Image Management Service

Best Practices

Issue	05
Date	2020-06-04

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Overview of IMS Best Practices....1
2 Creating a Windows Image Using VirtualBox and an ISO File....3
2.1 Introduction....3
2.2 Installing VirtualBox....4
2.3 Creating a VM and Installing the OS....7
2.3.1 Creating an Empty VM....7
2.3.2 Installing Windows on the VM....13
2.4 Configuring the VM....15
2.4.1 Installing UVP VMTools....15
2.4.2 Installing VirtualBox Guest Additions on the Windows VM....16
2.4.3 (Optional) Installing Cloudbase-Init....17
2.4.4 (Optional) Installing the One-Click Password Reset Plug-in....19
2.5 Exporting the Image File....19
2.6 Uploading and Registering the Image File....20
3 Creating a Linux Image Using VirtualBox and an ISO File....21
3.1 Introduction....21
3.2 Installing VirtualBox....22
3.3 Creating a VM and Installing the OS....25
3.3.1 Creating an Empty VM....25
3.3.2 Installing a Linux OS on the VM....31
3.4 Configuring the VM....34
3.4.1 Optimizing the VM....34
3.4.2 Installing Cloud-Init....37
3.4.3 Configuring Cloud-Init....43
3.4.4 (Optional) Installing the One-Click Password Reset Plug-in....48
3.4.5 Configuring NetworkManager....49
3.5 Exporting the Image File....50
3.6 Uploading and Registering the Image File....51
4 Cleaning Up the Disk Space of a Windows ECS....52
5 Converting the Image Format....63
5.1 Converting the Image Format Using qemu-img....63
5.2 Converting the Image Format Using qemu-img-hw....67

6 Creating a Private Image Using Packer..... 70
7 Configuring an ISO File as a Local Image Source..... 78
8 Migrating ECSs Across Accounts and Regions..... 82
A Change History..... 92

1 Overview of IMS Best Practices

This document summarizes operation practices in common application scenarios of Image Management Service (IMS). Each practice provides detailed solution description and operation guide, helping you easily build image-based services.

Table 1-1 IMS best practices

Practice	Description
Creating a Windows image from an ISO file using VirtualBox	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, and generate a VHD image using the created VM.
Creating a Linux image from an ISO file using VirtualBox	Describes how to create a Linux image using VirtualBox. To do so, you need to install VirtualBox, use an ISO file to create a VM, and generate a VHD image using the created VM.
Cleaning up the disk space of a Windows ECS	Describes how to clean up the disk space of a Windows ECS.
Converting the image format	Describes how to use qemu-img or Huawei-developed qemu-img-hw to convert the image format. qemu-img supports the mutual conversion of formats VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, and QED but does not support the conversion to ZVHD or ZVHD2. To convert an image file to any of the two formats, use qemu-img-hw.
Creating a private image using Packer	Describes how to create a Ubuntu 16.04 Server 64-bit private image from a CentOS 7.4 ECS using Packer and upload the created image to the cloud platform.

Practice	Description
Configuring an ISO file as a local image source	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.
Migrating ECSs across accounts and regions	Describes how to migrate an ECS with a website deployed across regions and accounts.

2 Creating a Windows Image Using VirtualBox and an ISO File

2.1 Introduction

VirtualBox

VirtualBox is a free and open-source hypervisor for x86 computers. Developed initially by InnoTek GmbH from Germany, it was acquired by Oracle Corporation and is now part of Oracle's xVM virtualization platform technology. VirtualBox is a virtualizer for x86 OSs based on the provided 32-bit or 64-bit Windows, Solaris, and Linux OSs. That is, users can install and run Solaris, Windows, DOS, Linux, OS/2 Warp, OpenBSD, and FreeBSD on VirtualBox as client OSs.

For more information about VirtualBox, visit the Oracle official website.

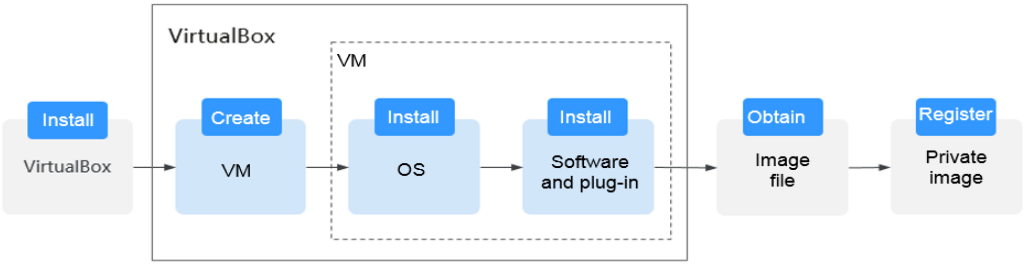
Download the installation package from **https://www.virtualbox.org/wiki/Downloads**.

