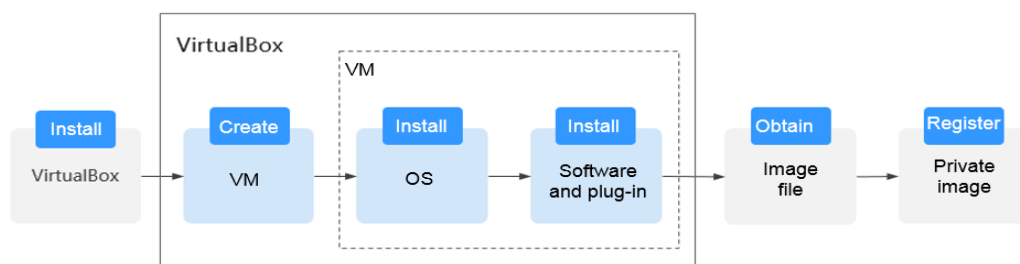
Tool	Description	Costs
VirtualBox	VirtualBox is free, open-source virtualization software. Download it from: <a href="https://www.virtualbox.org/wiki/Downloads">https://www.virtualbox.org/wiki/Downloads</a>	Free

Tool	Description	Costs
ISO image file	It is used to install an OS on an empty VM. Download it from <a href="https://ubuntu.com/download/server#downloads">https://ubuntu.com/download/server#downloads</a> For example, the file name is <b>Ubuntu-20.04-server.iso</b> .	Free
Cloud-Init	To ensure that you can inject custom information (for example, the login password) into ECSs created from the image, you are advised to install Cloud-Init on the VM that is used as the image source.  The method for obtaining Cloud-Init varies depending on the OS. For details, see <a href="#">(Optional) Install and Configuring Cloud-Init</a> .	Free
(Optional) One-click password reset plug-in	To ensure that you can reset the password of each ECS created from the image with a few clicks, you are advised to install the one-click password reset plug-in (CloudResetPwdAgent) on the VM that is used as the image source.  For 32-bit OSs: <a href="http://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip">http://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip</a> For 64-bit OSs: <a href="http://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip">http://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip</a>	Free

## Image Creation Process

The following figure shows how to use VirtualBox to create an image from an ISO file.

**Figure 3-1** Image creation process



1. Install VirtualBox: Prepare a host (64-bit Windows is recommended) and install VirtualBox on the host. For details, see [Installing VirtualBox](#).
2. Create a VM: Use VirtualBox to create an empty VM from which an image will be created. For details, see [Creating an Empty VM](#).
3. Install an OS on the VM: Mount an ISO file to install an OS for the VM. The ISO file determines the OS of the image you want to create. For details, see [Installing Linux on the VM](#).
4. Install software and plug-ins on the VM: To ensure that ECSs created from this image can run properly, install the required software and plug-ins on the VM, including native Xen and KVM drivers, Cloud-Init, and one-click password reset plug-in. For details, see [Configuring the VM](#).
5. Obtain the image file: Export an image file in VHD format from VirtualBox. For details, see [Obtaining the Image File](#).
6. Register a private image: Upload the exported VHD image file to an OBS bucket and register it as a private image. Then, you can use the private image to create ECSs. For details, see [Registering the Image File as a Private Image](#).

## 3.2 Installing VirtualBox

### Preparations

The host where VirtualBox is to be installed must meet the following requirements:

- A 64-bit Windows OS (recommended).
- At least 4 GB of memory and a dual-core processor. For example, the host specifications can be 8U16G.
- At least 20 GB of available disk space.
- CPU hardware virtualization (Intel VT-x or AMD-V) enabled. For how to enable it, see [Host CPU Settings \(Hardware Virtualization\)](#).

#### NOTE

For details about how to install VirtualBox, see the VirtualBox user guide at <https://www.virtualbox.org/manual/UserManual.html>.

### Host CPU Settings (Hardware Virtualization)

For an Intel host, perform the following operations to enable hardware virtualization:

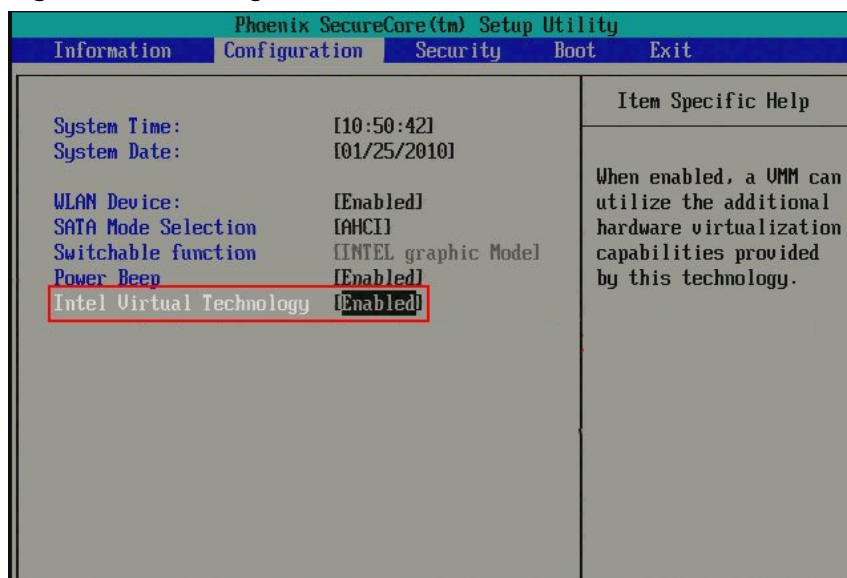
#### NOTE

The operations may differ depending on the CPU type. You can do it as prompted.

1. During the host startup, press the BIOS key set by the manufacturer to access the BIOS.
2. Choose **Configuration > Intel Virtual Technology**, and press **Enter**.
3. Select **Enabled** and press **Enter**. The value of **Intel Virtual Technology** will become **Enabled**.

4. Press **F10** to save the settings and exit.

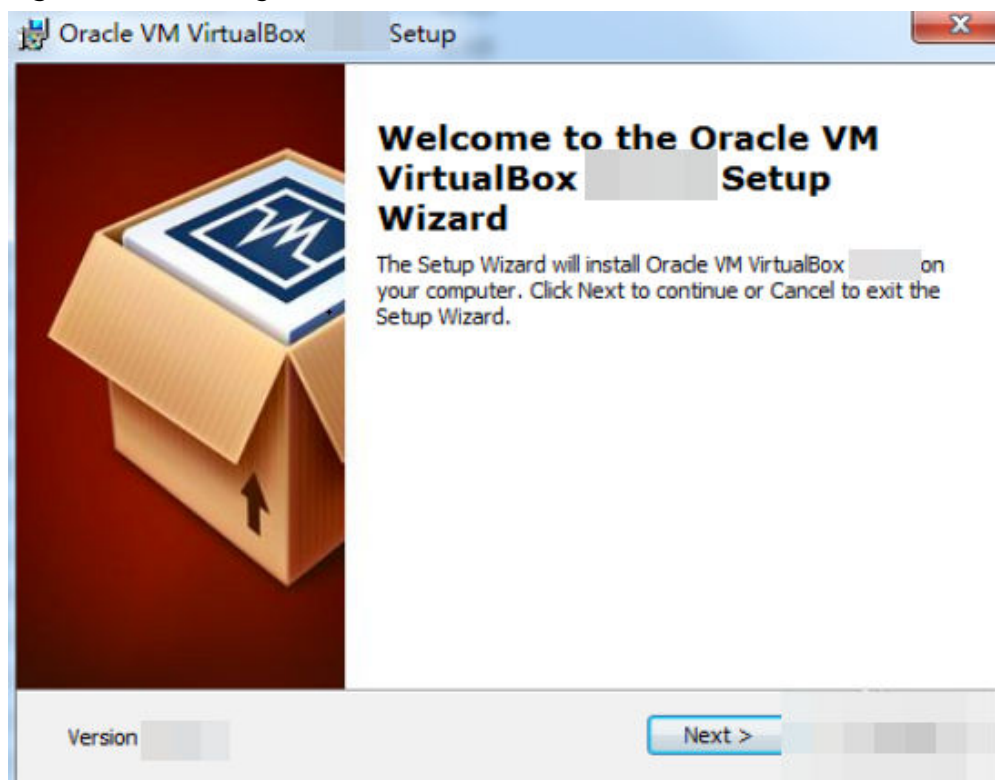
**Figure 3-2** Enabling hardware virtualization



## Procedure

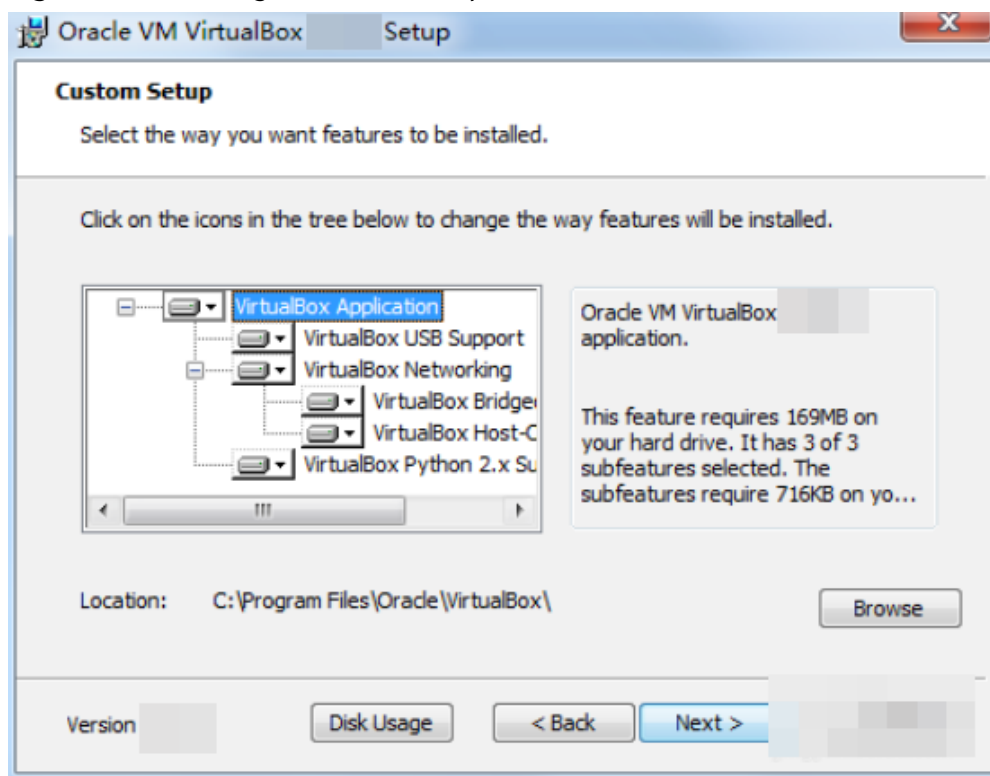
1. Download a VirtualBox package. VirtualBox-5.2.0 is used as an example. Download it from <https://www.virtualbox.org/wiki/Downloads>.
2. Decompress the package. Right-click **VirtualBox-5.2.0-118431-Win.exe**, choose **Run as administrator**, and click **Next**.

**Figure 3-3** Installing VirtualBox



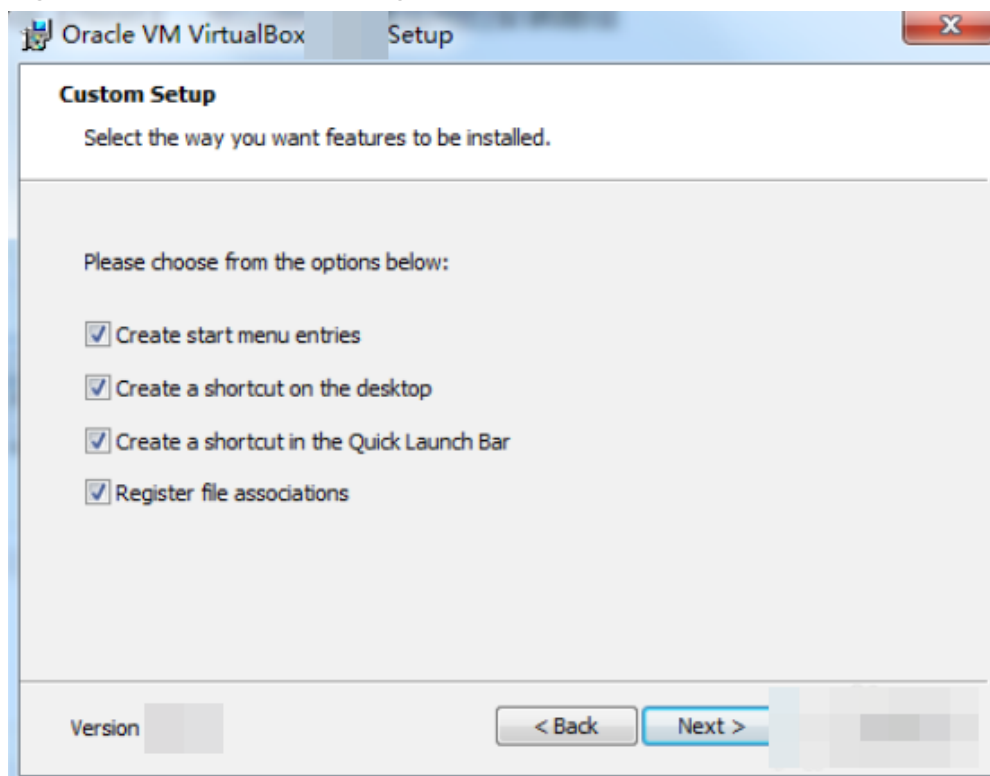
3. Select a VirtualBox installation path and click **Next**.

**Figure 3-4** Selecting an installation path



4. Personalize the settings and click **Next**.

**Figure 3-5** Personalized settings



5. Click **Finish**.

## 3.3 Creating a VM and Installing an OS

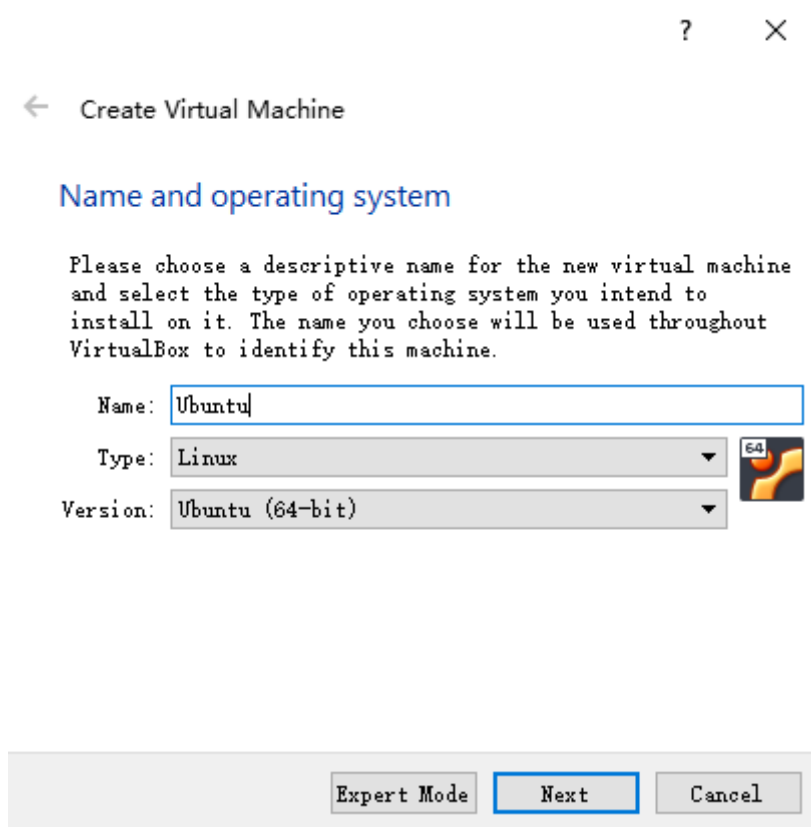
### Prerequisites

VirtualBox has been installed.

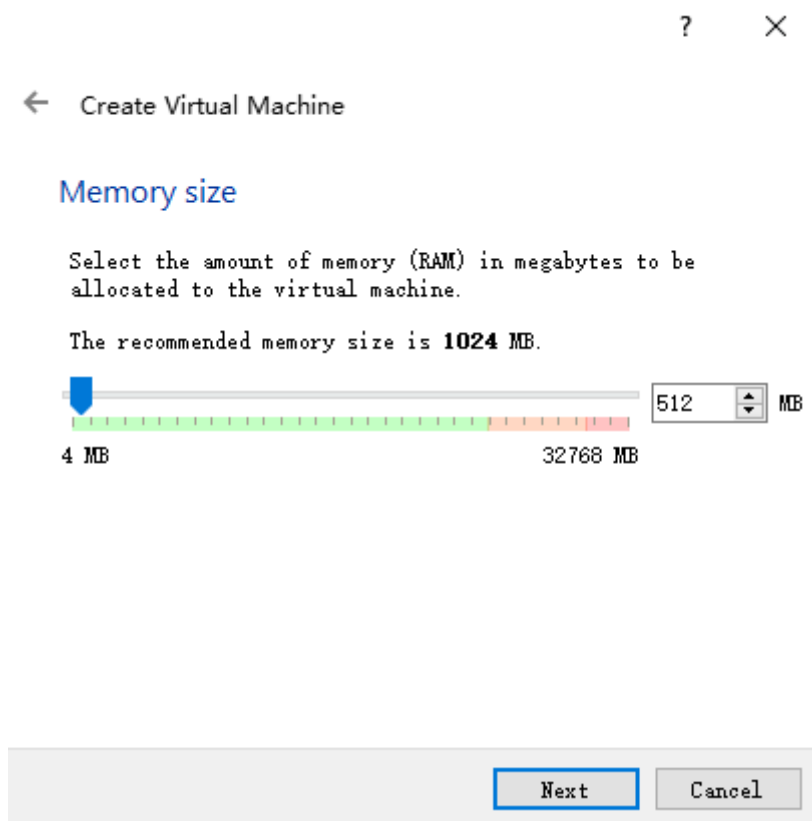
### Creating an Empty VM

1. Open VirtualBox and click **New**. In the displayed **Create Virtual Machine** dialog box, enter a VM name, select an OS type and version, and click **Next**.  
Take Ubuntu as an example. The type must be **Linux**.  
Ensure that the selected version is the same as that of the OS you want to install on the VM.

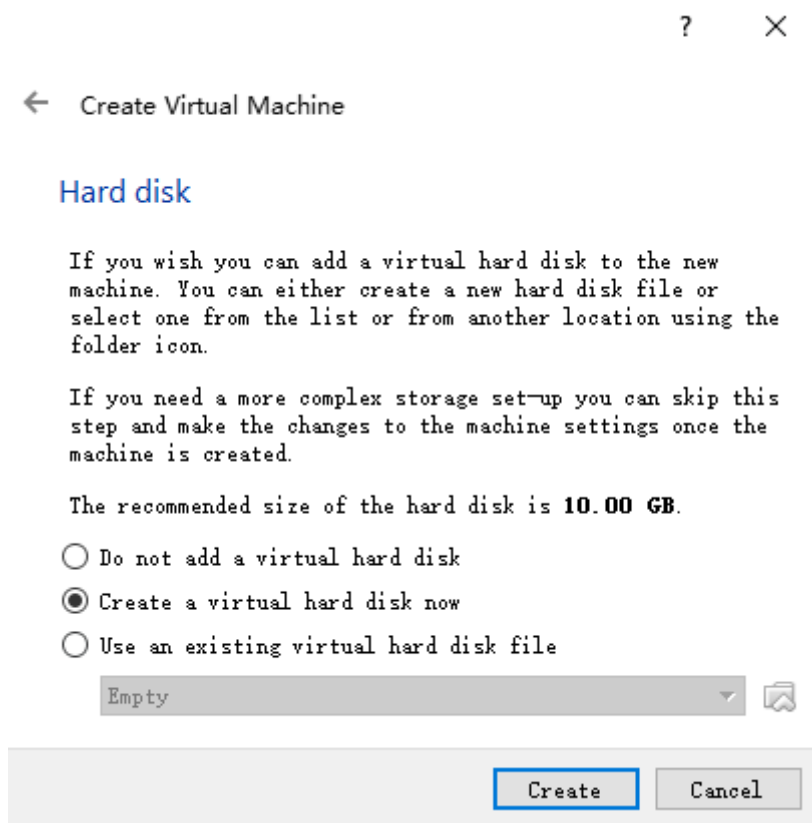
**Figure 3-6** Creating a VM



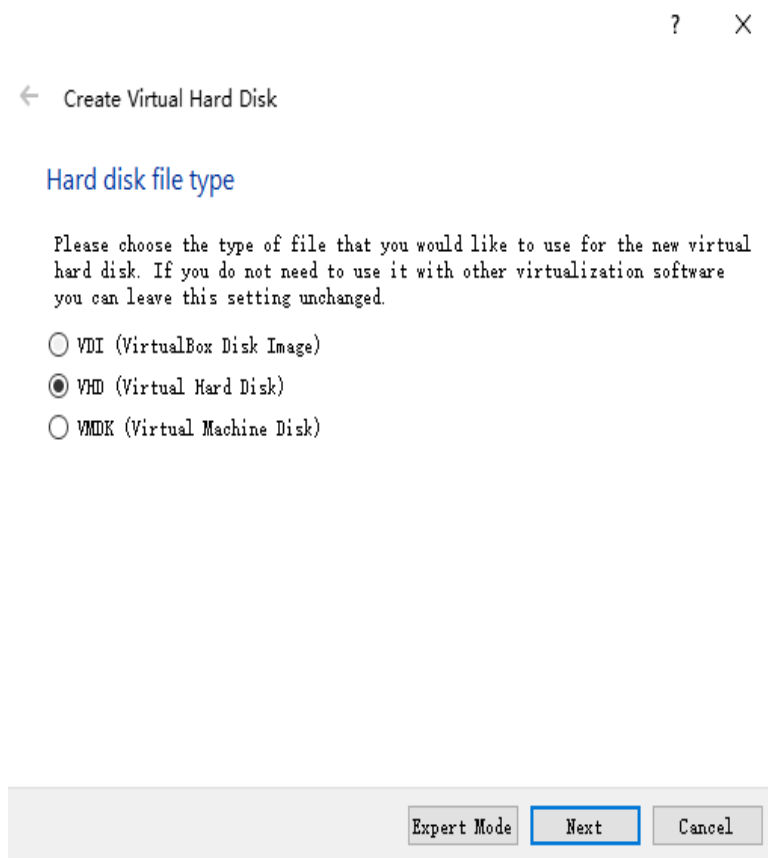
2. In the **Memory size** dialog box, set a value and click **Next**.  
You can reference the VM specifications or official OS requirements. The minimum value is 256 MB. You can set the memory size to 512 MB as an example.

**Figure 3-7** Setting the memory size

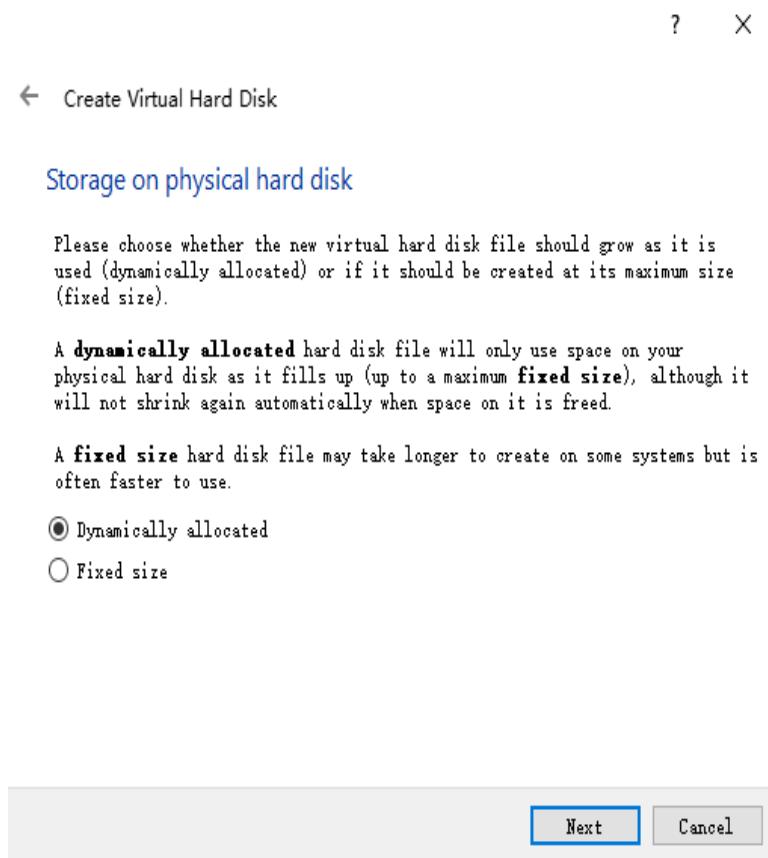
3. In the **Hard disk** dialog box, select **Create a virtual hard disk now** and click **Create**.

**Figure 3-8** Creating a virtual hard disk

4. In the **Hard disk file type** dialog box, select **VHD** and click **Next**.

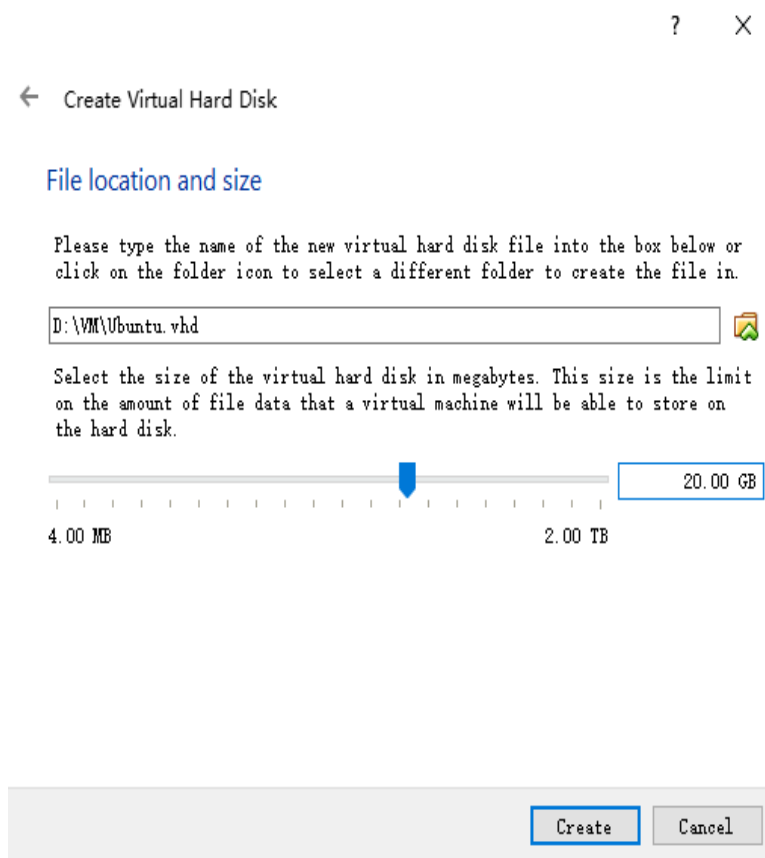
**Figure 3-9** Setting the hard disk file type

5. In the **Storage on physical hard disk** dialog box, select **Dynamically allocated** and click **Next**.

**Figure 3-10** Selecting the disk allocation mode

6. In the **File location and size** dialog box, set the disk size and storage location.

For example, you can set the disk size to 20 GB.

**Figure 3-11** Setting the disk location and size

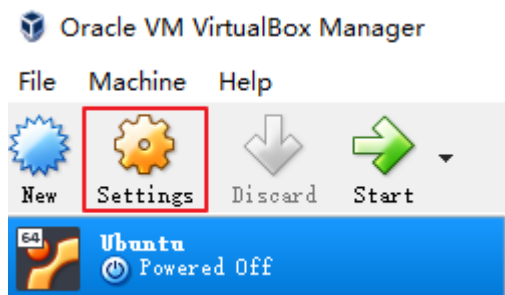
7. Click **Create**.


## Installing Linux on the VM

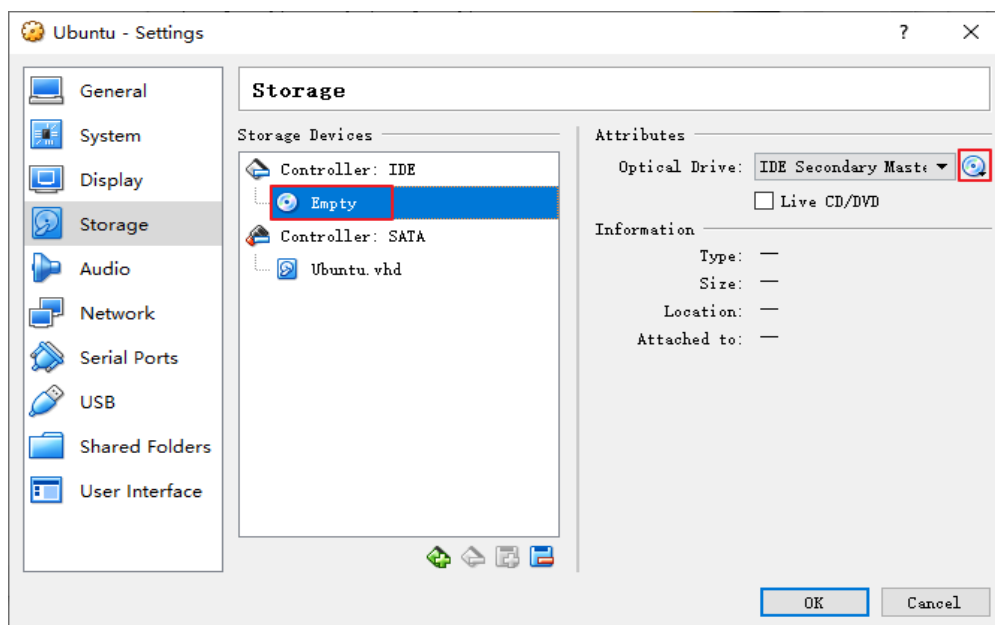
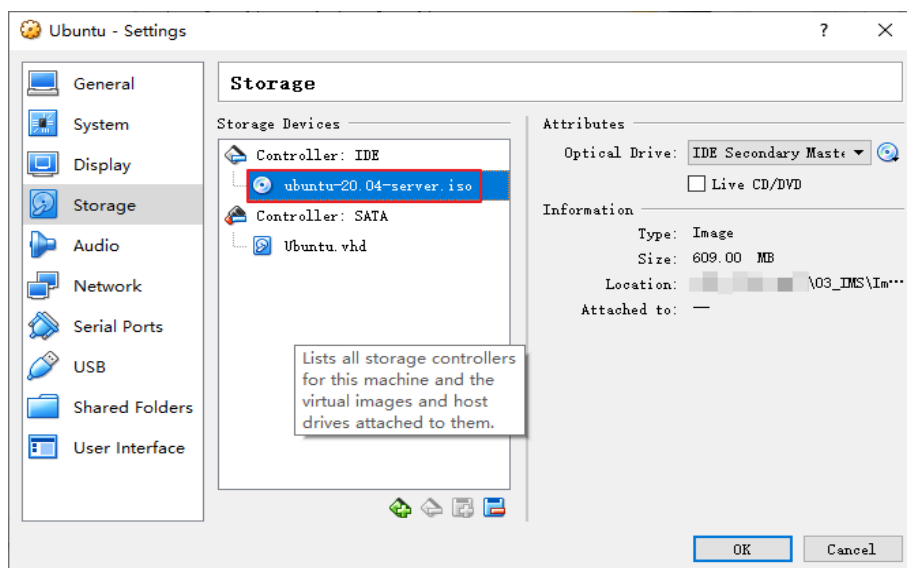
The procedure varies depending on the image file you use. This section uses Ubuntu 20.04 as an example.

Use an ISO file to install Linux for the empty VM. Assume that the ISO image file is **Ubuntu-20.04-server.iso**.

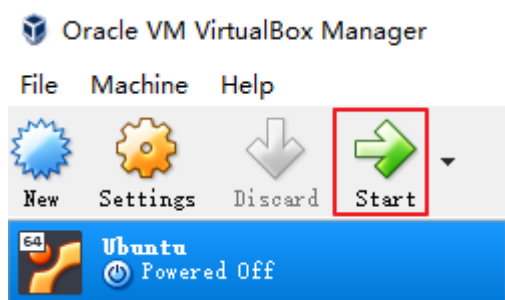
1. In VirtualBox Manager, select the new VM and click **Settings**.

**Figure 3-12** Setting the VM

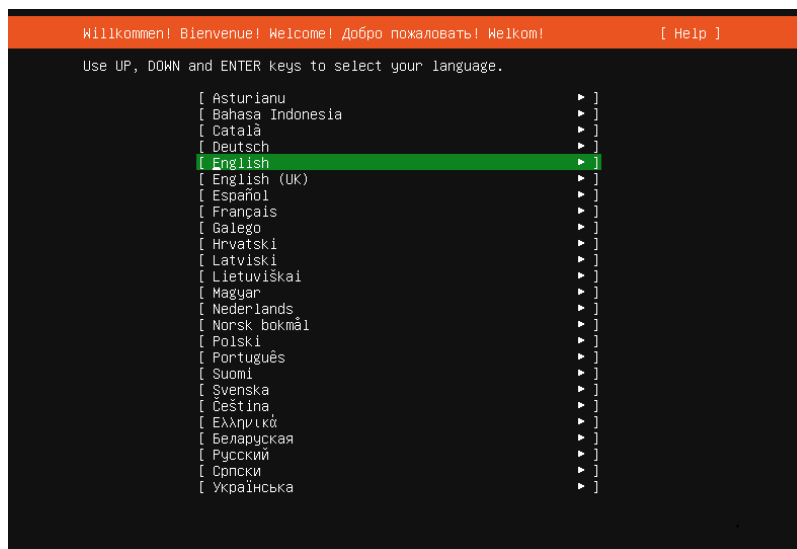
2. Choose **Storage > Empty**, click  in the **Attributes** area, and select the ISO image file **Ubuntu-20.04-server.iso**.

**Figure 3-13** Selecting the ISO file to be mounted**Figure 3-14** Mounted ISO file

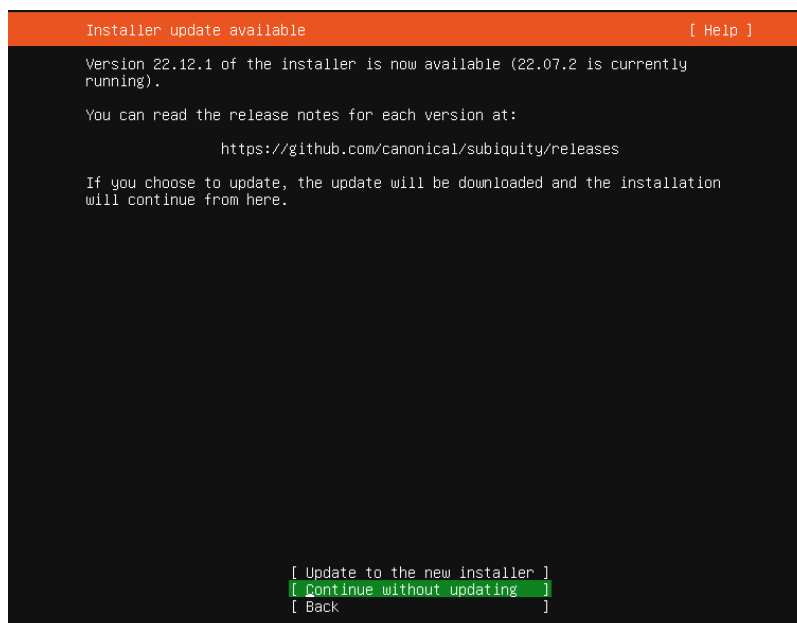
3. Click **OK**.
4. In VirtualBox Manager, select the new VM and click **Start**.

**Figure 3-15** Starting the VM

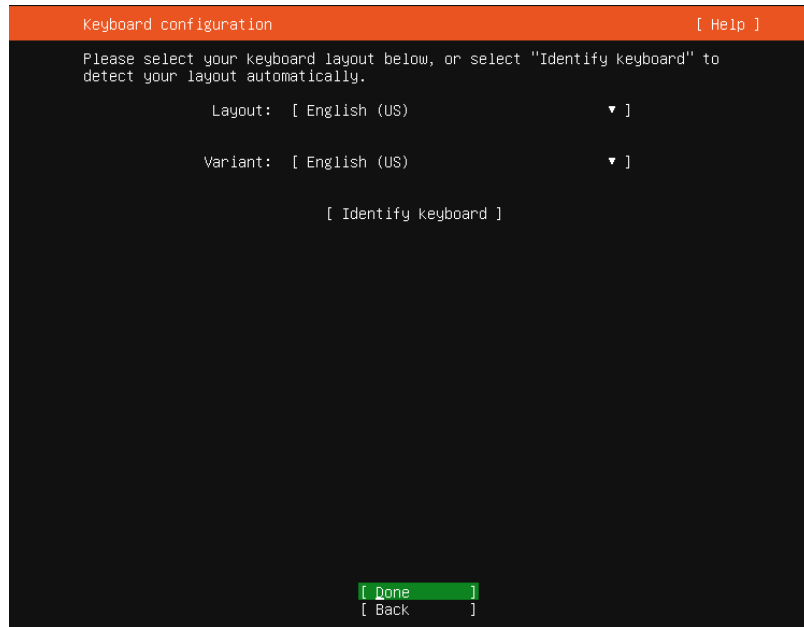
5. Install the OS.
  - a. Select **English** and press **Enter**.



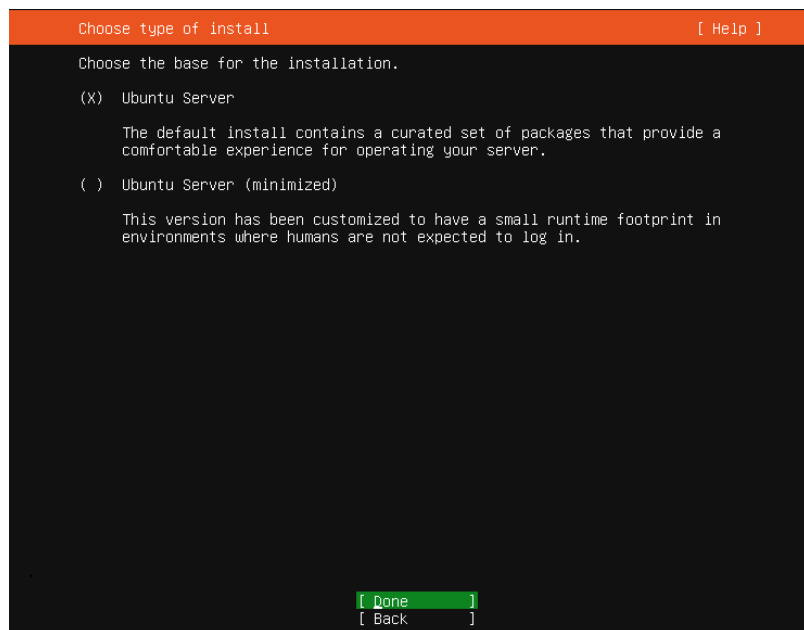
- b. Select **Continue without updating**.