Click **here** to see the OSs that can work with VirtualBox.

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 machine (64-bit Windows is recommended) and install VirtualBox on the host machine. For details about the preparations and installation process, see **Installing VirtualBox**.
2. Create a VM: Create an empty VM on VirtualBox as the image source. For details, see **Creating an Empty VM**.
3. Install the OS: Mount an ISO file to install an OS for the VM. The OS of 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: To ensure that the image to be created can be used to provision ECSs that can run properly, install the required software and plug-ins on the VM, including UVP VMTools, 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 **Exporting the Image File**.
6. Register a private image: Upload the exported VHD image file to the OBS bucket and register it as a private image. Then you can use the private image to create ECSs. For details, see **Uploading and Registering the Image File**.

2.2 Installing VirtualBox

This section describes how to install VirtualBox.

Preparations

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

- The host runs a 64-bit Windows OS.
- The host has a memory of at least 4 GB and uses a dual-core processor. For example, the host specifications can be 8U16G.
- The available hard disk space is at least 20 GB.
- The host CPU supports hardware virtualization (Intel VT-x or AMD-V virtualization). For how to enable this, 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)

Perform the following operations to enable hardware virtualization on an Intel host:

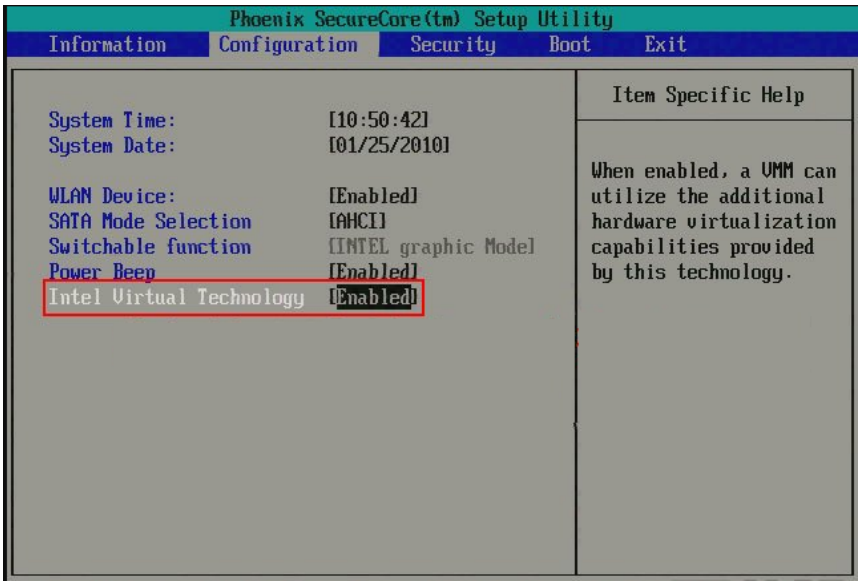
NOTE

The operations may differ depending on the host. You can enable hardware virtualization as prompted.

1. During startup, press the corresponding key to enter the BIOS.

2. Enter the BIOS, choose **Configuration** > **Intel Virtual Technology**, and press **Enter**.
3. Move the cursor to **Enabled** and press **Enter**. The value of **Intel Virtual Technology** will become **Enabled**.
4. Press **F10** to save the settings and exit. The hardware virtualization function is enabled.