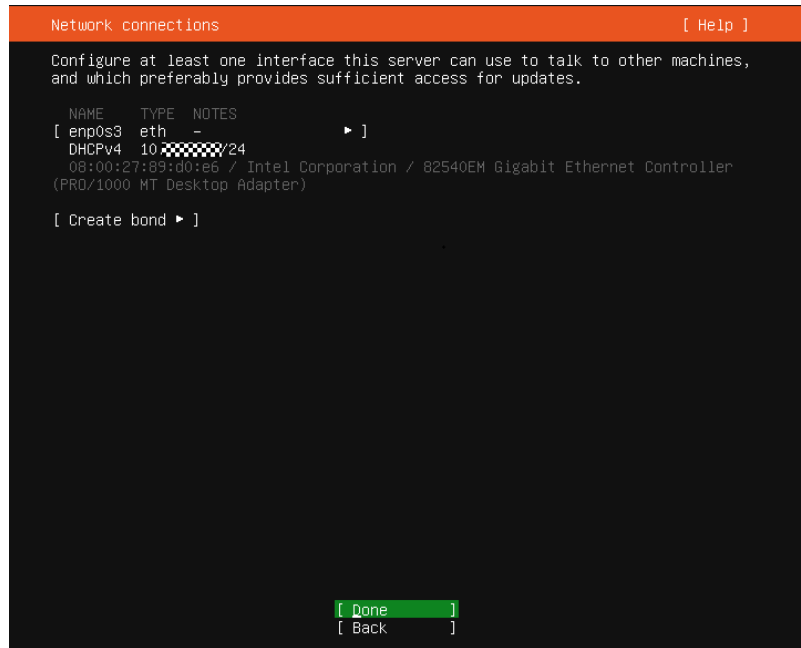
- c. Retain the default settings for the keyboard. Select **Done**.



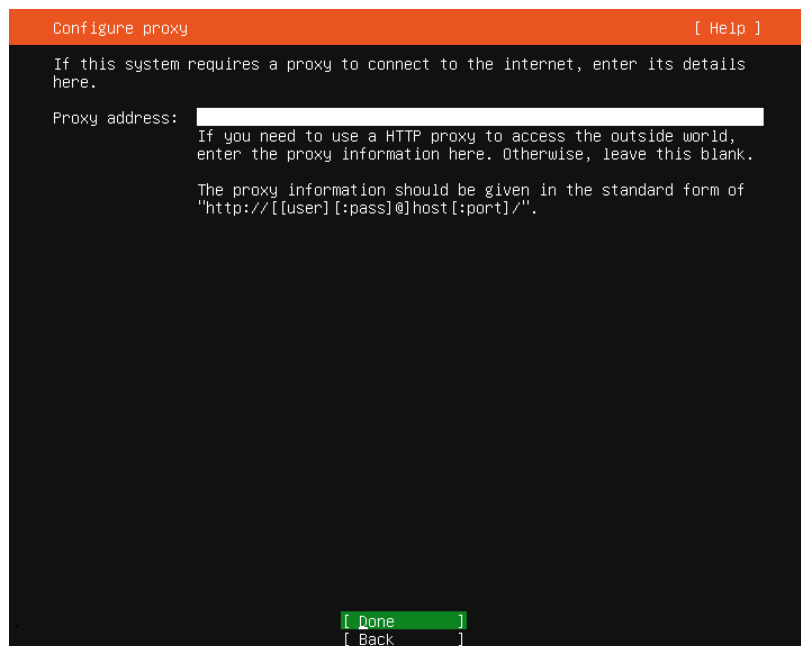
- d. Retain the default settings for the installation base. Select **Done**.



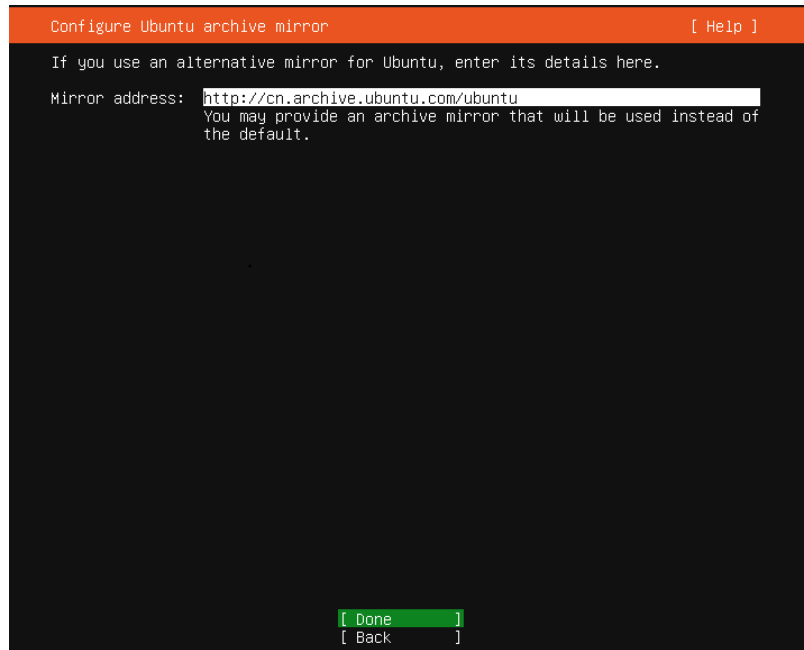
- e. Retain the default settings for the network. Select **Done**.  
The installation program will automatically identify the IP address. If the network cannot be found, the installation program can still continue and you can configure the network again after the installation is complete.



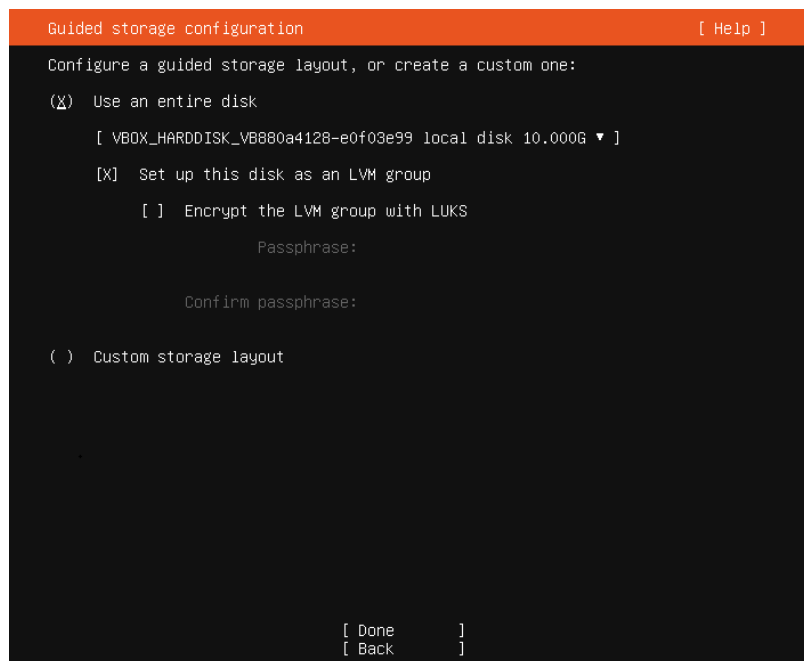
- f. Retain the default settings for the proxy. Select **Done**.



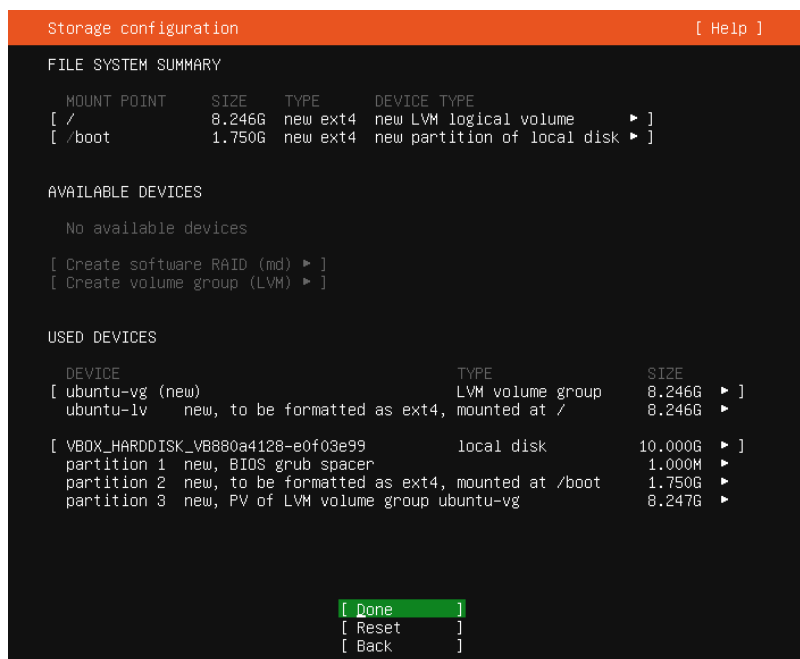
- g. Retain the default settings for the software source. Select **Done**.



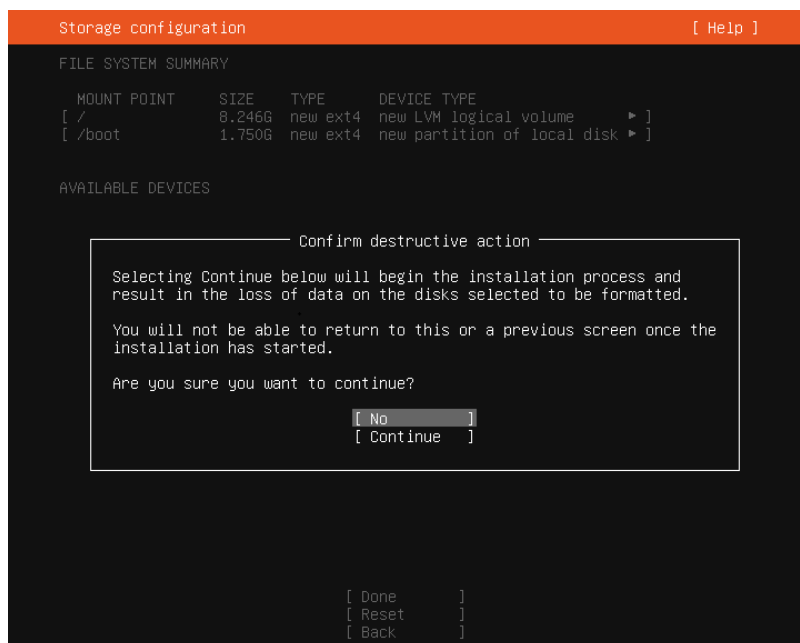
- h. Retain the default settings for disk partitioning (use an entire disk and set up this disk as an LVM group). Select **Done**.



The file system information will be displayed. Check it and select **Done**.



Confirm the destructive action and select **Continue**.



- i. Configure the server name, username, and password. Select **Done**.  
**Your name:** It is not a username for logging in to the server. You can consider it as server description.  
**Your Server's name:** It is a unique server name on the same network. The name cannot contain uppercase letters.  
**Pick a username:** It is a username for logging in to the server. If you forget it or its password, you will not be allowed to log in to the server.  
**Choose a password:** It is the password for logging in to the server.  
**Confirm your password:** Enter your password again.

Profile setup [ Help ]

Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.

Your name:

Your server's name:   
The name it uses when it talks to other computers.

Pick a username:

Choose a password:

Confirm your password:

[ Done ]

- j. Install SSH so that you can remotely connect to the Linux VM.  
Select **Install OpenSSH server**. Then, press **Tab** to select **Done**.

SSH Setup [ Help ]

You can choose to install the OpenSSH server package to enable secure remote access to your server.

☒ Install OpenSSH server

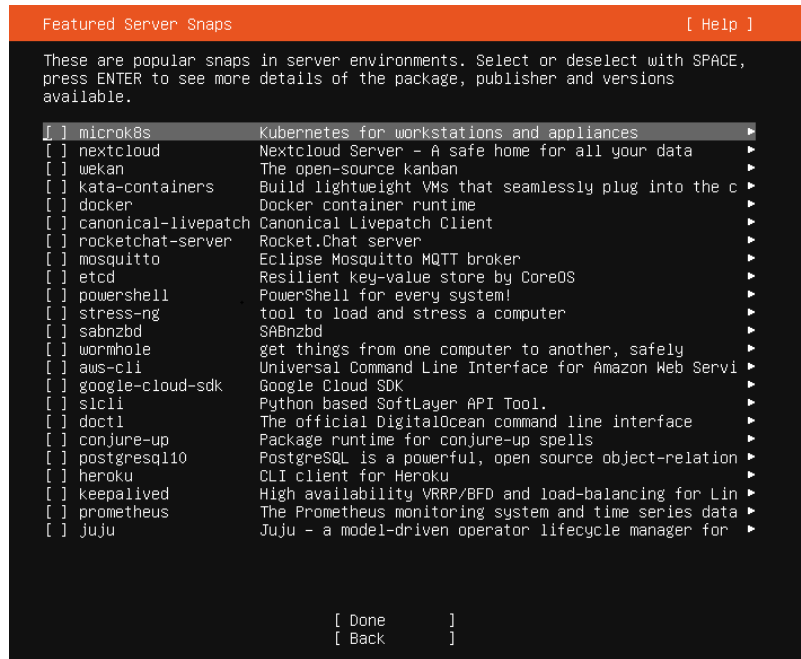
Import SSH identity: [ No ▼ ]  
You can import your SSH keys from GitHub or Launchpad.

Import Username:

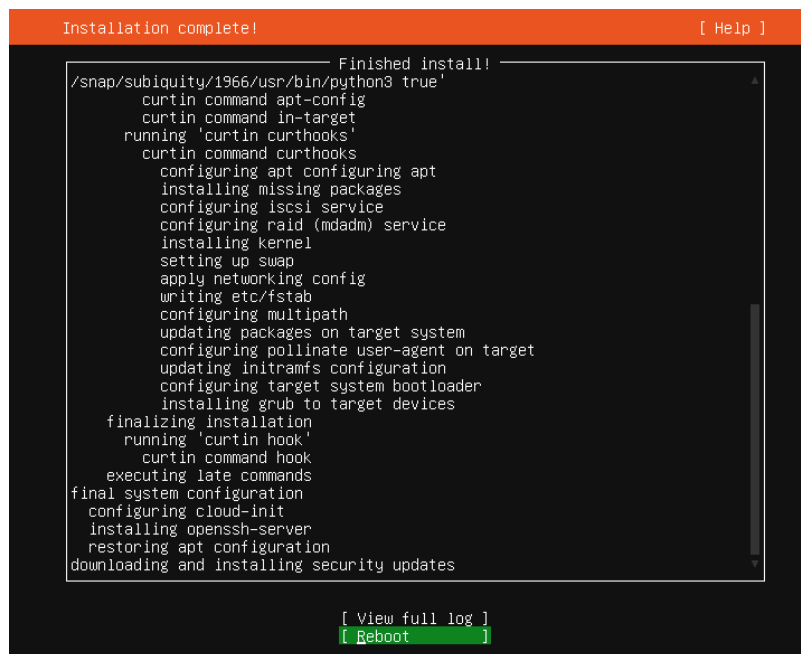
☒ Allow password authentication over SSH

[ Done ]  
[ Back ]

- k. Select **Done** to start the OS installation.



- l. After the installation is complete, select **Reboot** to restart the system.



## 3.4 Configuring the VM

### Install Native Xen and KVM Drivers

Ubuntu 20.04 is used as an example to illustrate the driver installation. For other OS types, see [Installing Native Xen and KVM Drivers on a Xen ECS](#).

1. Open the **modules** file.  
**vi /etc/initramfs-tools/modules**

- Press **i** to enter the editing mode and add native Xen (xen-pv) and KVM (VirtIO) drivers to the `/etc/initramfs-tools/modules` file (the format depends on the OS requirements).

```
[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
```

- Press **Esc**, enter **:wq**, and press **Enter** to save the settings and exit the vi editor.

- Generate initramfs or initrd again.

```
update-initramfs -u
```

- Check whether native Xen and KVM drivers are 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_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, the VM will not be affected but such drivers cannot be shown by running the **lsinitrd** command. You can run the following commands to check whether there are built-in drivers 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
[root@ CTU10000xxxx home]# cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y
CONFIG_XEN_BLKDEV_FRONTEND=y
CONFIG_XEN_NETDEV_FRONTEND=y
```

## Change Disk Identifiers in the GRUB Configuration File to the UUID Format

Take Ubuntu 20.04 as an example. Run **blkid** to obtain the UUID of the root partition. Modify the `/boot/grub/grub.cfg` file and use this UUID to configure the boot item. If the root partition is already using UUID, no modification is required. The procedure is as follows:

- Log in to the VM as **root**.
- List all types of mounted file systems and their 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"
```

3. Display the **grub.cfg** file content.

### 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  
}
```

4. Check whether 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 UUID format and no further action is required.
  - If **root=/dev/xvda1** is contained, the root partition is represented by a device name. Go to [5](#).
5. Obtain the UUID of the root partition based on **root=/dev/xvda1** and information obtained by running the **blkid** command.
6. Open the **grub.cfg** file.
7. Press **i** to enter the editing mode. Change the identifier of the root partition to the UUID format. For example, change **root=/dev/xvda1** to **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34**.
8. Press **Esc**, enter **:wq**, and press **Enter** to save the settings and exit the vi editor.
9. 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 '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=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34 ro
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-3.13.0-24-generic
}
```

## Change Disk Identifiers in the **fstab** File to the UUID Format

Take Ubuntu 20.04 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. List all types of mounted file systems and their 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"
```

2. Display the **fstab** file content.

### **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
```

3. Check whether disk identifiers in the **fstab** file are device names or UUIDs.
  - If they are UUIDs, no further action is required.
  - If they are device names, go to [4](#).
4. Open the **fstab** file.

### **vi /etc/fstab**
5. Press **i** to enter the editing mode and change disk identifiers to the UUID format.
6. Press **Esc**, enter **:wq**, and press **Enter** to save the settings and exit the vi editor.

## (Optional) Install and Configuring Cloud-Init

To ensure that you can inject custom information (for example, the login password) into ECSs created from the image, you are advised to install Cloud-Init on the VM that is used as the image source.

## Check Whether Cloud-Init Has Been Installed

The method of checking whether Cloud-Init is installed varies depending on the OS.

- 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.

After Cloud-Init is installed, perform the following operations:

- Determine whether to continue to use the SSH certificate in the VM OS. If no, 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**
- Delete the cache data generated by Cloud-Init to ensure that ECSs created from the image can be logged in by using a certificate:  
**sudo rm -rf /var/lib/cloud/\***

#### NOTE

After the operations are complete, do not restart the VM. Otherwise, you need to perform these operations again.

## **(Recommended) Install Cloud-Init Using the Official Installation Package**

The method of installing Cloud-init varies depending on the OS. Perform the installation as **root**.

The following describes how to install Cloud-Init in 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 for CoreOS.

- SUSE Linux  
URLs for obtaining a 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 a repo installation package matching your OS.

Take SUSE Enterprise Linux Server 12 as an example.

- a. Log in to the VM.
- b. Add a network installation source.  
**zypper ar https://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/SLE\_12\_SP3/Cloud:Tools.repo**
- c. Update the network installation source.  
**zypper refresh**
- d. Install Cloud-Init.  
**zypper install cloud-init**
- e. 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, prevent DHCP from changing the hostname.

1. 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 3-2** lists the URLs for obtaining a Cloud-Init installation package for CentOS. Select an epel-release installation package matching your OS.

**Table 3-2** Network installation sources of Cloud-Init

OS	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>

OS	Version	How to Obtain
	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. Install Cloud-Init.

```
yum install network-installation-source/epel-release-x-y.noarch.rpm
```

```
yum install cloud-init
```

 NOTE

*network-installation-source* indicates the address of the Cloud-Init epel-release installation package, and *x-y* indicates the version of the Cloud-Init epel-release matching your OS. Replace them with the actual values based on [Table 3-2](#).

- 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. 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 that address. If the file does not contain the address, configure the address by following the instructions on the Fedora official website.

- a. Install Cloud-Init.

```
yum install cloud-init
```

- b. 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 that address. If the file does not contain the address,

configure the address by following the instructions on the Debian or Ubuntu official website.

- a. Install Cloud-Init.

```
apt-get update
```

```
apt-get install cloud-init
```

- b. 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 in 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]#
[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 the Cloud-Init version and 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 22.04/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 the Cloud-Init version and 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 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
```

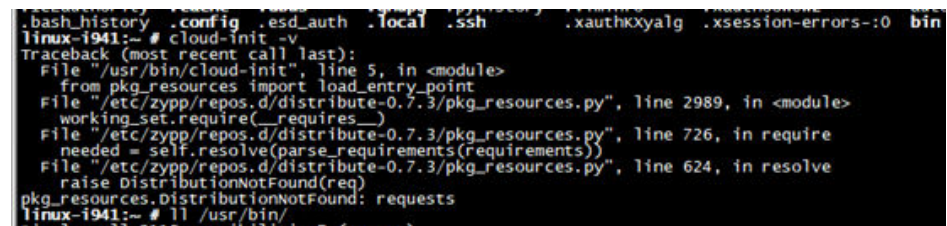
- d. Refresh the SUSE repository.