Figure 2-2 Enabling the hardware virtualization function

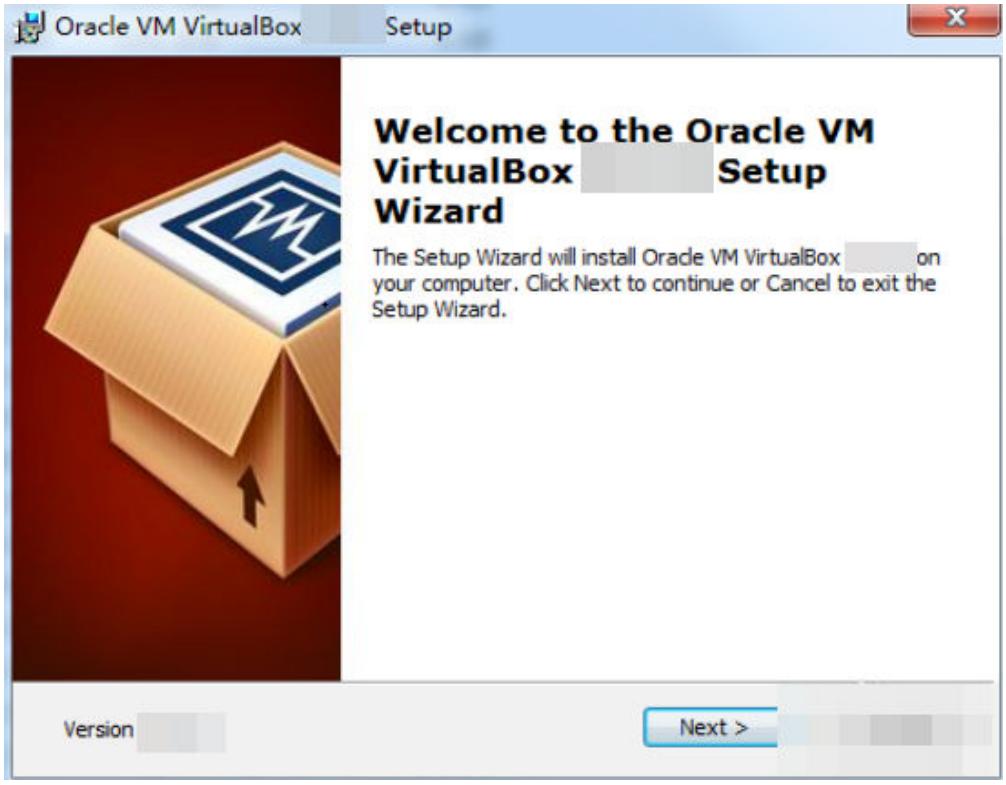


Procedure

1. Download the VirtualBox installation package.

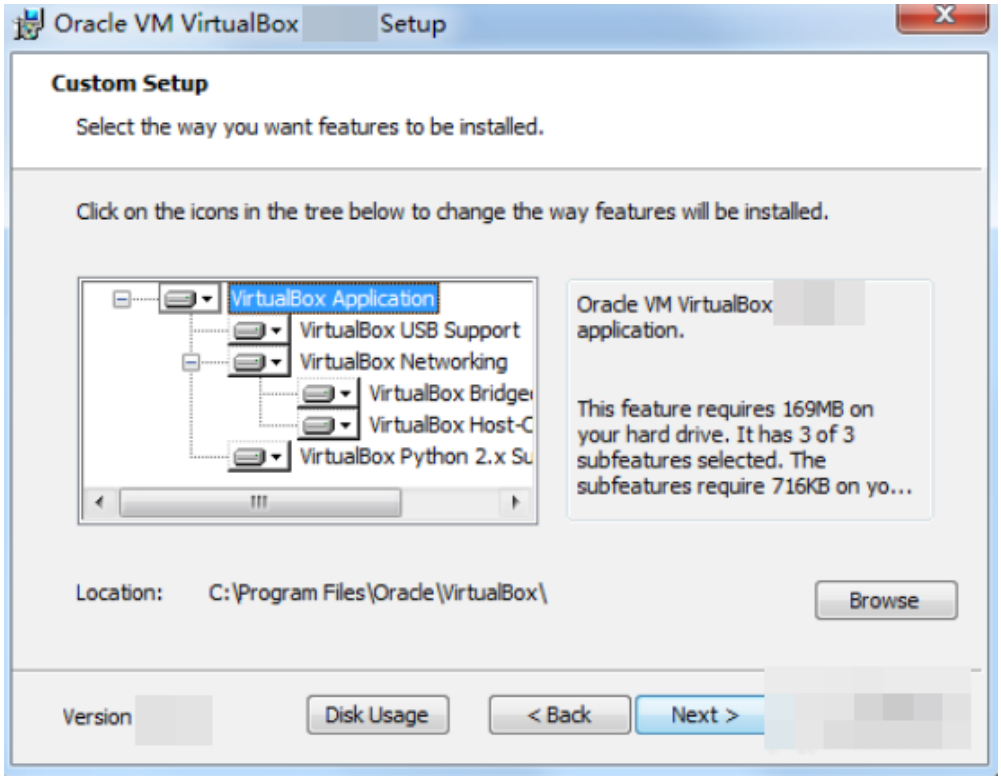
   Download the installation package from **https://www.virtualbox.org/wiki/Downloads**.
2. Decompress the installation package. Take VirtualBox-5.2.0 as an example. Right-click **VirtualBox-5.2.0-118431-Win.exe**, choose **Run as administrator**, and complete the installation as prompted.