```
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.



```
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/  
ls: cannot access 'ls': No such file or directory
```

```

100% |████████████████████████████████████████████████████████████████████████████████| 1.3MB 60kB/s
Collecting wheel
  Downloading https://files.pythonhosted.org/packages/1b/d2/22cde5ea9af055f81814f9f2545f5ed8a053eb749c08d186b369959189a8/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-i941:~ # pip -V
pip 10.0.1 from /usr/lib/python2.7/site-packages/pip (python 2.7)
linux-i941:~ #

```

`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 - DataSourceMware.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)
  --More--
ecs-suse-cloud:~ # cd /home/
ecs-suse-cloud:/home #
ecs-suse-cloud:/home # ls
sles_socket-tool user.txt
ecs-suse-cloud:/home #
ecs-suse-cloud:/home #

```

- j. Check the Cloud-Init version and whether Cloud-Init is running properly.
- ```

cloud-init -v
cloud-init init --local

```

## Configure Cloud-Init

1. Enable SSH authentication and remote password login for user **root**.

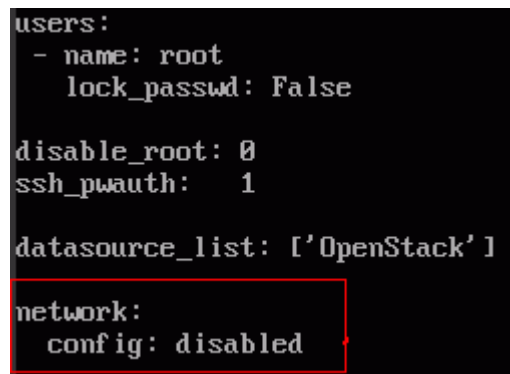
Take CentOS 6.7 as an example. If **disable\_root** in the **/etc/cloud/cloud.cfg** file is **0**, **root** login is enabled. (In some OSs, **true** indicates disabled and **false** indicates enabled). Set **ssh\_pwauth** to **1** (indicating remote password login is enabled) and **lock\_passwd** to **False** (indicating that user passwords are not locked).

```
users:
- name: root
  lock_passwd: False

disable_root: 0
ssh_pwauth: 1
```

**NOTE**

- If you inject a password, use it for remote login through SSH or noVNC.
  - If you inject a key, use it for remote login through SSH.
2. Modify the **/etc/cloud/cloud.cfg** file to disable Cloud-Init's network configuration capability.  
If the Cloud-Init version is 0.7.9 or later, add the following content to **/etc/cloud/cloud.cfg**:

**Figure 3-16** Disabling Cloud-Init's network configuration capability

```
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 YAML format.

3. Enable the agent to access the IaaS OpenStack data source.  
Add the following content 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 for reference only.
  - 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 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.
4. 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 VM startup.

**Figure 3-17** 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
```

5. Run `vi /etc/ssh/sshd_config` 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

6. 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
```

7. Modify the configuration so that the hostname of the ECSs created from the image does not contain the **.novalocal** suffix and can contain a dot (.).

- a. 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
#return "%s.%s" % (hostname, domain) # Comment out 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. Go to the **cloudinit/sources** directory.

```
cd /usr/lib/python*/site-packages/cloudinit/sources/
```

The Python version varies depending on the OS.

- c. Delete the **\_\_init\_\_.pyc** file and the optimized and compiled **\_\_init\_\_.pyo** file.

```
rm -rf __init__.pyc
```

```
rm -rf __init__.pyo
```

- d. Clear logs.

```
rm -rf /var/lib/cloud/*
```

```
rm -rf /var/log/cloud-init*
```

Delete all files except log-related configuration files from the **/etc/cloud/cloud.cfg.d/** directory.

8. Modify 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
```

9. Delete user **linux** and the **/home/linux** directory from the image template.

```
userdel linux
```

```
rm -fr /home/linux
```

10. Ensure that Cloud-Init is enabled.

If the **/etc/cloud/cloud-init.disabled** file exists, run **cloud-init clean --machine-id**. If there is no such a file, skip this step.

## Check the Cloud-Init Configuration

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) Set the password validity period of a system user to the maximum.

**chage -M 99999 \$user\_name**

*user\_name* is a system user, for example **root**.

You are advised to set the password validity period to **99999**.

## (Optional) Install the One-Click Password Reset Plug-In

To ensure that you can reset the password of each ECS created from the image with a few clicks, you are advised to install the one-click password reset plug-in (CloudResetPwdAgent) on the VM that is used as the image source.

1. Download the CloudResetPwdAgent (one-click password reset plug-in) package.

 NOTE

The one-click password reset plug-in can be automatically updated only if an EIP is bound to the VM.

You can download the **CloudResetPwdAgent.zip** package from:

For 32-bit OSs: [http://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/32/reset\\_pwd\\_agent/CloudResetPwdAgent.zip](http://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip)

For 64-bit OSs: [http://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/64/reset\\_pwd\\_agent/CloudResetPwdAgent.zip](http://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip)

2. Decompress **CloudResetPwdAgent.zip**.

**unzip -o -d output-directory CloudResetPwdAgent.zip**

There is no special requirement for the directory that stores the decompressed **CloudResetPwdAgent.zip**. You can choose a directory as you need. If the directory is **/home/PwdAgent/test**, the command is as follows:

**unzip -o -d /home/PwdAgent/test CloudResetPwdAgent.zip**

3. Install the one-click password reset plug-in.

- a. Open the **CloudResetPwdAgent.Linux** file.

**cd CloudResetPwdAgent/CloudResetPwdAgent.Linux**

- b. Add the execute permission for the **setup.sh** file.

**chmod +x setup.sh**

- c. Install the plug-in.

**sudo sh setup.sh**

If "cloudResetPwdAgent install successfully" is displayed and "Failed to start service cloudResetPwdAgent" is not displayed, the installation is successful.

 NOTE

If the installation failed, check whether the installation environment meets the requirements and install the plug-in again.

## Configure NetworkManager

Linux allows you to use NetworkManager to automatically configure the VM network. You are advised to use NetworkManager for new OS versions. Alternatively, you can use the native network service of the OS.

### Red Hat, Oracle, CentOS 6.x, CentOS 7.x, EulerOS 2.x, Fedora 22, or Later

Install NetworkManager and use it for automatic network configuration.

1. Install NetworkManager.  
**yum install NetworkManager**
2. Delete **ifcfg-eth1** to **ifcfg-eth11** from the **/etc/sysconfig/network-scripts/** directory and retain only **ifcfg-eth0**.
3. Disable the network service.  
**service network stop**
4. Disable automatic startup of the network service.  
**chkconfig network off**
5. Restart MessageBus and NetworkManager and enable NetworkManager to start automatically at system startup.  
**service messagebus restart**  
**service NetworkManager restart**  
**chkconfig NetworkManager on**

### Debian 9.0 or Later

Install NetworkManager and use it for automatic network configuration.

1. Install NetworkManager.  
**apt-get install network-manager**
2. In the **/etc/NetworkManager/NetworkManager.conf** file, change the value of **managed** to **true**.
3. Modify **/etc/network/interfaces** and retain only **eth0**.
4. Disable the network service, restart MessageBus and NetworkManager, and enable NetworkManager to start automatically at system startup.  
**service network-manager restart**  
**chkconfig network-manager on**  
**service networking stop**  
**service messagebus restart**  
**service network-manager restart**

### Ubuntu 14 or Later

Install NetworkManager and use it for automatic network configuration.

1. Install NetworkManager.  
**apt-get install network-manager**

2. In the `/etc/NetworkManager/NetworkManager.conf` file, change the value of **managed** to **true**.
3. Modify `/etc/network/interfaces` and retain only **eth0**.
4. Disable the network service.  
**service networking stop**
5. Disable automatic startup of the network service.  
**chkconfig network off**
6. Restart D-Bus and NetworkManager.  
**service dbus restart**  
**service network-manager restart**

## SUSE 11 SP3 and openSUSE 13 or Later

Install NetworkManager and use it for automatic network configuration.

1. Delete **ifcfg-eth1** to **ifcfg-eth11** from the `/etc/sysconfig/network-scripts/` directory and retain only **ifcfg-eth0**.
2. Install NetworkManager.  
**zypper install NetworkManager**
3. Start YaST, choose **Network Devices** in the navigation pane on the left, and select **Network Settings** in the right pane. In the **Network Setup Method** area of the **Global Options** page, change **Traditional Method with ifup** to **User Controlled with NetworkManager**.

## 3.5 Obtaining the Image File

After the VM is configured, perform the following operations to generate and export a Linux image file:

1. Open VirtualBox, select the VM, choose **Settings > Storage**, and select **Linux.vhd**.  
**Linux** is the VM name.
2. In the right pane, view the image file location.
3. Go to the location to obtain the generated **Linux.vhd** image file.

## 3.6 Registering the Image File as a Private Image

Upload the image file to an OBS bucket and register it as a private image.

### Constraints

- Only an unencrypted image file or an image file encrypted using SSE-KMS can be uploaded to an OBS bucket.
- When uploading an image file, you must select an OBS bucket with the storage class of Standard.

## Procedure

1. Use OBS Browser+ to upload the image file. For details, see [OBS Browser+ Best Practices](#).

For how to download OBS Browser+, see [https://support.huaweicloud.com/intl/en-us/browsertg-obs/obs\\_03\\_1003.html](https://support.huaweicloud.com/intl/en-us/browsertg-obs/obs_03_1003.html).

2. Register the image file as a private image. For details, see [Registering an Image File as a Private Image](#).

# 4 Creating a Private Image Using Packer

Packer is an open-source tool for creating custom images. Packer's behavior is determined by a template which is a HashiCorp Configuration Language (HCL2) or JSON file and mainly contains three component types: builder, provisioner, and post-processor. These components can be flexibly combined in the template to automatically create image files for multiple cloud platforms in parallel. Packer simplifies private image creation by using manageable code. It enables you to flexibly customize images and easily use identical images between different cloud platforms.

This section describes how to use Packer to create an Ubuntu 22.04 Server 64-bit private image on a CentOS 8.2 64-bit ECS.

## Constraints

Full-ECS images cannot be used as an image source when you use Packer to create private images.

## Procedure



## Install Packer

1. Log in to the management console, create an ECS (for example, an ECS running CentOS 8.2 64-bit), and bind an EIP to the ECS.
2. Log in to the ECS.
3. Visit <https://www.packer.io/downloads> and download the latest version of Packer that matches the ECS OS and architecture.
4. Install Packer (**packer\_1.9.1\_linux\_amd64.zip** as an example).  
**wget --no-check-certificate https://releases.hashicorp.com/packer/1.9.1/packer\_1.9.1\_linux\_amd64.zip**

 NOTE

- Ensure that you have bound an EIP to the ECS so that the ECS can access the Internet.
  - If the message "command not found" is displayed, the wget tool is not installed. Run **yum install wget** to install it.
5. Decompress the Packer package.  
**unzip packer\_1.9.1\_linux\_amd64.zip**
6. Move the Packer package to the **/usr/local/bin** directory.  
**mv packer /usr/local/bin**

 NOTE

- The **/usr/local/bin** directory has been added to environment variables. You can also move the Packer package to other directory that has been added to environment variables.
7. Check whether Packer is installed.  
**packer -v**
- If the Packer version number is returned, Packer is installed successfully.
  - If "command not found" is displayed, the Packer installation failed. Check whether the directory where Packer resides has been added to environment variables.

 NOTE

Run **env | grep PATH** to check whether the environment variable **PATH** contains the Packer installation directory.

If **PATH** does not contain the Packer installation directory, perform the following operations to add it to **PATH**:

1. Open the **profile** file.  
**vim /etc/profile**
2. Press **i** to enter the editing mode and add **export PATH=\$PATH:/usr/local/bin** to the end of the file.  
If your Packer resides in a directory other than **/usr/local/bin**, replace **/usr/local/bin** in the command with the actual directory.
3. Press **Esc** to exit the editing mode. Enter **:wq** and press **Enter** to save the changes and exit.
4. Run the following command to make the change take effect:  
**source /etc/profile**

## Create a Packer Template

To create an image using Packer, you need a template in .pkr.hcl format. In the template, you need to configure **builders**, **provisioners**, and post-processors. In a provisioner, you can modify the source image as you need. For example, you can modify the configurations and specify the software to be pre-installed. In this example, a post-processor is used to redirect the output path of manifest. If your Packer template has multiple builders, you can locate the ID of the image created by each builder based on the manifest output. For more information about builders, provisioners, and post-processors, see the [Packer official documentation](#).

This section takes a Shell provisioner as an example.

1. Create a **hwcloud.pkr.hcl** file:  
**touch hwcloud.pkr.hcl**
2. Open the **hwcloud.pkr.hcl** file.  
**vim hwcloud.pkr.hcl**
3. Press **i** to enter the editing mode and edit the template as needed. For parameter details, see [Table 4-1](#). The following content is for reference only.

```
packer {
  required_plugins {
    huaweicloud = {
      version = ">= 1.0.0"
      source  = "github.com/huaweicloud/huaweicloud"
    }
  }
}

source "huaweicloud-ecs" "artifact" {
  region          = "xxx"
  availability_zone = "xxx"
  flavor          = "c6.large.2"
  source_image_name = "Ubuntu 22.04 server 64bit"
  image_name       = "Ubuntu-2204-image-powered-by-Packer"
  image_tags = {
    builder = "packer"
    os      = "Ubuntu-22.04-server"
  }

  ssh_username = "root"
  eip_type      = "5_bgp"
  eip_bandwidth_size = 5
}

build {
  sources = ["source.huaweicloud-ecs.artifact"]

  provisioner "shell" {
    inline = ["apt-get update -y"]
  }

  post-processor "manifest" {
    strip_path = true
    output     = "packer-result.json"
  }
}
```

 **NOTE**

In [Table 4-1](#), **region**, **availability\_zone**, **flavor**, and **source\_image\_name** are the attributes of the generated temporary ECS from which the private image will be created.

**Table 4-1** Packer template parameters

| Parameter  | Description                                                                      | Mandatory |
|------------|----------------------------------------------------------------------------------|-----------|
| region     | Region name. Obtain the region name from <a href="#">Regions and Endpoints</a> . | Yes       |
| flavor     | Flavor of the temporary ECS.                                                     | Yes       |
| image_name | Name of the private image to be created.                                         | Yes       |

| Parameter          | Description                                                                                                                                                                                                                                                                                                                                        | Mandatory |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| image_tags         | Tags of the private image to be created.                                                                                                                                                                                                                                                                                                           | No        |
| availability_zone  | AZ. Obtain the AZ from <a href="#">Regions and Endpoints</a> .                                                                                                                                                                                                                                                                                     | No        |
| source_image_name  | Name of the source image. This image is used to create the temporary ECS mentioned above. You can obtain the source image name from the public image list on the IMS console.<br><b>NOTE</b><br>To specify a source image, you can also use <b>source_image</b> to specify an image ID or use <b>source_image_filter</b> to filter a source image. | No        |
| ssh_username       | SSH login username of the private image to be created.<br>This parameter is mandatory for SSH login.                                                                                                                                                                                                                                               | No        |
| eip_type           | EIP line type.                                                                                                                                                                                                                                                                                                                                     | No        |
| eip_bandwidth_size | EIP bandwidth (Mbit/s). This parameter is mandatory if access to the Internet is required.<br><b>NOTE</b><br><b>eip_type</b> and <b>eip_bandwidth_size</b> are configured to create a new EIP. To use an existing EIP, configure <b>reuse_ips</b> and <b>floating_ip</b> .                                                                         | No        |
| provisioner        | Provisioner type. For details, see <a href="#">Packer Provisioners</a> .                                                                                                                                                                                                                                                                           | Yes       |
| post-processor     | Post-processor type.                                                                                                                                                                                                                                                                                                                               | No        |

 **NOTE**

For more parameters, see <https://github.com/huaweicloud/packer-plugin-huaweicloud/wiki>.

## Create a Private Image Using Packer

1. After the Packer template is created, import AK and SK.  
export HW\_ACCESS\_KEY=<AccessKey ID>  
export HW\_SECRET\_KEY=<AccessKey Secret>
2. Use Packer to create an image.  
**packer build hwcloud.pkr.hcl**

```
huaweicloud-ecs.artifact: output will be in this color.

==> huaweicloud-ecs.artifact: Loading availability zones...
    huaweicloud-ecs.artifact: the specified availability_zone ap-southeast-1a is available
==> huaweicloud-ecs.artifact: Loading flavor: c6.large.2
==> huaweicloud-ecs.artifact: Creating temporary keypair: packer_64abc4fd-xxxx-xxxx-xxxx-2139eee76819...
==> huaweicloud-ecs.artifact: Created temporary keypair: packer_64abc4fd-xxxx-xxxx-xxxx-2139eee76819
    huaweicloud-ecs.artifact: Found Image ID: 19d9079e-xxxx-xxxx-xxxx-642116ad6557
==> huaweicloud-ecs.artifact: Creating temporary VPC...
    huaweicloud-ecs.artifact: temporary VPC ID: 6e309adc-xxxx-xxxx-xxxx-4c3356b972c7
==> huaweicloud-ecs.artifact: Creating temporary subnet...
    huaweicloud-ecs.artifact: temporary subnet ID: 66ab3bc3-xxxx-xxxx-xxxx-d8ca2d9378cc
    huaweicloud-ecs.artifact: the [default] security groups will be used ...
==> huaweicloud-ecs.artifact: Creating EIP ...
    huaweicloud-ecs.artifact: Created EIP: '0cd696e3-xxxx-xxxx-xxxx-220b8d277604' (159.xxx.xxx.180)
==> huaweicloud-ecs.artifact: Launching server in AZ ap-southeast-1a...
    huaweicloud-ecs.artifact: Waiting for server to become ready...
    huaweicloud-ecs.artifact: Server ID: 13f78f88-xxxx-xxxx-xxxx-7e8c27a9ad1f
==> huaweicloud-ecs.artifact: Using SSH communicator to connect: 159.138.141.180
==> huaweicloud-ecs.artifact: Waiting for SSH to become available...
==> huaweicloud-ecs.artifact: Connected to SSH!
==> huaweicloud-ecs.artifact: Provisioning with shell script: /tmp/packer-shell2456008753
huaweicloud-ecs.artifact: Hit:1 http://repo.huaweicloud.com/ubuntu jammy InRelease

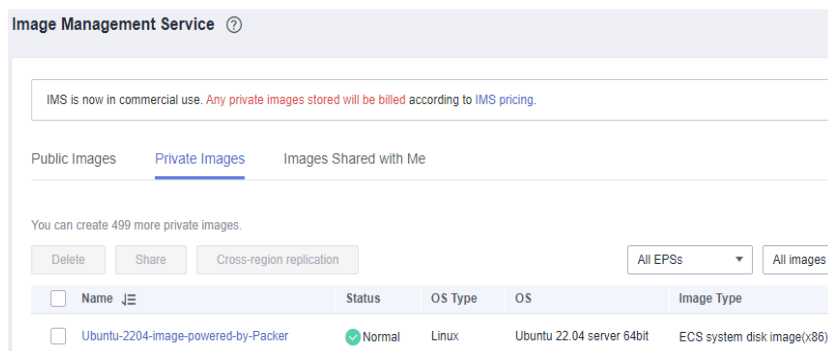
.....
    huaweicloud-ecs.artifact: Fetched 5,536 kB in 3s (2,006 kB/s)
    huaweicloud-ecs.artifact: Reading package lists...
==> huaweicloud-ecs.artifact: Stopping server: 13f78f88-xxxx-xxxx-xxxx-7e8c27a9ad1f ...
    huaweicloud-ecs.artifact: Waiting for server to stop: 13f78f88-xxxx-xxxx-xxxx-7e8c27a9ad1f ...
==> huaweicloud-ecs.artifact: Creating the system image: Ubuntu-2204-image-powered-by-Packer ...
    huaweicloud-ecs.artifact: Image: 62dc6e37-xxxx-xxxx-xxxx-a2a00a677f5b
==> huaweicloud-ecs.artifact: Terminating the source server: 13f78f88-xxxx-xxxx-xxxx-7e8c27a9ad1f...
==> huaweicloud-ecs.artifact: Deleted temporary public IP '0cd696e3-xxx-xxxx-xxxx-220b8d277604' (159.xxx.xxx.180)
==> huaweicloud-ecs.artifact: Deleting temporary subnet: 66ab3bc3-xxxx-xxxx-xxxx-d8ca2d9378cc...
==> huaweicloud-ecs.artifact: Deleting temporary VPC: 6e309adc-xxxx-xxxx-xxxx-4c3356b972c7...
==> huaweicloud-ecs.artifact: Deleting temporary keypair: packer_64abc4fd-xxxx-xxxx-xxxx-2139eee76819 ...
==> huaweicloud-ecs.artifact: Running post-processor: (type manifest)
Build 'huaweicloud-ecs.artifact' finished after 5 minutes 48 seconds.