Figure 2-3 Installing VirtualBox



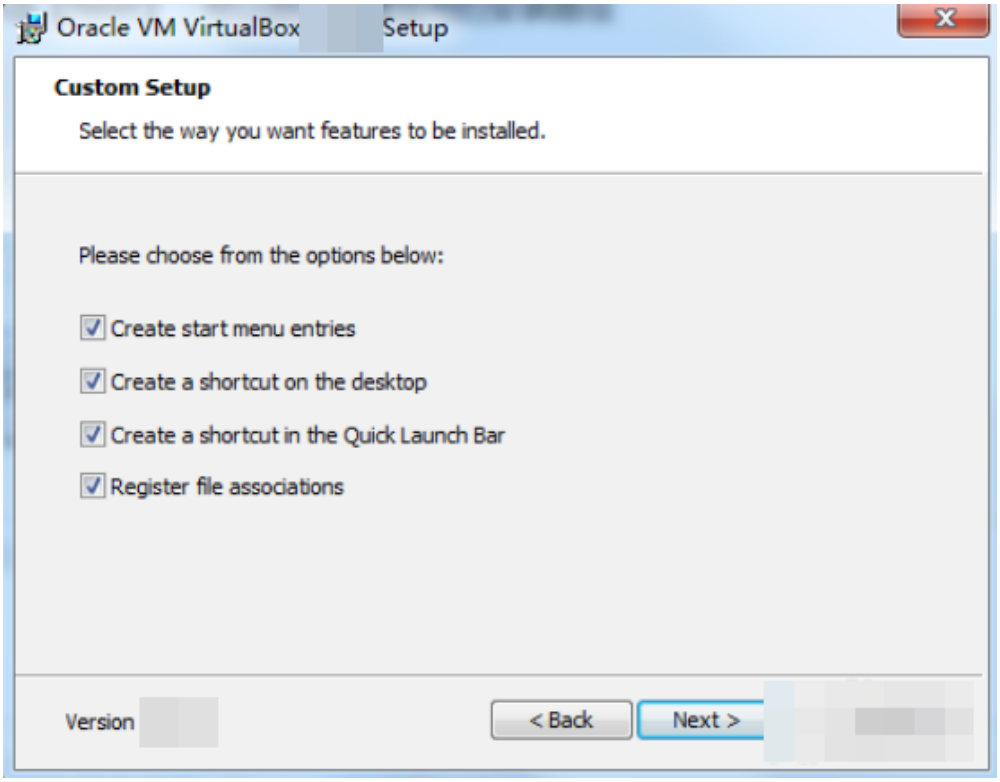
3. Select the VirtualBox installation path and click **Next**.

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 the OS

This section describes how to create an empty VM and install the OS on the VM after installing VirtualBox.

2.3.1 Creating an Empty VM

Prerequisites

VirtualBox has been installed.

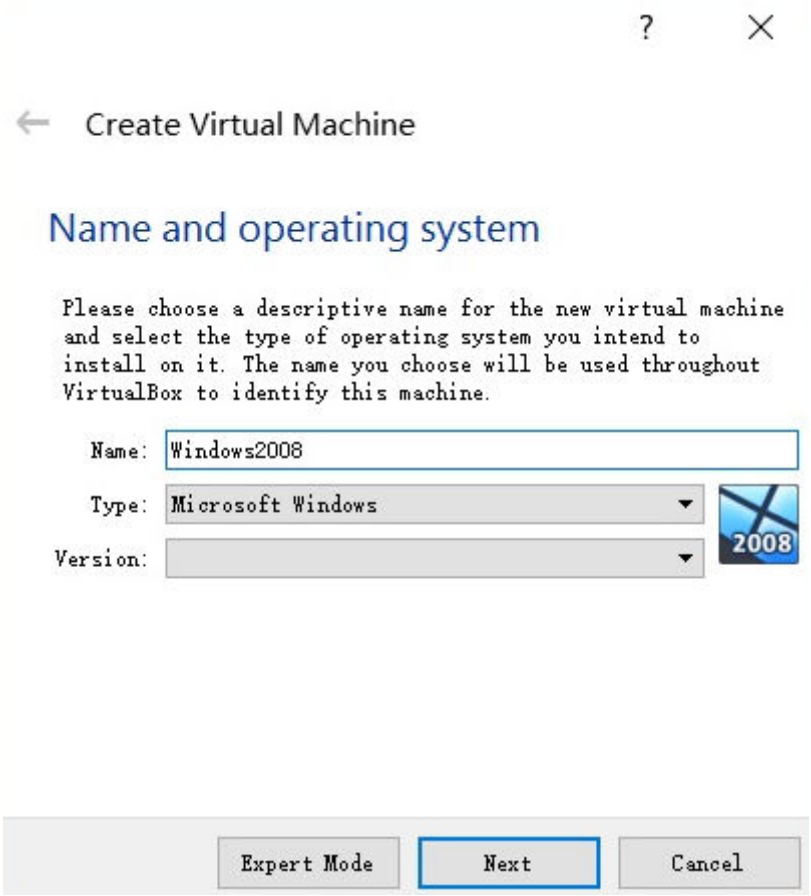
Procedure

1. Open VirtualBox and click **New**. In the displayed **Create Virtual Machine** dialog box, enter the VM name, select the OS type and version, and click **Next**.

   Take Windows 2008 64bit as an example. The OS type must be **Microsoft Windows**.

   Ensure that the selected version is the same as that of the OS to be installed.

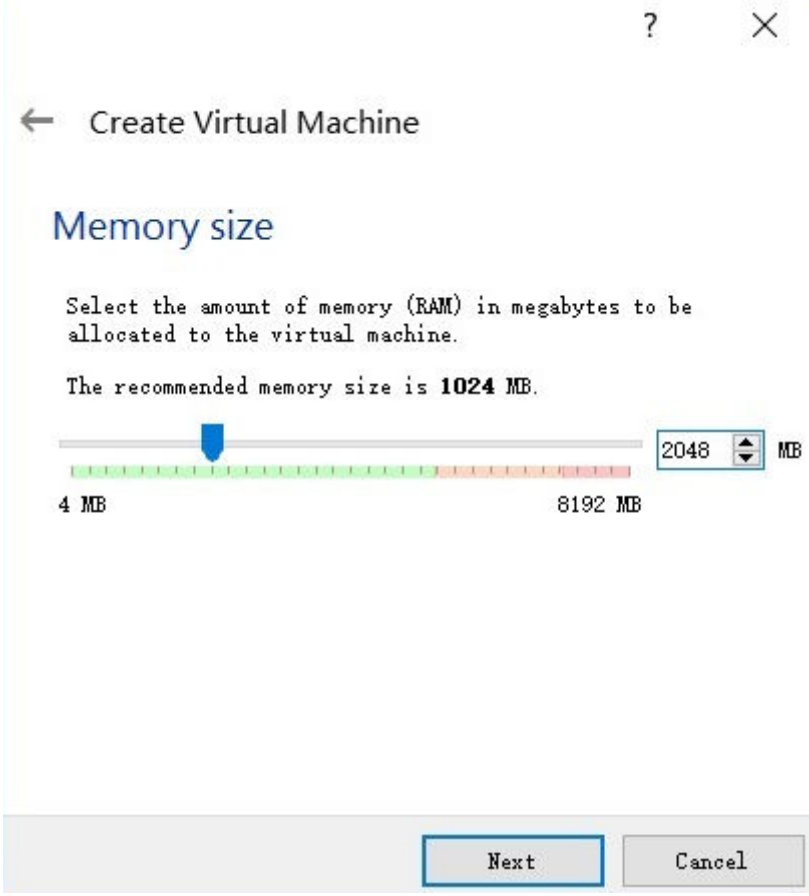
Figure 2-6 Creating a VM



2. In the **Memory size** dialog box, set the memory size and click **Next**.

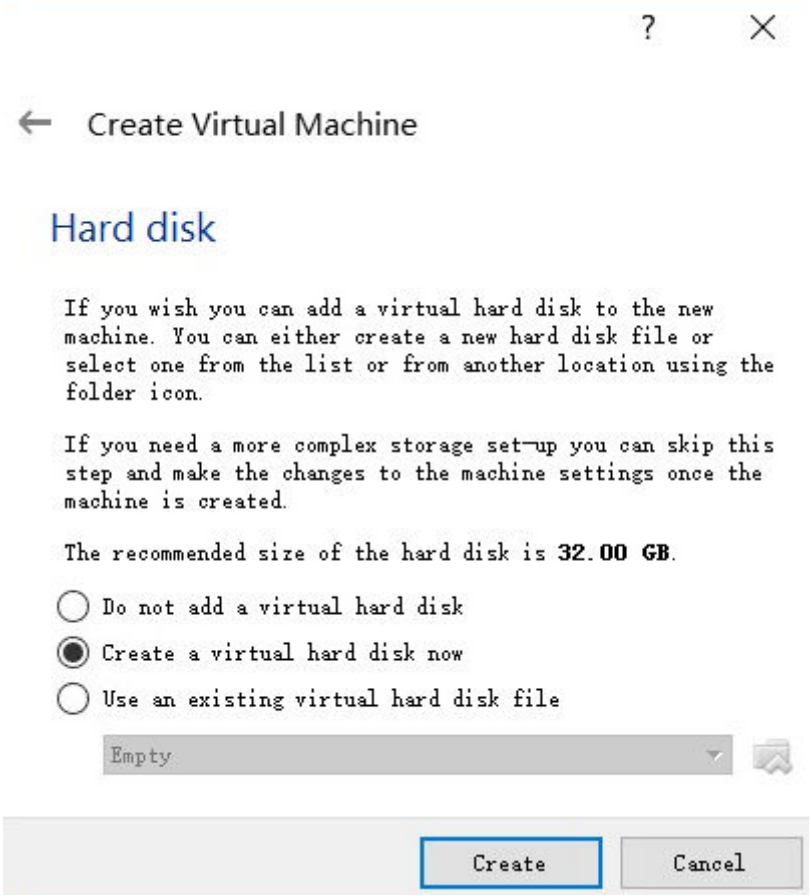
   For details about how to set the memory, see the VM configuration and official requirements for the OS. In this section, the memory is set to 2048 MB.