==> Wait completed after 5 minutes 48 seconds

==> Builds finished. The artifacts of successful builds are:
--> huaweicloud-ecs.artifact: An image was created: 62dc6e37-xxxx-xxxx-xxxx-a2a00a677f5b
```

3. Log in to the management console and click **Image Management Service** under **Compute**.
4. Click the **Private Images** tab and view the image created using Packer. [Figure 4-1](#) shows the created image.

**Figure 4-1** Viewing the private image created using Packer



## Helpful Links

Packer official guide: <https://www.packer.io/intro/getting-started/install.html>

# 5 Cleaning Up the Disk Space of a Windows ECS

---

## Scenarios

To clean up the disk space of a Windows ECS, you need to perform the following operations.

### Disable Virtual Memory

Some disk space of an ECS serves as virtual memory which can be used when the ECS memory is exhausted. However, when the memory usage is high, frequent switching between the memory and virtual memory causes a large number of extra I/Os, deteriorating the I/O performance. You can disable virtual memory to free up disk space on Windows.

An ECS running Windows Server 2008 R2 Standard 64-bit is used as an example to describe how to disable virtual memory.

1. Right-click the **Computer** icon and choose **Properties**. In the displayed window, click **Advanced System Settings**.
2. In the **System Properties** dialog box, click the **Advanced** tab.
3. Click **Settings** in the **Performance** area.
4. In the displayed **Performance Options** dialog box, click the **Advanced** tab and then **Change**. The **Virtual Memory** dialog box is displayed.
5. Delete virtual memory.

In the **Virtual Memory** dialog box, deselect **Automatically manage paging file size for all drives**, select the paging file of the disk whose virtual memory is to be deleted, select **No paging file**, and click **Set**.

 **CAUTION**

If the warning "If you disable the paging file or set the initial size to less than xxx megabytes and a system error occurs, Windows might not record details that could help identify the problem. Do you want to continue?" is displayed, set the initial size to xxx shown in the warning. The partition for storing paging files must have sufficient space. If the disk resources are insufficient, virtual memory will be insufficient. You only need to set virtual memory in one partition of the ECS.

6. Choose **Start > Control Panel > Appearance and Personalization > Show hidden files and folders**. The **Folder Options** dialog box is displayed. Click the **View** tab, deselect **Hide protected operating system files (Recommended)**, and select **Show hidden files, folders, and drives**. When you deselect **Hide protected operating system files (Recommended)**, a warning is displayed, as shown in [Figure 5-1](#). Click **Yes** and then click **Apply**.

**Figure 5-1** Warning

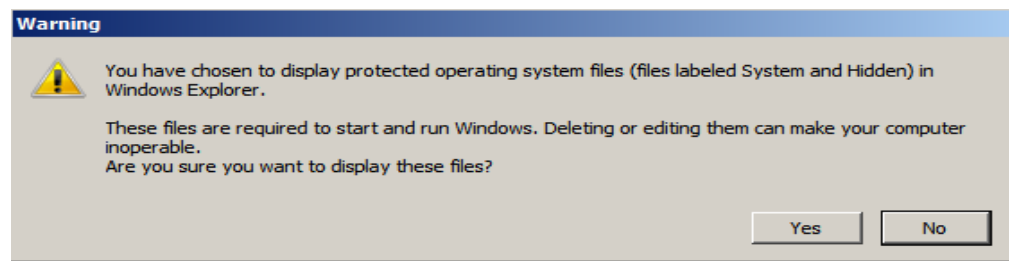
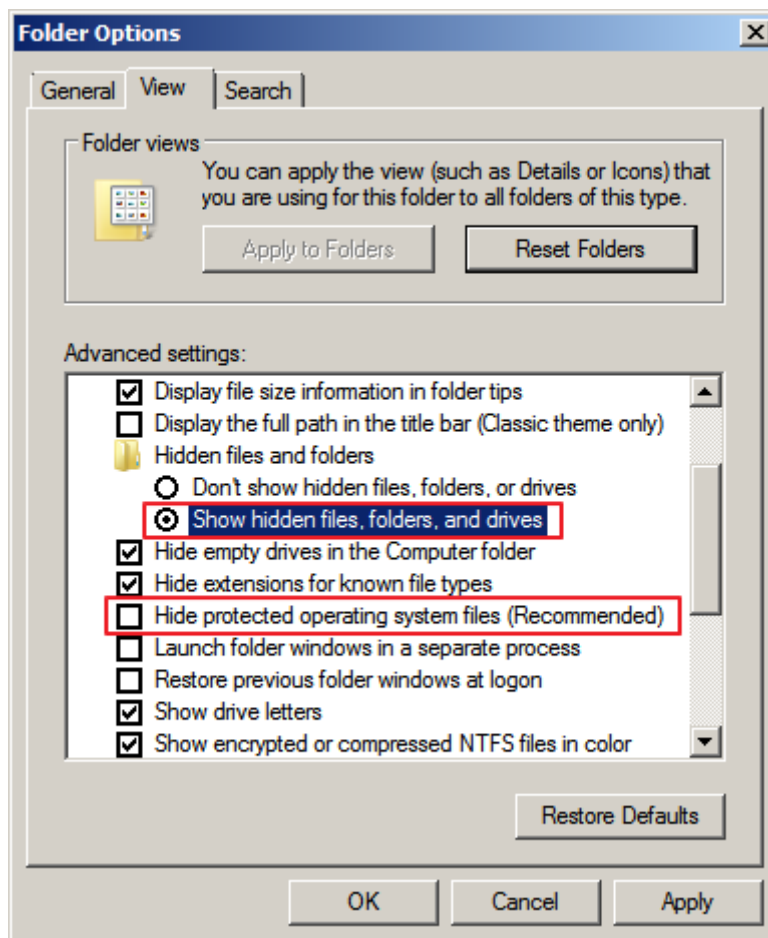


Figure 5-2 Showing hidden files



7. After file hiding is disabled, delete the hidden file **pagefile.sys** from disk C. After the OS is restarted, the available space increases.

## Disable Hibernation

An ECS running Windows Server 2008 R2 Standard 64-bit is used as an example to describe how to disable hibernation.

Method 1: Delete the **Hiberfil.sys** file.

The **Hiberfil.sys** file is generated by Windows hibernation and occupies large system disk space. It saves memory data and sessions to disks so that the memory image file required by sessions can be quickly restored after the computer is restarted. Perform the following steps to delete the **Hiberfil.sys** file to free up some disk space:

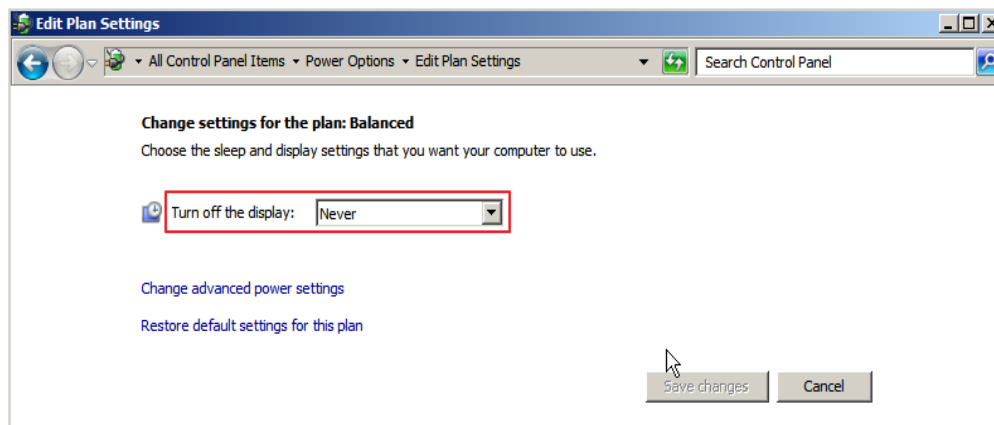
1. Run **cmd.exe** as an administrator to open the command line interface (CLI).
2. Run the following command to disable hibernation (the **Hiberfil.sys** file will be automatically deleted):

**powercfg -h off**

Method 2: Disable hibernation.

1. Choose **Start > Control Panel > Appearance and Personalization > Personalization > Change screen saver** and click **Change power settings**.

2. In the **Power Options** window, click **Change plan settings** on the right of **Balanced (recommended)**.
3. Set **Turn off the display** to **Never**.

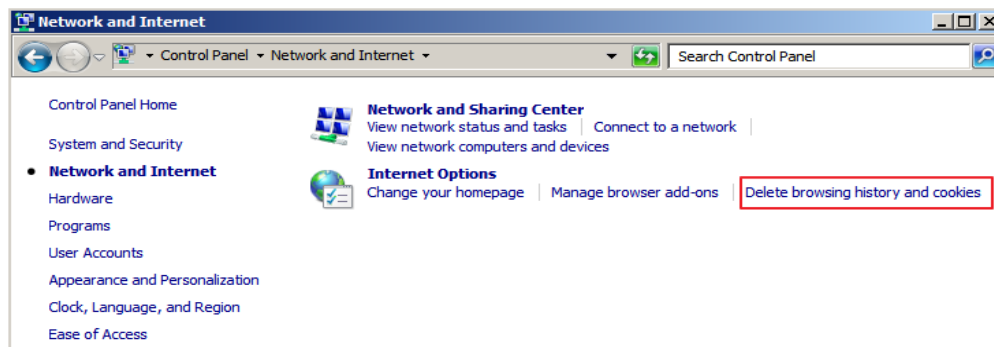


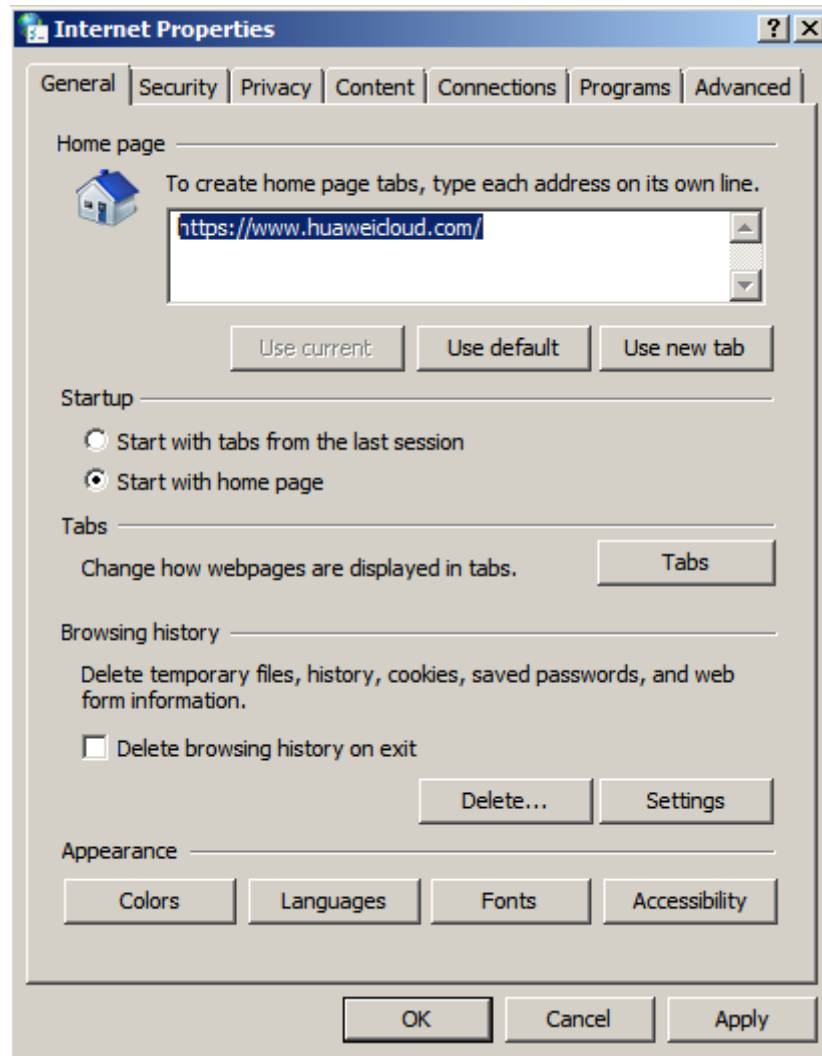
## Delete Internet Explorer Temporary Files

An ECS running Windows Server 2008 R2 Standard 64bit is used as an example to describe how to delete temporary files generated by Internet Explorer.

Internet Explorer stores all information about Internet access in a specified folder, including Internet Explorer cache files, cookies files, browsing history, visited websites, URLs in the address bar, and Internet Explorer forms/passwords. Perform the following steps to delete temporary files generated by Internet Explorer:


1. Choose **Start > Control Panel > Network and Internet > Internet Options**. Click **Delete browsing history and cookies** to delete cookies and temporary files of Internet Explorer.





2. After the preceding step is performed, there may be residual files or records left. Open the **C:\Windows\temp** and **C:\Users\Username\AppData\Local\Temp** folders and delete all files from them. (The folders store visited websites and other temporary data.)

 C:\Windows\Temp

 C:\Users\Administrator\AppData\Local\Temp

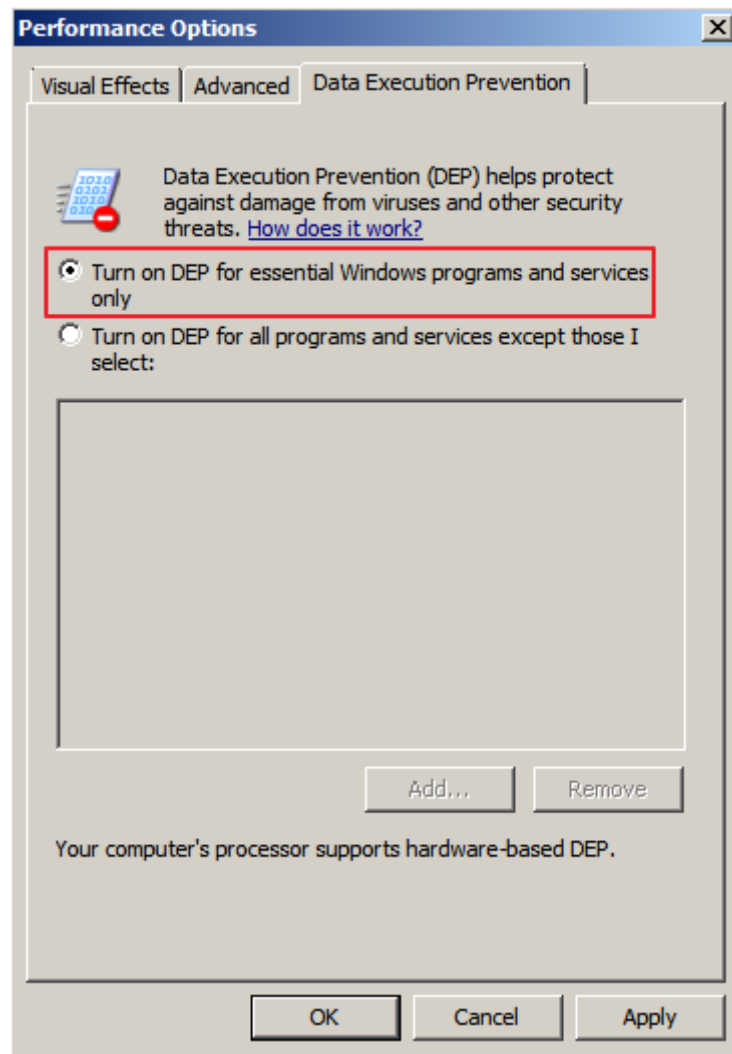
## Disable Data Execution Prevention (DEP)

DEP reserves a part of ECS memory for temporarily storing application data and another part of memory for temporarily storing application instructions. This protects ECSs from viruses and other security threats.

An ECS running Windows Server 2008 R2 Standard 64-bit is used as an example to describe how to disable DEP.

1. Right-click the **Computer** icon and choose **Properties**. In the displayed window, click **Advanced System Settings**.
2. In the **System Properties** dialog box, click the **Advanced** tab.

3. Click **Settings** in the **Performance** area.
4. In the **Performance Options** dialog box, click the **Data Execution Prevention** tab, select **Turn on DEP for essential Windows programs and services only**, and click **Apply**.



## Delete Redundant Application Files

The **C:\Windows\prefetch** folder stores the index files generated by applications. The files are used to improve system performance and speed up system startup and file reading. However, the number of files increases with time. Deleting redundant files can free up disk space on Windows.

Delete all files from the **C:\Windows\prefetch** folder to delete redundant application files.

## Clean Up Disks

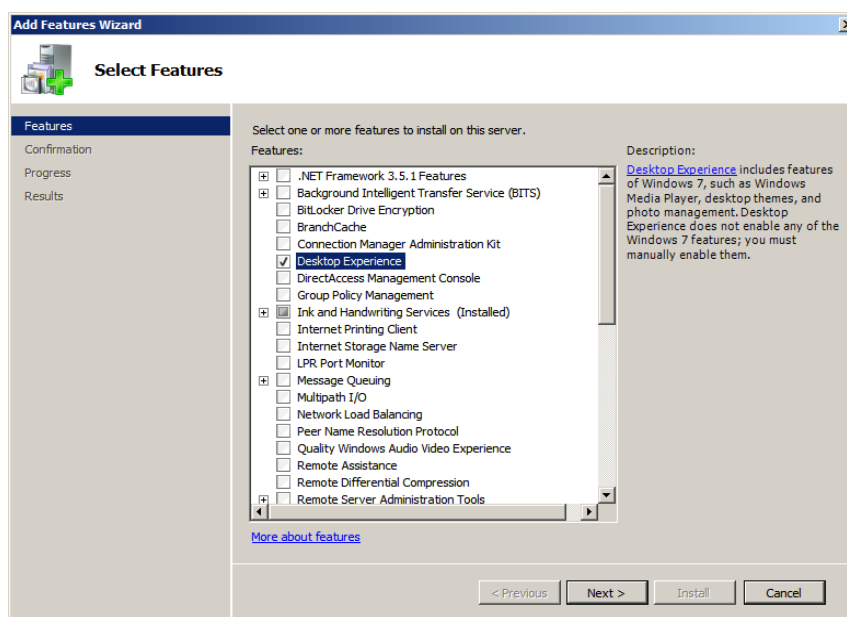
You can use **Disk Cleanup** of ECSs to delete temporary files, empty the recycle bin, and delete redundant system files and other files.

On the ECS, click **Start**. In the search box, enter **Disk Cleanup**. Click the displayed **Disk Cleanup** to scan for the space that can be freed up. After the scan is complete, confirm the files to be deleted and click **OK** to start disk cleanup.

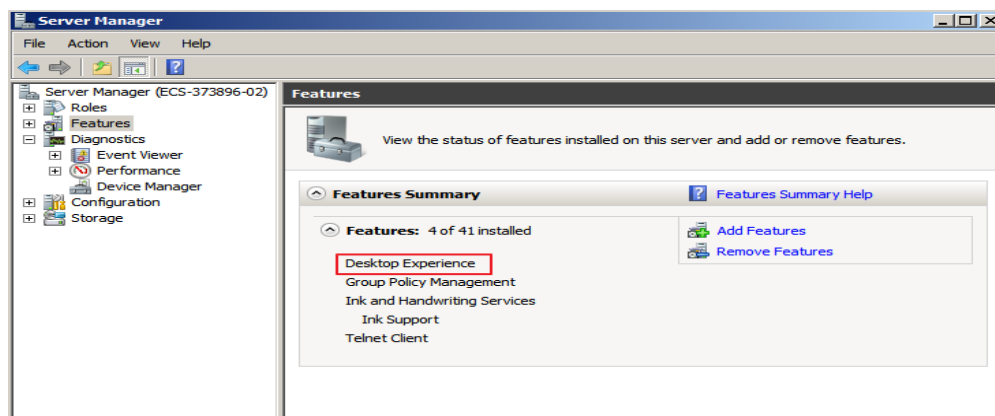
If **Disk Cleanup** is unavailable, you need to install Desktop Experience first. An ECS running Windows Server 2008 R2 Standard 64bit is used as an example to describe how to install Desktop Experience.

1. Choose **Start > All Programs > Administrative Tools > Server Manager**. In the navigation pane, click **Features**.
2. Click **Add Features**.
3. In the **Select Features** dialog box, select **Desktop Experience** and click **Next**.

**Figure 5-3** Installing Desktop Experience



4. In the **Confirm Installation Selections** dialog box, confirm the installation of Desktop Experience, and click **Install**.
5. When the installation progress reaches 100% in the **Results** dialog box, the system prompts you to restart the server. Click **Close**, and then click **Yes** to restart the server.
6. After the server is restarted, start the server manager. In the **Function Summary** area, check whether Desktop Experience is installed.

**Figure 5-4** Successful installation of Desktop Experience

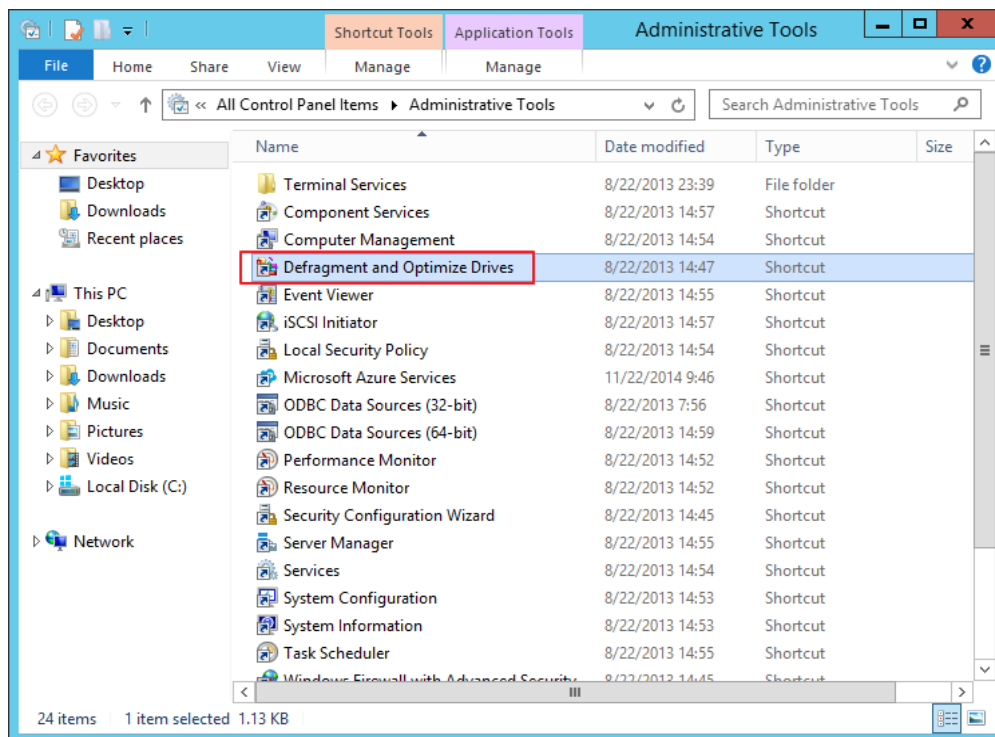
7. Choose **Start > All Programs > Accessories > System Tools > Disk Cleanup** to start the disk cleanup tool.

## Defragment and Optimize Drives

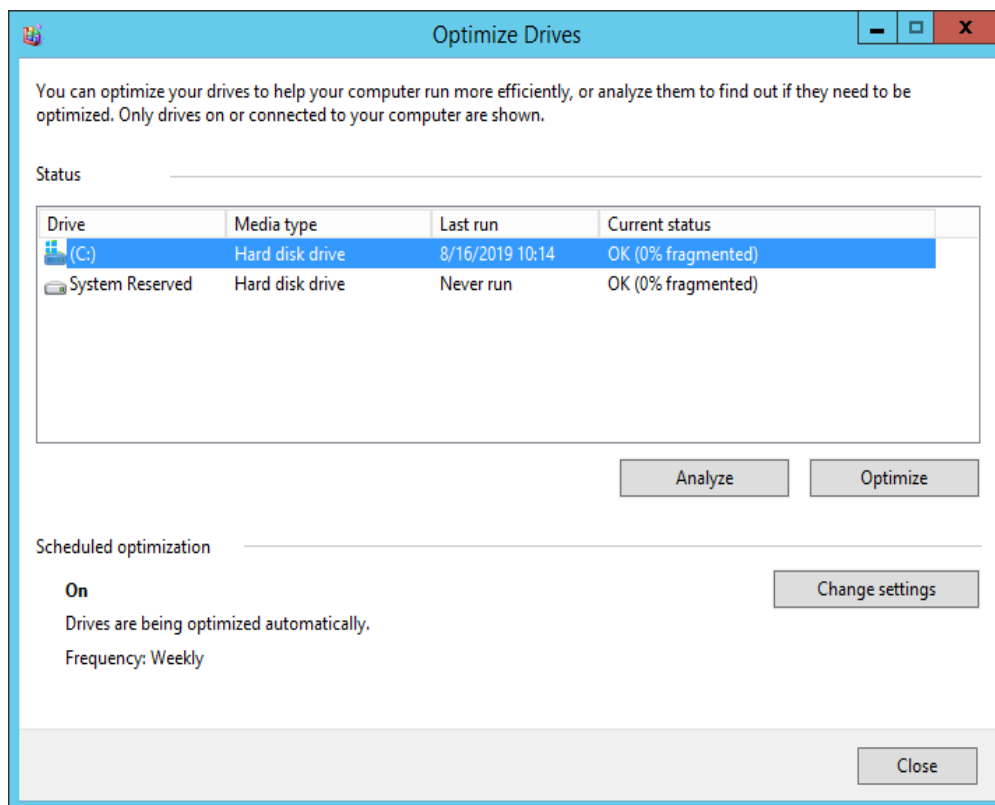
Disk defragmentation is a process in which system software or professional disk defragmentation software is used to organize the fragments generated during the long-term use of disks into the smallest number of contiguous fragments, improving the performance and speed of the server.

An ECS running Windows Server 2012 R2 Datacenter 64bit is used as an example to describe how to defragment and optimize drives.

1. Choose **Control Panel > All Control Panel Items > Administrative Tools**, and double-click **Defragment and Optimize Drives**.



2. Select the disk partition to be optimized, and then click **Analyze** to analyze whether the disk partition needs to be optimized. If the analysis result indicates that optimization is necessary, click **Optimize**.



## Delete .dmp Files

When a blue screen of death (BSOD) occurs on a Windows ECS, the system automatically generates a BSOD error file with the suffix .dmp. A .dmp file is a system error file in Windows, such as, **memory.dmp** and **minixxxx.dmp**.

You can manually delete .dmp files from disk C to free up system disk space.

---

### CAUTION

After the .dmp file is deleted, the BSOD cause on the ECS cannot be queried.

---

## Clean Up Component Store

Windows Component Store stores all the files required for installing Windows. Updated installation files are also stored in Component Store, which causes the size of Component Store to increase as the update increases.

An ECS running Windows Server 2012 R2 Datacenter 64-bit is used as an example to describe how to clean up Component Store.

1. In Windows PowerShell, run the following command to delete the backup files generated during the Service Pack installation:

**dism /online /cleanup-image /spsuperseded**