Figure 2-7 Setting the memory size



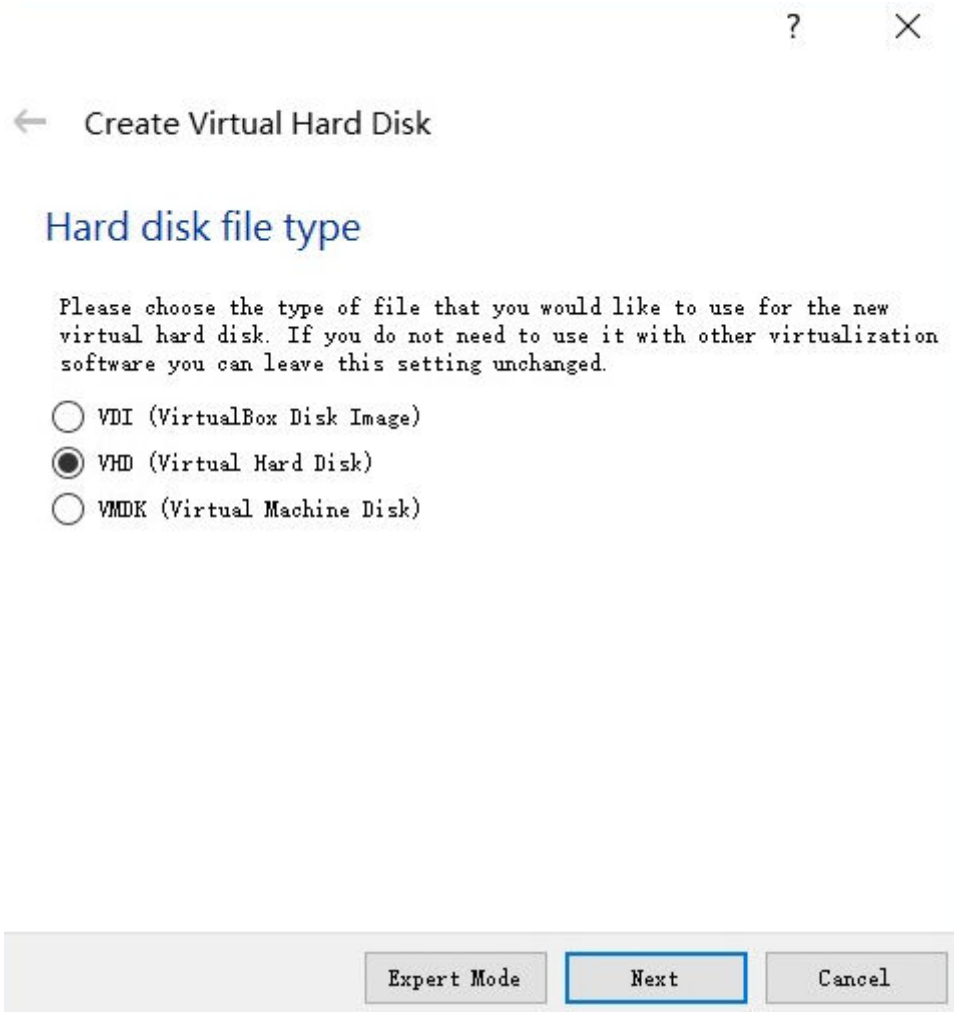
3. In the **Hard disk** dialog box, select **Create a virtual hard disk now** and click **Create**.

Figure 2-8 Creating a virtual hard disk



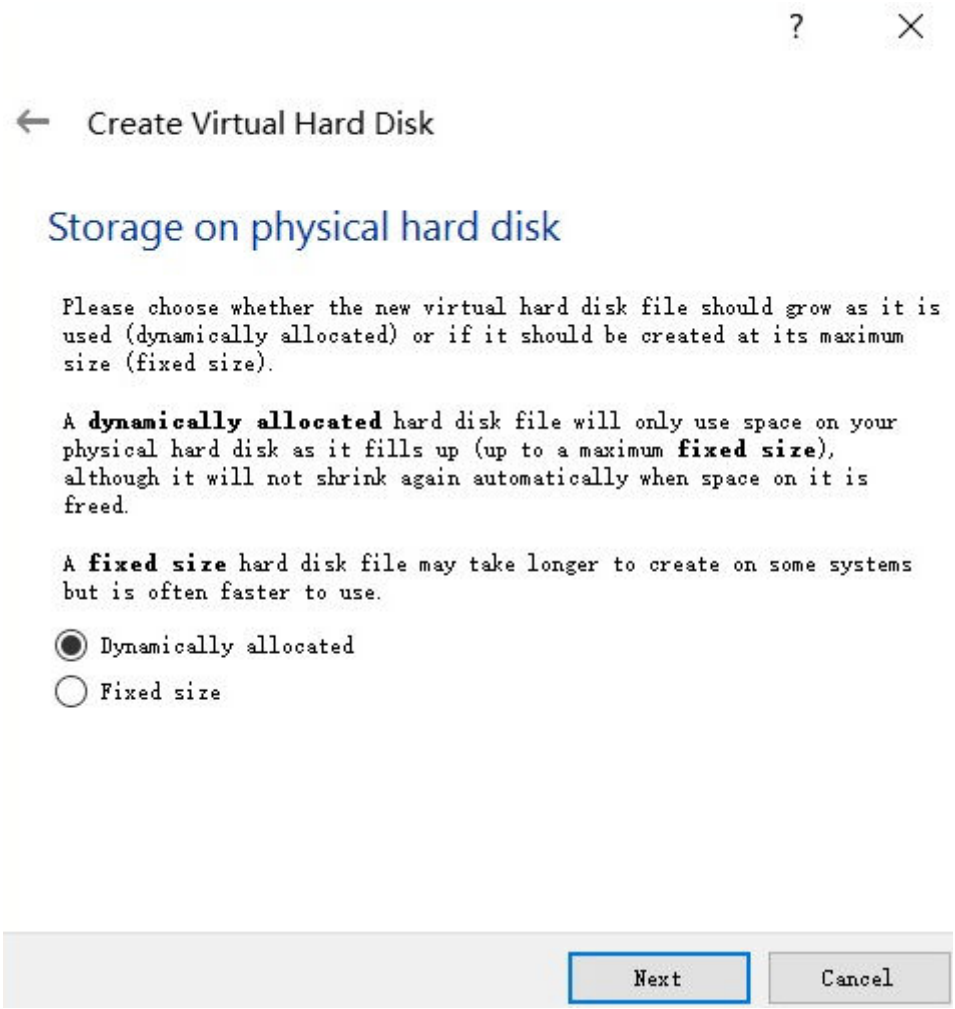
4. In the **Hard disk file type** dialog box, select **VHD** as the file type of the virtual hard disk and click **Next**.

Figure 2-9 Selecting the file type of the virtual hard disk



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

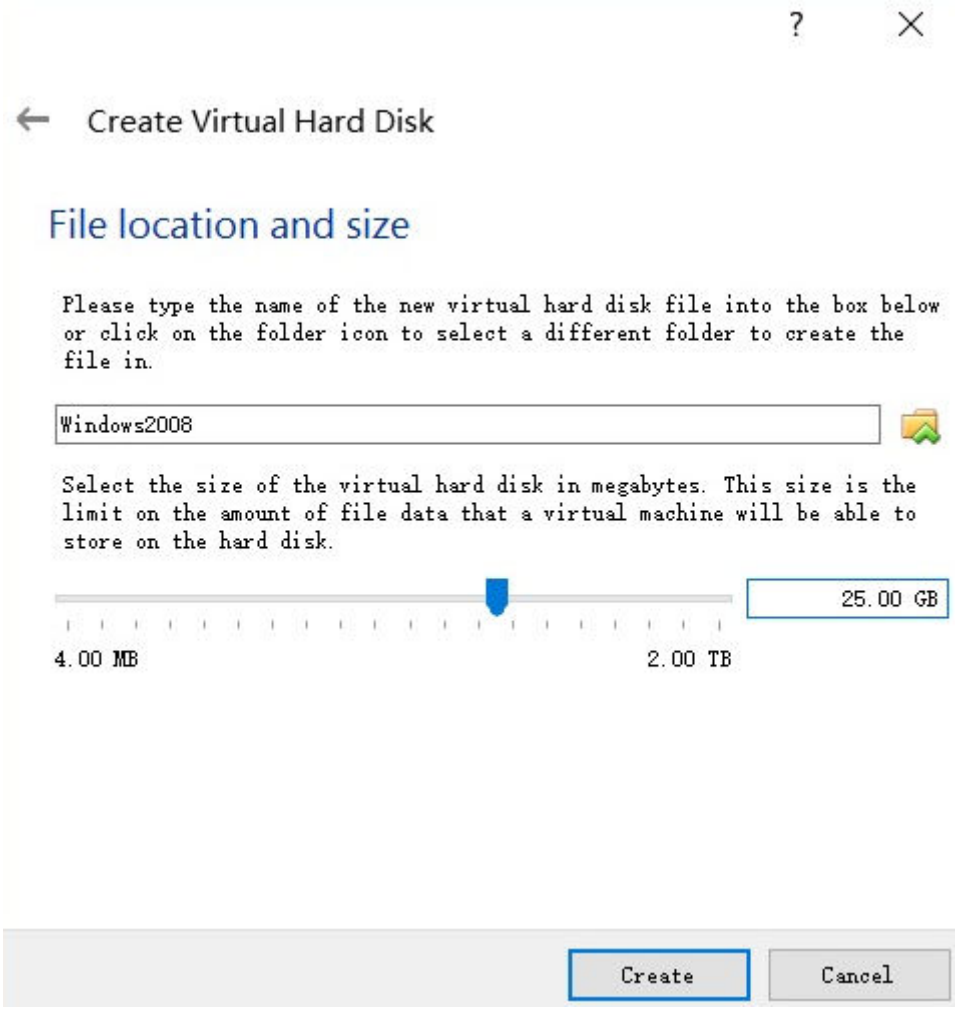
Figure 2-10 Selecting the disk allocation mode