```
PS C:\Users\Administrator> dism /online /cleanup-image /spsuperseded
Deployment Image Servicing and Management tool
Version: 6.3.9600.19408
Image Version: 6.3.9600.19397
Service Pack Cleanup cannot proceed: No Service Pack backup files were found.
The operation completed successfully.
```

2. Check the size of Component Store.

#### **Dism.exe /Online /Cleanup-Image /AnalyzeComponentStore**

```
PS C:\Users\Administrator> Dism.exe /Online /Cleanup-Image /AnalyzeComponentStore
Deployment Image Servicing and Management tool
Version: 6.3.9600.19408
Image Version: 6.3.9600.19397
[=====99.9%=====]
Component Store (WinSxS) information:
Windows Explorer Reported Size of Component Store : 7.90 GB
Actual Size of Component Store : 7.75 GB
    Shared with Windows : 4.12 GB
    Backups and Disabled Features : 3.33 GB
    Cache and Temporary Data : 297.92 MB
Date of Last Cleanup : 2019-08-16 11:00:48
Number of Reclaimable Packages : 3
Component Store Cleanup Recommended : Yes
The operation completed successfully.
```

3. Clean up Component Store.

#### **Dism.exe /online /Cleanup-Image /StartComponentCleanup**

```
PS C:\Users\Administrator> Dism.exe /online /Cleanup-Image /StartComponentCleanup
Deployment Image Servicing and Management tool
Version: 6.3.9600.19408
Image Version: 6.3.9600.19397
[=====100.0%=====]
The operation completed successfully.
PS C:\Users\Administrator> _
```

## Delete System Logs

System logs record hardware and software information, system problems, and system events. You can use the logs to locate error causes or track attacker actions. System logs include application logs, security logs, startup logs, and event forwarding logs. The **System32 > LogFiles** folder on disk C of Windows stores the operation logs and event logs of Windows. Deleting the folder can free up the space of disk C.

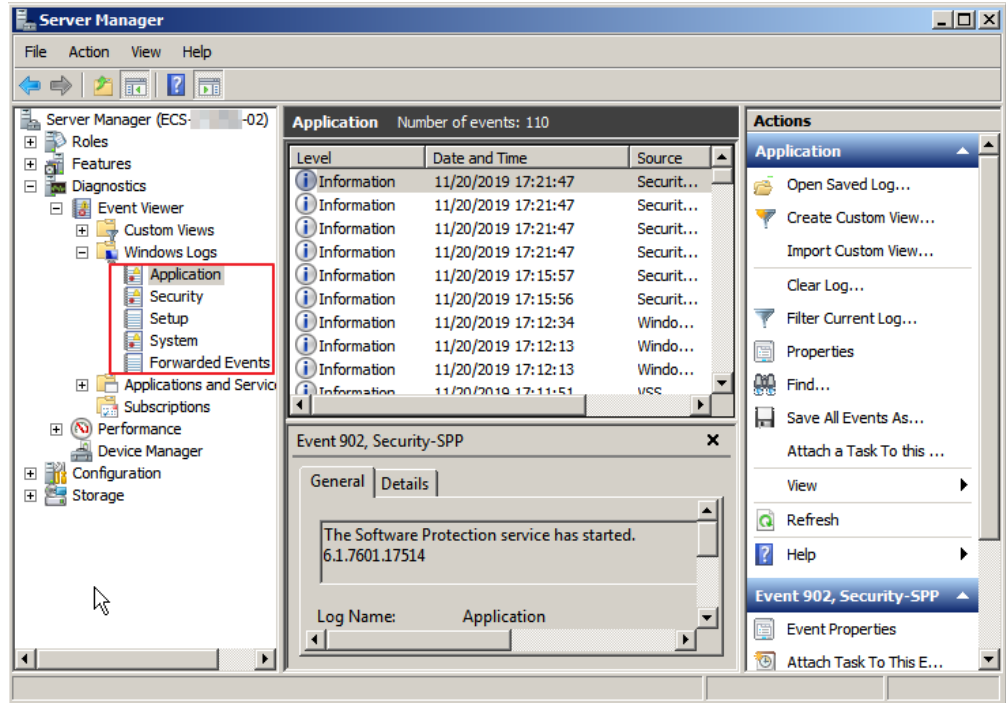
An ECS running Windows Server 2008 R2 Standard 64-bit is used as an example to describe how to delete system logs.

1. Open the **C:\Windows\System32\LogFiles** folder, and delete all the files and folders from it.



C:\Windows\System32\LogFiles

1. Choose **Start**, right-click **Computer**, and choose **Manage** from the shortcut menu.
2. In the displayed window, choose **Diagnostics > Event Viewer > Windows Logs** and delete logs of **Application**, **Security**, **Setup**, **System**, and **Forwarded Events**.



# 6 Converting the Image Format

## 6.1 Converting the Image Format Using qemu-img

### Scenarios

You can import an image file in VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, QED, ZVHD, or ZVHD2 format to Huawei Cloud. Image files in other formats need to be converted before being imported. The open-source tool **qemu-img** is provided for you to convert image file formats.

### Description

This section describes how to convert an image format on a local Windows or Linux PC.

### Tool and Costs

**Table 6-1** Tool and costs

| Tool     | Description                                                                                                                                                                  | Costs |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| qemu-img | <b>qemu-img</b> is an open-source tool for converting image formats.<br>You can obtain it from:<br><a href="https://qemu.weilnetz.de/w64/">https://qemu.weilnetz.de/w64/</a> | Free  |

### Constraints

- **qemu-img** can be used for mutual conversion of image formats VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, and QED.
- ZVHD and ZVHD2 are the cloud's self-developed image file formats and cannot be identified by **qemu-img**. To convert image files to any of the two

formats, use the **qemu-img-hw** tool. For details, see [Converting the Image Format Using qemu-img-hw](#).

- When you run a command to convert the format of VHD image files, replace **vhd** with **vpc**.

For example, to convert a CentOS 6.9 image file from VHD to QCOW2, run the following command:

```
qemu-img convert -p -f vpc -O qcow2 centos6.9.vhd centos6.9.qcow2
```

#### NOTE

If an error occurs, delete **-f vpc**. Then, qemu-img can identify the correct image format.

## Windows

1. Install qemu-img.
  - a. Download the qemu-img package from <https://qemu.weilnetz.de/w64/>.
  - b. Double-click the setup file to install qemu-img in **D:\Program Files\qemu** (an example installation path).
2. Configure environment variables.
  - a. Choose **Start > Computer** and right-click **Properties**.
  - b. Click **Advanced system settings**.
  - c. In the **System Properties** dialog box, click **Advanced > Environment Variables**.
  - d. In the **Environment Variables** dialog box, search for **Path** in the **System Variable** area and click **Edit**. Add **D:\Program Files\qemu** to **Variable Value**. Use semicolons (;) to separate variable values.

#### NOTE

If **Path** does not exist, add it and set its value to **D:\Program Files\qemu**.

- e. Click **OK**.
3. Verify the installation.

Choose **Start > Run**, enter **cmd**, and press **Enter**. In the **cmd** window, enter **qemu-img --help**. If the qemu-img version information is contained in the command output, the installation is successful.
  4. Convert the image format.
    - a. In the **cmd** window, run the following commands to switch to **D:\Program Files\qemu**:  
**d:**  
**cd D:\Program Files\qemu**
    - b. Convert the image file format from VMDK to QCOW2.  
**qemu-img convert -p -f vmdk -O qcow2 centos6.9.vmdk centos6.9.qcow2**  
The parameters are described as follows:
      - **-p** indicates the image conversion progress.

- **-f** indicates the source image format.
- The part following **-O** (which must be in upper case) consists of the required format, source image file, and target image file.

After the conversion is complete, the target image file is displayed in the directory where the source image file is located.

The following information is displayed:

```
# qemu-img convert -p -f vmdk -O qcow2 centos6.9.vmdk centos6.9.qcow2
(100.00/100%)
```

- c. Query details about the converted image file in QCOW2 format.

#### **qemu-img info centos6.9.qcow2**

The following information is displayed:

```
# qemu-img info centos6.9.qcow2
image: centos6.9.qcow2
file format: qcow2
virtual size: 1.0G (1073741824 bytes)
disk size: 200K
cluster_size: 65536
Format specific information:
  compat: 1.1
  lazy refcounts: false
```

## Linux

### NOTE

If any error occurs, see "Appendix 2: Common qemu-img-hw Errors" in [Converting the Image Format Using qemu-img-hw](#).

1. Install qemu-img.
  - For Ubuntu or Debian, run the following command:  
**apt install qemu-img**
  - For CentOS, Red Hat, or Oracle, run the following command:  
**yum install qemu-img**
  - For SUSE or openSUSE, run the following command:  
**zypper install qemu-img**

2. Check whether the installation is successful.

#### **qemu-img -v**

If the version information and help manual of the qemu-img tool are contained in the command output, the installation is successful. If CentOS 7 is used, the command output is as follows:

```
[root@CentOS7 ~]# qemu-img -v
qemu-img version 1.5.3, Copyright (c) 2004-2008 Fabrice Bellard
usage: qemu-img command [command options]
QEMU disk image utility

Command syntax:
check [-q] [-f fmt] [--output=ofmt] [-r [leaks | all]] [-T src_cache] filename
create [-q] [-f fmt] [-o options] filename [size]
commit [-q] [-f fmt] [-t cache] filename
compare [-f fmt] [-F fmt] [-T src_cache]
```

3. Convert the image format. For example, convert the format of an image file from VMDK to QCOW2 in CentOS 7.

- a. Convert the image file format to QCOW2.

```
qemu-img convert -p -f vmdk -O qcow2 centos6.9.vmdk  
centos6.9.qcow2
```

The parameters are described as follows:

- **-p**: indicates the conversion progress.
- **-f** indicates the source image format.
- The part following **-O** (which must be in upper case) consists of the required image format, source image file, and target image file.

After the conversion is complete, the target image file is displayed in the directory where the source image file is located.

The following information is displayed:

```
[root@CentOS7 home]# qemu-img convert -p -f vmdk -O qcow2 centos6.9.vmdk  
centos6.9.qcow2  
(100.00/100%)
```

- b. Query details about the converted image file in QCOW2 format.

```
qemu-img info centos6.9.qcow2
```

The following information is displayed:

```
[root@CentOS7 home]# qemu-img info centos6.9.qcow2  
image: centos6.9.qcow2  
file format: qcow2  
virtual size: 1.0G (1073741824 bytes)  
disk size: 200K  
cluster_size: 65536  
Format specific information:  
  compat: 1.1  
  lazy refcounts: false
```

## Examples

- Scenario

A pre-allocated image depends on two files: **xxxx.vmdk** (configuration file) and **xxxx-flat.vmdk** (data file) and cannot be directly imported to the cloud platform. When you export a pre-allocated image in VMDK monolithic flat format from the VMware platform, you must convert its format to common VMDK or QCOW2 before it can be imported to the cloud platform.

The following uses the files **centos6.9-64bit-flat.vmdk** and **centos6.9-64bit.vmdk** as an example to describe how to use **qemu-img** to convert image formats.

- Procedure

1. Query image file details.

```
ls -lh centos6.9-64bit*
```

```
qemu-img info centos6.9-64bit.vmdk
```

```
qemu-img info centos6.9-64bit-flat.vmdk
```

The following information is displayed:

```
[root@CentOS7 tmp]# ls -lh centos6.9-64bit*  
-rw-r--r--. 1 root root 10G Jun 13 05:30 centos6.9-64bit-flat.vmdk  
-rw-r--r--. 1 root root 327 Jun 13 05:30 centos6.9-64bit.vmdk  
[root@CentOS7 tmp]# qemu-img info centos6.9-64bit.vmdk  
image: centos6.9-64bit.vmdk
```

```
file format: vmdk
virtual size: 10G (10737418240 bytes)
disk size: 4.0K
Format specific information:
  cid: 3302005459
  parent cid: 4294967295
  create type: monolithicFlat
  extents:
    [0]:
      virtual size: 10737418240
      filename: centos6.9-64bit-flat.vmdk
      format: FLAT
[root@CentOS7 tmp]# qemu-img info centos6.9-64bit-flat.vmdk
image: centos6.9-64bit-flat.vmdk
file format: raw
virtual size: 10G (10737418240 bytes)
disk size: 0
```

#### NOTE

The command output shows that the format of **centos6.9-64bit.vmdk** is VMDK and that of **centos6.9-64bit-flat.vmdk** is RAW. You can convert the format of only **centos6.9-64bit.vmdk**. For details about how to convert it, see [3](#).

2. Query the configuration file of the pre-allocated image.

#### **cat centos6.9-64bit.vmdk**

The following information is displayed:

```
[root@CentOS7 tmp]# cat centos6.9-64bit.vmdk
# Disk DescriptorFile
version=1
CID=c4d09ad3
parentCID=ffffffff
createType="monolithicFlat"

# Extent description
RW 20971520 FLAT "centos6.9-64bit-flat.vmdk" 0

# The Disk Data Base
#DDB

ddb.virtualHWVersion = "4"
ddb.geometry.cylinders = "20805"
ddb.geometry.heads = "16"
ddb.geometry.sectors = "63"
ddb.adapterType = "ide"
```

3. Place **centos6.9-64bit-flat.vmdk** and **centos6.9-64bit.vmdk** in the same directory. Run the following command to convert the format of **centos6.9-64bit.vmdk** to QCOW2 using **qemu-img**:

```
[root@CentOS7 tmp]# qemu-img convert -p -f vmdk -O qcow2 centos6.9-64bit.vmdk centos6.9-64bit.qcow2
(100.00/100%)
```

4. Query details about the converted file in QCOW2 format.

#### **qemu-img info centos6.9-64bit.qcow2**

The following information is displayed:

```
[root@CentOS7 tmp]# qemu-img info centos6.9-64bit.qcow2
image: centos6.9-64bit.qcow2
file format: qcow2
virtual size: 10G (10737418240 bytes)
disk size: 200K
cluster_size: 65536
Format specific information:
  compat: 1.1
  lazy refcounts: false
```

## Follow-up Procedure

After the image file format is converted, you can use `obsutil` to upload the image file to an OBS bucket for creating a private image. For details about how to use `obsutil` to upload an image file, see [Uploading an Object](#).

## 6.2 Converting the Image Format Using `qemu-img-hw`

### Scenarios

You can import an image file in VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, QED, ZVHD, or ZVHD2 format to Huawei Cloud. Image files in other formats need to be converted into any of these formats using the open-source tool **`qemu-img`** before being imported. However, the **`qemu-img`** tool cannot convert image files to the ZVHD or ZVHD2 format. To convert image files to any of the two formats, use the cloud's self-developed tool **`qemu-img-hw`**. This section describes how to use **`qemu-img-hw`** to convert an image file to ZVHD2.

### Tool and Costs

**Table 6-2** Tool and costs

| Tool                     | Description                                                                                                                                                                                                                                                                                                                 | Costs |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| <code>qemu-img-hw</code> | <b><code>qemu-img-hw</code></b> is used for converting image formats.<br>You can obtain it from:<br><a href="https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/imageImportTools/qemu-img-hw.zip">https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/imageImportTools/qemu-img-hw.zip</a> | Free  |

### Constraints

**`qemu-img-hw`** can be used only in Linux. You can run it on a local Linux server or a Linux ECS on the cloud platform. The following procedure uses a EulerOS ECS as an example.

### Procedure

1. Upload the image file to be converted to the ECS.
  - If your local PC runs a Linux OS, 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 your local PC runs a Windows OS, use a file transfer tool, such as WinSCP, to upload the image file to the ECS.

2. Obtain the **qemu-img-hw** package, upload it to the ECS, and then decompress it.

**Table 6-3** qemu-img-hw package

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

 **NOTE**

This tool can be used only on x86 servers.

3. Convert the image format.
  - a. Go to the directory where **qemu-img-hw** is stored, for example, **/usr/qemu-img-hw**.  
**cd /usr/qemu-img-hw**
  - b. Add the execute permission to the tool.  
**chmod +x qemu-img-hw**
  - c. Run **qemu-img-hw** to convert the image file to the ZVHD2 format.  
The command format of **qemu-img-hw** is as follows:  
**./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**

## 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 {image-file}**  
An example command is **qemu-img-hw info test.zvhd2**.
- Viewing help information: **qemu-img-hw -help**

## Appendix 2: Common qemu-img-hw Errors

- 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.

- Symptom:

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

```
./qemu-img-hu: error while loading shared libraries: libcrypto.so.10: cannot open shared object file: No such file or directory
```

Solution: Run **openssl version** to check whether the OpenSSL version is later than 1.0. If yes, install OpenSSL 1.0.

Run the following commands to install OpenSSL 1.0:

```
wget https://github.com/openssl/openssl/releases/download/
OpenSSL_1_0_2k/openssl-1.0.2k.tar.gz
```

```
tar -xvf openssl-1.0.2k.tar.gz
```

```
cd openssl-1.0.2k
```

```
./config -d shared --prefix=/tmp/openssl (custom installation directory)
```

```
make
```

```
make install
```

```
cp /tmp/openssl/lib/libcrypto.so.1.0.0 /usr/lib64/libcrypto.so.10
```

Delete the **/usr/lib64/libcrypto.so.10** file if you do not need it any longer.

## Follow-up Procedure

After the image file format is converted, you can use `obsutil` to upload the image file to an OBS bucket for creating a private image. For details about how to use `obsutil` to upload an image file, see [Uploading an Object](#).

# 7

## Configuring an ISO File as a Local Image Source

---

### Context

When you install software on a Linux ECS, the network may be disconnected or resources on the network may be invalid, resulting in software installation failures. In this case, you can configure an ISO file as a local image source to install the software.

### Package Managers

Before configuring a local source, you need to determine the package manager to be used. Generally, there are three types of package managers: yum, apt, and zypper.

- yum is for RHEL-based OSs: RHEL, CentOS, EulerOS, and Fedora.
- apt is for Debian and Ubuntu.
- zypper is for SUSE and openSUSE.

### Configure a Local Image Source

Configure a local image source by following the instructions in [yum](#), [apt](#), or [zypper](#).

- yum
  - a. Upload the ISO file to the ECS and mount it to the **/mnt** directory.  
**mount XXX.iso /mnt**
  - b. Enter the **/etc/yum.repo.d** directory where the yum configuration file is stored and back up all **.repo** files. Then, create a new **.repo** configuration file, for example **local.repo**. Add the following information to the **local.repo** file:

```
[rhel-local]
name=local
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

 NOTE

The **/mnt** directory specified in the configuration file must be the same as the mounting directory of the ISO file.

- c. Clear yum.  
**yum clean all**
- d. Generate a new cache.  
**yum makecache**
- apt
  - a. Upload the ISO file to the ECS and mount it to the **/mnt** directory.  
**mount XXX.iso /mnt**
  - b. Add the **apt cdrom** source.  
**apt-cdrom -m -d /mnt/ add**
  - c. View the added source in the configuration file.  
**cat /etc/apt/sources.list**
  - d. Update the source.  
**apt-get update**
- zypper
  - a. Upload the ISO file to the ECS.
  - b. Add the ISO file as the source.  
**sudo zypper addrepo iso:/?iso=/media/SOFTWARE/openSUSE-11.4-DVD-i586.iso DVDISO**  
In the preceding command:
    - **/media/SOFTWARE/openSUSE-11.4-DVD-i586.iso** is the location of the ISO file.
    - **DVDISO** is the source alias.
  - c. Check whether the source is successfully added.  
**zypper repos**
  - d. Refresh the source.  
**zypper refresh**

## Examples

The operations in [Configure a Local Image Source](#) may be different depending on the OS version. Basically, you need to add a source and refresh it. Debian 10.1.0 and CentOS 8.0 are used as examples to describe how to add a local source.

- Debian 10.1.0  
Run **cat /etc/apt/sources.list** to check whether the **sources.list** file contains a default cdrom source.

**Figure 7-1** Viewing the source

```
root@debian:~# cat /etc/apt/sources.list
#
# deb cdrom:[Debian GNU/Linux 10.1.0 _Buster_ - Official arm64 DVD Binary-1 20190907-14:13]/ buster main
deb cdrom:[Debian GNU/Linux 10.1.0 _Buster_ - Official arm64 DVD Binary-1 20190907-14:13]/ buster main
deb http://security.debian.org/debian-security buster/updates main
deb-src http://security.debian.org/debian-security buster/updates main
```

The source directs to the CD-ROM drive **/dev/cdrom**. Debian 10.1.0 provides a soft link to link the CD-ROM drive to **/media/cdrom**.

**Figure 7-2** Checking the media directory

```
root@debian:~# ls -l /media/
total 8
lrwxrwxrwx 1 root root    6 Nov  5 14:40 cdrom -> cdrom0
drwxr-xr-x 2 root root 4096 Nov  5 14:40 cdrom0
drwxr-xr-x 2 root root 4096 Nov  5 14:40 cdrom1
```

Therefore, mount the ISO file to **/media/cdrom**.

- CentOS 8.0
  - a. Mount the ISO file to the **/mnt** directory.
  - b. Rename all source files except **CentOS-Media.repo** in the **/etc/yum.repo.d** directory as .bak files or move them to another directory.
  - c. Modify the **CentOS-Media.repo** file.

**Figure 7-3** Modifying the CentOS-Media.repo file

```
[c8-media-BaseOS]
name=CentOS-BaseOS-$releasever - Media
baseurl=file:///mnt/BaseOS
gpgcheck=0
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-centosofficial

[c8-media-AppStream]
name=CentOS-AppStream-$releasever - Media
baseurl=file:///mnt/AppStream
gpgcheck=0
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-centosofficial
```

The modifications in the red box are as follows:

- Set **baseurl** to **file:///mnt/BaseOS** and **file:///mnt/AppStream**. **mnt** is the mounting directory of the ISO file. Delete invalid paths from the default configuration, or a checksum error will occur.
- Change the value of **gpgcheck** to **0**, indicating that the check is not performed.

- Change the value of **enabled** to **1** for the configurations to take effect.
- d. Clear yum and generate a new cache.  
**yum clean all && yum makecache**

# 8 Migrating ECSs Across Accounts and Regions

## Context

You can migrate an ECS by deploying the services on a new ECS, using Server Migration Service (SMS), or using Image Management Service (IMS). If you want to migrate ECSs between Huawei Cloud accounts and across regions, you are advised to use IMS to implement the migration.

Table 8-1 ECS migration methods

| Migrati on Method                | Description                                                                                                                                                                   | Characteristics                                                                                                                                                                                                                                                                            | Constraints                                                                                                |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Deployin g services on a new ECS | Purchase a new ECS to deploy the services. In this way, you need to upload files, install software, create file directories, and assign file permissions again.               | Service migration is not required but data on the data disk needs to be migrated.                                                                                                                                                                                                          | Services need to be deployed and configured on the new ECS, consuming a lot of labor, materials, and time. |
| Server Migrati on Service        | You can use SMS to migrate x86 physical servers or VMs from private or public clouds to Huawei Cloud through physical to virtual (P2V) or virtual to virtual (V2V) migration. | <ul style="list-style-type: none"><li>You only need to install and configure an Agent on the source server and create a migration task on SMS. SMS will complete the migration.</li><li>Services are not interrupted during the migration. Resumable data transfer is available.</li></ul> | The server to be migrated must be able to access the Internet.                                             |

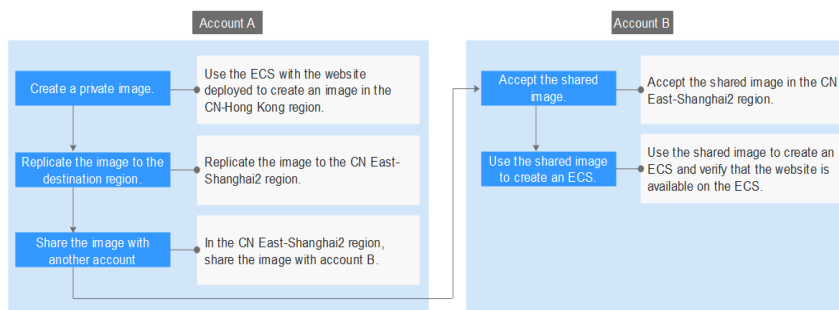
| Migrati<br>on<br>Method                                | Description                                                                                                                                                                                                                                            | Characteristics                                                                                                                                                                                                                                                                                                                                                                                                                                             | Constraints                                                                           |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Image<br/>Manage<br/>ment<br/>Service<br/>(IMS)</b> | Migrate a server from an on-premises IDC, private cloud, or other public clouds to Huawei Cloud, or migrate an ECS between Huawei Cloud accounts or across regions by importing private images, replicating images across regions, and sharing images. | <ul style="list-style-type: none"><li>Only image files in VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, QED, ZVHD, or ZVHD2 format can be imported.</li><li>IMS is compatible with mainstream OSs, such as SUSE, Oracle Linux, Red Hat, Ubuntu, openSUSE, CentOS, Debian, Fedora, and EulerOS.</li><li>You can create system disk images, data disk images, and full-ECS images that can be used to create identical ECSs for batch service deployment.</li></ul> | Local storage space is required and only image files no larger than 1 TB can be used. |

## Cross-Account, Cross-Region ECS Migration

To migrate an ECS to a different account and to another region, use the ECS to create an image, replicate the image to the destination region under the same account, and then share the image with the target account. The target account accepts the shared image and uses the image to create a new ECS.

For example, if a website is set up on an ECS in the CN-Hong Kong region and you want to migrate the ECS to the CN East-Shanghai2 region under another account, the process is as follows:

**Figure 8-1** Migration process

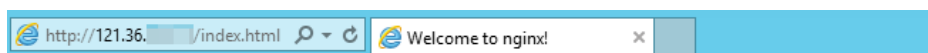


1. **Create a private image**
2. **Replicate the image to the destination region**

3. [Share the image with the target account](#)
4. [Accept the shared image](#)
5. [Use the shared image to create an ECS](#)

## Step 1: Create a Private Image

Use the ECS with the website deployed to create an image in the CN-Hong Kong region. Assume that the ECS web address is `http://121.36.xxx.xxx/index.html`.



### Welcome to nginx!

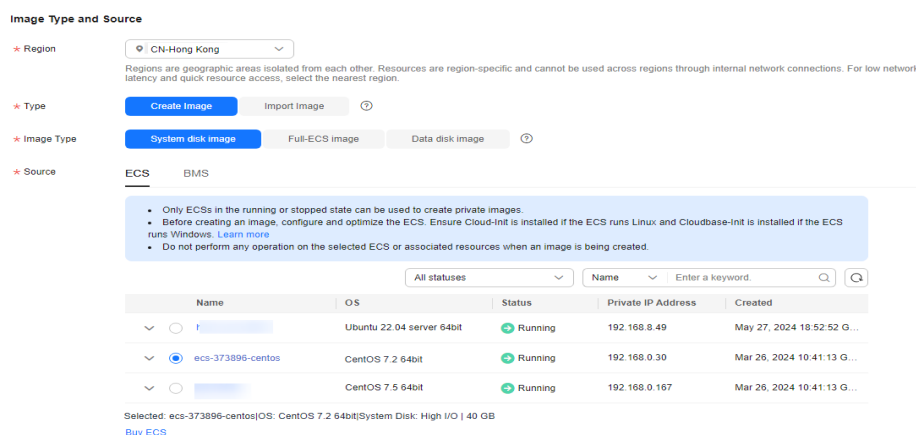
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

1. Log in to the management console and switch to the CN-Hong Kong region.
2. Under **Service List**, choose **Compute > Elastic Cloud Server**.  
The **Elastic Cloud Server** page is displayed.
3. Locate the row that contains the ECS with the website deployed (for example, **ecs-373896-centos**), and choose **More > Manage Image > Create Image** in the **Operation** column.  
The **Create Image** page is displayed.
4. Set parameters.

Figure 8-2 Creating a private image



- **Type:** Select **Create Image**.
- **Image Type:** Select **System disk image**.
- **Source:** Select **ECS** and then select **ecs-373896-centos** from the list.
- **Name:** Enter a name for the image, for example, **migrate\_test**.

- **Enterprise Project:** Select **default**.
5. Click **Next**.
  6. Confirm the settings, read and agree to the agreement, and click **Submit**.
  7. The system redirects to the private image list. Wait for several minutes and check whether the private image is successfully created.

**Figure 8-3** Viewing private images

| <input type="checkbox"/> Name         | Status | OS Type | OS          | Image Type                 |
|---------------------------------------|--------|---------|-------------|----------------------------|
| <input type="checkbox"/> migrate_test | Normal | Linux   | CentOS 7... | ECS system disk image(x86) |

## Step 2: Replicate the Image to the Destination Region

Replicate the private image created in [Step 1: Create a Private Image](#) to the CN East-Shanghai2 region. Before performing the replication, create an IAM agency.

1. Create an IAM agency.
  - a. In the upper right corner of the page, click the username and select **Identity and Access Management**.
  - b. In the navigation pane, choose **Agencies**.
  - c. Click **Create Agency**.
  - d. On the **Create Agency** page, set the following parameters:
    - **Agency Name:** Enter an agency name, for example, **ims\_admin\_agency**.

**Figure 8-4** Creating an agency

\* Agency Name

\* Agency Type ☐ Account  
Delegate another HUAWEI CLOUD account to perform operations on your resources  
☒ Cloud service  
Delegate a cloud service to access your resources in other cloud services

\* Cloud Service

\* Validity Period

Description

40/255

- **Agency Type:** Select **Cloud service**.
- **Cloud Service:** This parameter is available only if you select **Cloud service** for **Agency Type**. Click **Select**. In the displayed **Select Cloud Service** dialog box, select **Image Management Service (IMS)** and click **OK**.
- **Validity Period:** Select **Unlimited**.
- **Description:** This parameter is optional. You can enter **Agency with IMS Administrator privileges**.
- **Permissions:** Click **Assign Permissions**. By default, **Policy View** is displayed. Enter **IMS Administrator** in the search box, select the **IMS Administrator** check box, select **CN-Hong Kong** and **CN East-Shanghai2** in the **Project [Region]** column, and click **OK**.

**CAUTION**

Do not select **All projects** in the **Project [Region]** column. Otherwise, the created agency will be invalid.

**Figure 8-5** Configuring permissions

Assign Permissions

Multiple policies can be selected. You can also [modify](#) or [create](#) policies. ①

View Selected (1) All policies/roles IMS Administrator X Q C Policy view Project view

| <input checked="" type="checkbox"/>   | Policy/Role Name  | Description       | Project [Region]                                                 |
|---------------------------------------|-------------------|-------------------|------------------------------------------------------------------|
| ② <input checked="" type="checkbox"/> | IMS Administrator | IMS Administrator | ③ ap-southeast-1 [CN-Hong Kong]<br>cn-east-2 [CN East-Shanghai2] |

JSON

```
1 {
2   "Version": "1.0",
3   "Statement": [
4     {
5       "Action": [
6         "ims:*:*",
7         "ecs:*:list",
8         "ecs:*:get",
9         "evs:*:get"
10      ],
11      "Effect": "Allow"
12    }
13  ],
14  "Depends": [
15    {
16      "catalog": "OBS",
17      "display_name": "Tenant Administrator"
18    }
19  ]
20 }
```

Cancel OK

- e. Click **OK**.

**Figure 8-6** Viewing agencies

| Agency Name/ID   | Delegated Party                           | Validity Peri... | Created              | Description | Operation     |
|------------------|-------------------------------------------|------------------|----------------------|-------------|---------------|
| ims_admin_agency | Cloud service<br>Image Management Service | Unlimited        | Jun 04, 2020 10:3... |             | Modify   More |

2. Under **Service List**, choose **Compute > Image Management Service**. Then, click the **Private Images** tab.

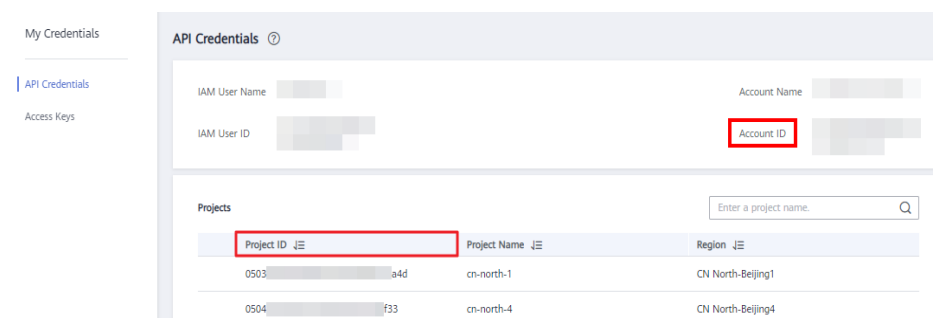
- The **Private Images** page is displayed.
- Locate the row that contains the **migrate\_test** image, and choose **More > Replicate** in the **Operation**.  
The **Replicate Image** dialog box is displayed.
  - Set parameters.
    - Name**: Retain the default value **copy\_ap-southeast-1\_migrate\_test**.
    - Destination Region**: Select **CN East-Shanghai2**.
    - Destination Project**: Select **cn-east-2**.
    - IAM Agency**: Select **ims\_admin\_agency** created in 1.
  - Click **OK**.
  - Switch to the CN East-Shanghai2 region. Wait for several minutes and check whether the image is successfully replicated.

**Figure 8-7** Viewing private images

| <input type="checkbox"/> Name                             | Status              | OS Type | OS            | Image Type            |
|-----------------------------------------------------------|---------------------|---------|---------------|-----------------------|
| <input type="checkbox"/> copy_ap-southeast-1_migrate_test | <span>Normal</span> | Linux   | CentOS 7.2... | ECS system disk image |

### Step 3: Share the Image with the Target Account

Before the image sharing, obtain the project ID of the target account. (You can obtain the project ID from **My Credentials**. For details, see [Figure 8-8](#).)

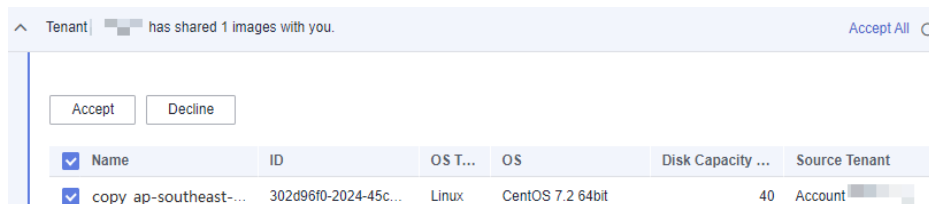
**Figure 8-8** Viewing the project ID or account ID

- In the CN East-Shanghai2 region, choose **Service List > Compute > Image Management Service** and click the **Private Images** tab.  
The **Private Images** page is displayed.
- Locate the row that contains the **copy\_ap-southeast-1\_migrate\_test** private image. Choose **More > Share** in the **Operation** column.  
The **Share Image** dialog box is displayed.
- In the **Share Image** dialog box, enter the project ID of the target account.
- Click **OK**.

### Step 4: Accept the Shared Image

Accept the shared image in the East-Shanghai2 region.

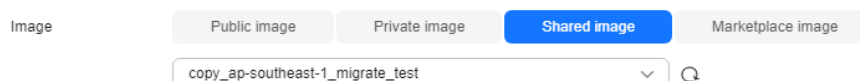
1. Log in to the management console using the account the image is shared with and switch to the CN East-Shanghai2 region.
2. Under **Service List**, choose **Compute > Image Management Service**. Then, click the **Images Shared with Me** tab.
3. Select **copy\_ap-southeast-1\_migrate\_test** and click **Accept**.  
After the image is accepted, it is displayed in the shared image list.

**Figure 8-9** Accepting a shared image

## Step 5: Use the Shared Image to Create an ECS

Use the shared image to create an ECS and verify that the website is available on the ECS.

1. Locate the row that contains the shared image **copy\_ap-southeast-1\_migrate\_test**, and click **Apply for Server** in the **Operation** column.  
The page for purchasing ECSs is displayed.
2. Configure the billing mode, AZ, specifications, and network as needed to create an ECS. Retain the default value for **Image**.

**Figure 8-10** Selecting an image

3. Wait for several minutes and check whether the new ECS is displayed in the ECS list.

**Figure 8-11** Viewing ECSs

| <input type="checkbox"/> | Name/ID                                    | Monitoring | AZ  | Status  | Specifications/Image                                            | IP Address                                             |
|--------------------------|--------------------------------------------|------------|-----|---------|-----------------------------------------------------------------|--------------------------------------------------------|
| <input type="checkbox"/> | ecs-5d74<br>249b8e52-87e6-49d2-95ec-730... |            | AZ1 | Running | 2 vCPUs   4 GB   s6.large.2<br>copy_ap-southeast-1_migrate_test | 124.70... (EIP) 5 M...<br>192.168.10.178 (Private I... |

4. Access the website to check whether the website is available on the new ECS.  
In the address box of the browser, enter **http://ECS EIP/index.html**, for example, **http://124.70.xxx.xxx/index.html**. If the website can be normally accessed, the migration is successful. No further action is required.

**Figure 8-12** Verifying the website



# 9 Creating a Data Disk Image to Migrate Service Data Across Accounts

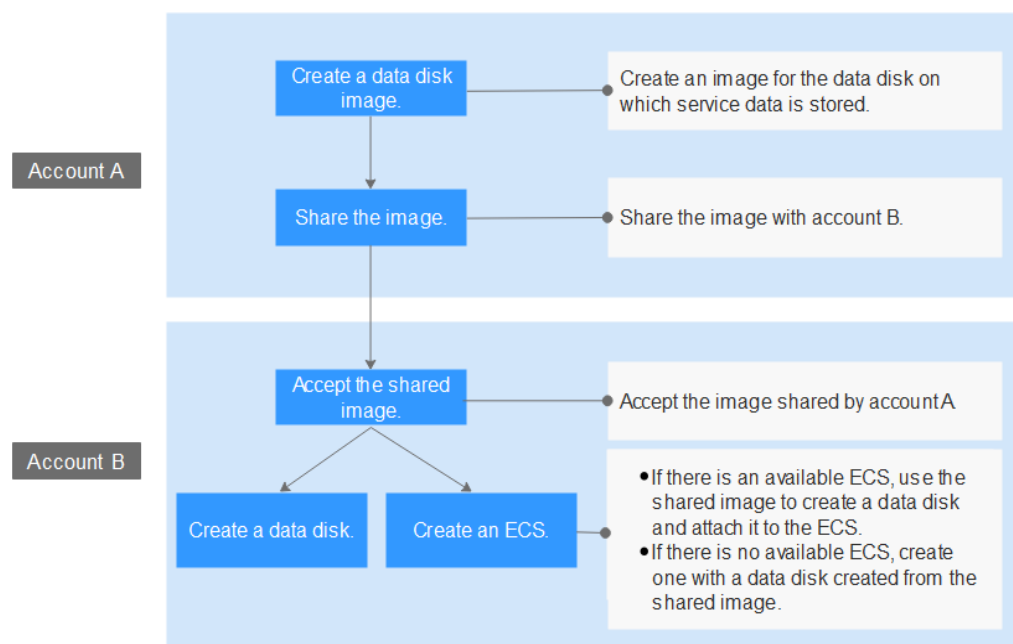
## Scenarios

Generally, service data is stored on data disks. To migrate the data across accounts, you need to create data disk images and share them with the target account. This section uses Linux as an example to describe how to migrate service data (stored on data disks) across accounts in the same region.

## Introduction

To migrate service data stored on a data disk across accounts, create an image from the data disk, share the image with the target account. The target account accepts the shared image and attaches the new data disk created from the shared image to an existing or new ECS.

**Figure 9-1** Migration process



1. [Create a data disk image](#)
2. [Share the image with the target account](#)
3. [Accept the shared image](#)
4. [Create a data disk or an ECS](#)

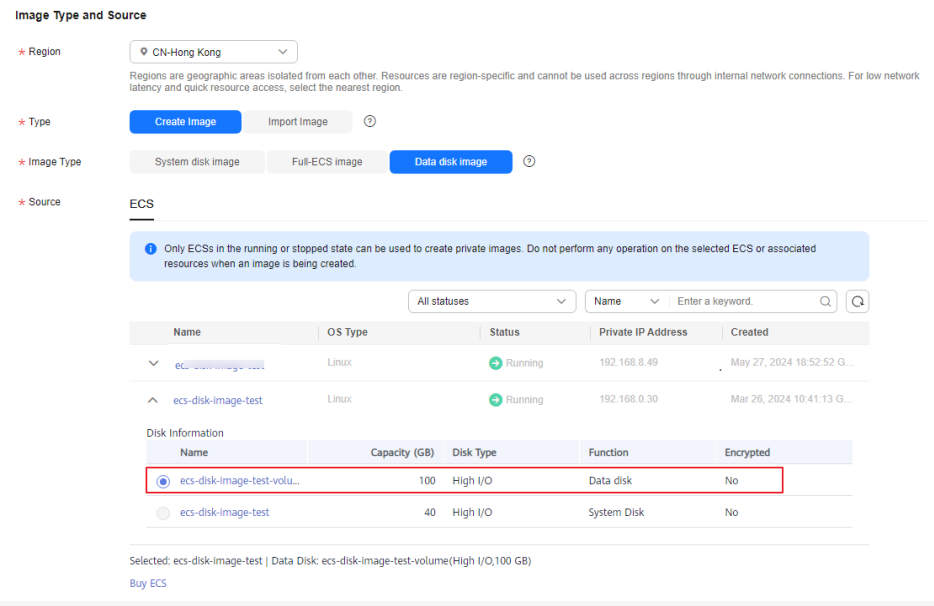
Step 1: Create a Data Disk Image

Assume that `qianyi.txt` is stored on the data disk of your ECS and you want to migrate the file to another account.

```
[root@ecs-disk-image-test data]# cat qianyi.txt
This is a test.
[root@ecs-disk-image-test data]# df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs  2.0G   0    2.0G   0% /dev
tmpfs           tmpfs     2.0G   0    2.0G   0% /dev/shm
tmpfs           tmpfs     2.0G  9.0M   2.0G   1% /run
tmpfs           tmpfs     2.0G   0    2.0G   0% /sys/fs/cgroup
/dev/vda1       ext4      43G   2.2G   38G    6% /
tmpfs           tmpfs     398M   0    398M   0% /run/user/0
/dev/vdb1       ext4     106G   63M  101G    1% /mnt/data
[root@ecs-disk-image-test data]#
```

1. Log in to the management console and switch to the CN-Hong Kong region.
2. Under **Service List**, choose **Compute > Image Management Service**.  
The **Image Management Service** page is displayed.
3. In the upper right corner, click **Create Image**.  
The **Create Image** page is displayed.
4. Set parameters.

Figure 9-2 Creating a data disk image



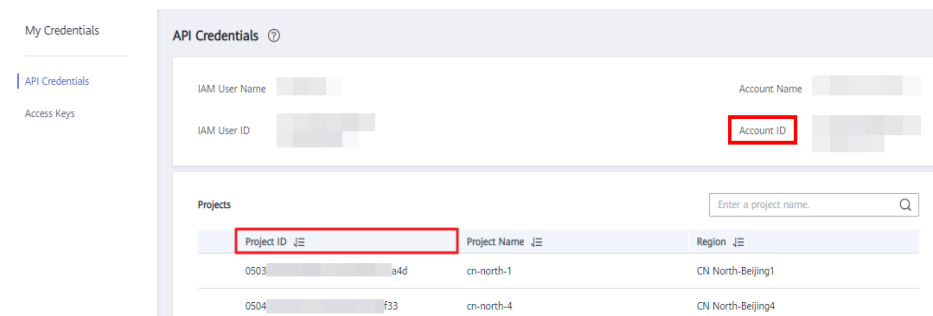
- **Type:** Select **Create Image**.
  - **Image Type:** Select **Data disk image**.
  - **Source:** Select **ECS** and then select the **data disk ecs-disk-image-test-volume** data disk.
  - **Name:** Enter a name for the data disk image, for example, **disk-image-test**.
  - **Enterprise Project:** Select **default**.
5. Click **Next**.
  6. Confirm the settings, read and agree to the agreement, and click **Submit**.
  7. The system redirects to the private image list. Wait for several minutes and check whether the data disk image is successfully created.

**Figure 9-3** Viewing private images

| <input type="checkbox"/> | Name <span>⌵</span> | Status                | OS Type | OS | Image Type      | Disk Capacity (GB) | Encrypted |
|--------------------------|---------------------|-----------------------|---------|----|-----------------|--------------------|-----------|
| <input type="checkbox"/> | disk-image-test     | <span>✓</span> Normal | Linux   | -- | Data disk image | 100                | No        |

## Step 2: Share the Image with the Target Account

Share the data disk image created in [Step 1: Create a Data Disk Image](#) with the target account. Before the image sharing, obtain the project ID of the target account. (You can obtain the project ID from **My Credentials**. For details, see [Figure 9-4](#).)

**Figure 9-4** Viewing the project ID or account ID

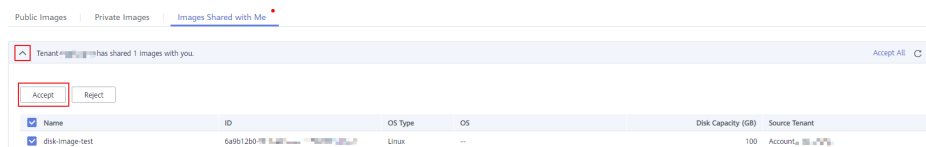
1. Locate the row that contains the **disk-image-test** private image. Choose **More > Share** in the **Operation** column.  
The **Share Image** dialog box is displayed.
2. In the **Share Image** dialog box, enter the project ID of the target account.
3. Click **OK**.

## Step 3: Accept the Shared Image

Accept the shared data disk image.

1. Log in to the management console using the account the image is shared with and switch to the CN-Hong Kong region.

2. Under **Service List**, choose **Compute > Image Management Service**. Then, click the **Images Shared with Me** tab.
3. Select **disk-image-test** and click **Accept**.

**Figure 9-5** Accepting a shared image

After the image is accepted, it is displayed in the shared image list.

## Step 4: Create a Data Disk or an ECS

Use the shared image to create a new data disk and attach it to an existing ECS. Alternatively, create an ECS with a data disk created from the shared image. Then, check whether the service data is successfully migrated.

- Create a new data disk and attach it to an existing ECS.
  - a. Locate the row that contains the shared image **disk-image-test**, and click **Create Data Disk** in the **Operation** column.

**Figure 9-6** Creating a data disk

| <input type="checkbox"/>            | Name            | OS Type | OS | Image Type      | Disk Capacity (GB) | Source Tenant | Source Project Name | Source Project ID | Operation             |
|-------------------------------------|-----------------|---------|----|-----------------|--------------------|---------------|---------------------|-------------------|-----------------------|
| <input checked="" type="checkbox"/> | disk-image-test | Linux   | -- | Data disk image | 100                | Account       | ap-southeast-1      | b1e456f           | Create Data Disk More |

The page for purchasing EVS disks is displayed.

- b. Configure the billing mode and disk specifications as needed. The AZ must be the same as that of the ECS to which the data disk will be attached. Click **Next**.
- c. Return to the EVS disk list. Wait for several minutes until the EVS disk is created successfully.
- d. Locate the row that contains the new EVS disk and click **Attach** in the **Operation** column to attach the data disk to the ECS.
- e. Log in to the ECS and check whether the service data is successfully migrated.

Run the **fdisk -l** command. The command output shows that the new data disk has been partitioned.

```
[root@ecs-f04d ~]# fdisk -l
```

Disk /dev/vda: 42.9 GB, 42949672960 bytes, 83886080 sectors  
Units = sectors of 1 \* 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disk label type: dos  
Disk identifier: 0x000f1217

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

Disk /dev/vdb: 107.4 GB, 107374182400 bytes, 209715200 sectors  
Units = sectors of 1 \* 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disk label type: dos  
Disk identifier: 0x7abde66f

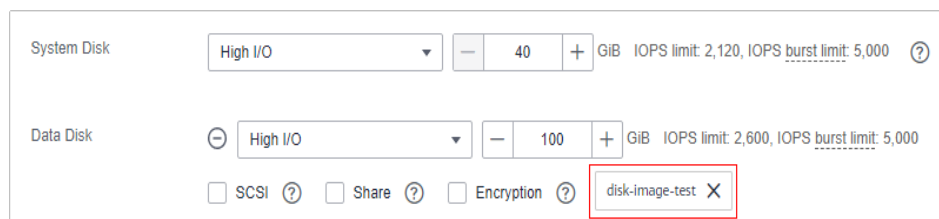
| Device    | Boot | Start | End       | Blocks    | Id | System |
|-----------|------|-------|-----------|-----------|----|--------|
| /dev/vdb1 |      | 2048  | 209715199 | 104856576 | 83 | Linux  |

Mount the new partition to a directory of the ECS and check the **qianyi.txt** file. The file content is properly printed, which means that the service data migration is successful.

```
[root@ecs-f04d ~]# cd /mnt
[root@ecs-f04d mnt]# ls
[root@ecs-f04d mnt]# mkdir data
[root@ecs-f04d mnt]# ls
data
[root@ecs-f04d mnt]# mount /dev/vdb1 /mnt/data
[ 170.467473] EXT4-fs (vdb1): recovery complete
[ 170.468655] EXT4-fs (vdb1): mounted filesystem with ordered data mode. Opts: (null)
[root@ecs-f04d mnt]# cd data
[root@ecs-f04d data]# ls
lost+found qianyi.txt
[root@ecs-f04d data]# cat qianyi.txt
This is a test.
```

- Create an ECS with a data disk attached.
  - a. Under **Service List**, choose **Compute > Elastic Cloud Server**.
  - b. In the upper right corner, click **Buy ECS**.  
The page for purchasing ECSs is displayed.
  - c. Configure the billing mode, AZ, and specifications as needed and add a data disk which will be created from the shared data disk image. Complete the ECS creation as instructed.

**Figure 9-7** Adding a data disk



- d. Wait for several minutes and check whether the new ECS is displayed in the ECS list.
- e. Log in to the new ECS and check whether the service data is successfully migrated.

Run the **fdisk -l** command. The command output shows that the new data disk has been partitioned. Mount the new partition to a directory of the ECS and check the **qianyi.txt** file. The file content is properly printed, which means that the service data migration is successful.

```
[root@ecs-38e4 ~]# fdisk -l

Disk /dev/vda: 42.9 GB, 42949672960 bytes, 83886080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000f1217

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

Disk /dev/vdb: 107.4 GB, 107374182400 bytes, 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x7abde66f

   Device Boot      Start         End      Blocks   Id  System
/dev/vdb1             2048    209715199    104856576   83   Linux
[root@ecs-38e4 ~]# mkdir /mnt/data
[root@ecs-38e4 ~]# mount /dev/vdb1 /mnt/data
[ 1177.739741] EXT4-fs (vdb1): recovery complete
[ 1177.741032] EXT4-fs (vdb1): mounted filesystem with ordered data mode. Opts: (null)
[root@ecs-38e4 ~]# cd /mnt/data
[root@ecs-38e4 data]# ls
lost+found  qianyi.txt
[root@ecs-38e4 data]# cat qianyi.txt
This is a test.
```

# 10 IMS Security

---

Huawei Cloud and you share the responsibility for security. Huawei Cloud ensures the security of cloud services. As a tenant, you should take advantage of the security capabilities provided by Huawei Cloud to protect your data and use the cloud securely. For details, see [Shared Responsibilities](#).

This section provides actionable guidance for enhancing the overall security of IMS.

Consider the security configurations from the following aspects:

## Create an Encrypted Image from an Image File

1. Upload an image file to an OBS bucket.
2. On the IMS console, select **Import Image** for **Type** and **System disk image**, **Data disk image**, or **ISO image** for **Image Type**. If the image file is in ZVHD2 or RAW format, do not select **Enable Fast Create**.
3. Select **KMS encryption** and select a key from list. An encrypted image will be created.

## Create an Encrypted Image from 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 from this ECS will also be encrypted.

The key used for encrypting the image is the same as that used for encrypting the system disk.

## Create an Encrypted Image by Replicating an Image

If you want to convert an unencrypted image into an encrypted one, you can replicate this image as a new one and encrypt the new image using a key.