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

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

Figure 2-11 Setting the disk location and size



7. Click **Create**.

2.3.2 Installing Windows on the VM

The installation procedure varies depending on the image file you use. Install the OS as prompted. This section uses Windows Server 2008 R2 as an example to describe how to install a Windows OS on the VM.

NOTE

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

Prerequisites

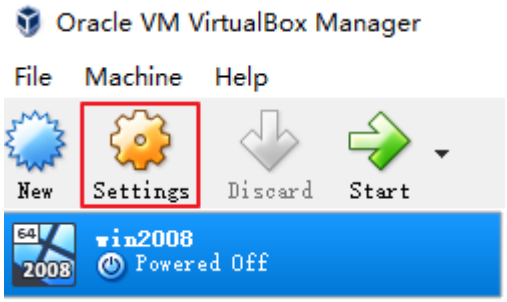
You have obtained the ISO image file, for example, **Windows_server_2008_r2.iso**.

Procedure

Use the ISO file to install the OS for the newly created empty VM.

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

Figure 2-12 Configuring 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

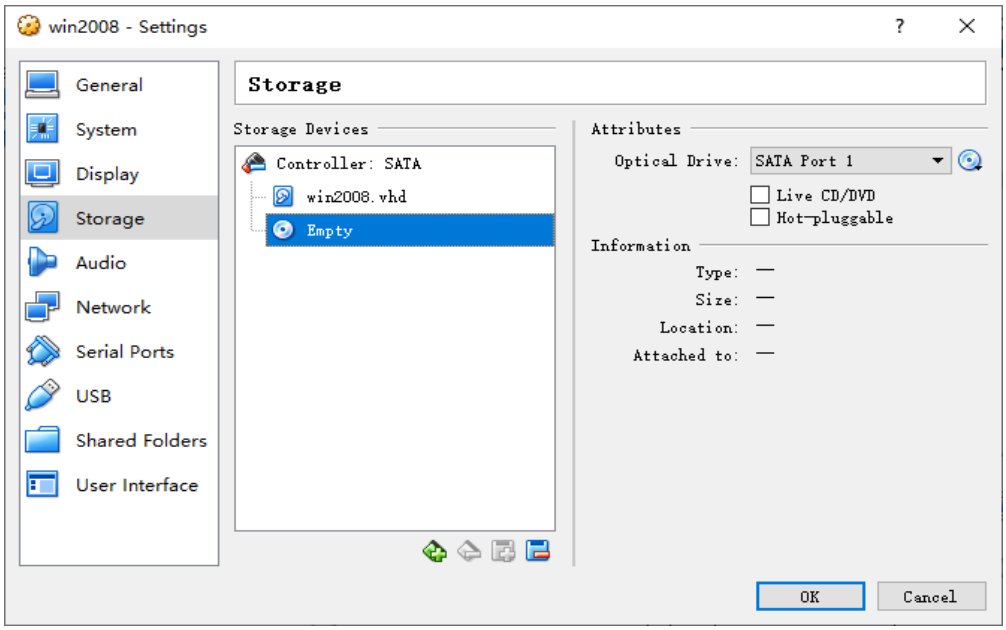
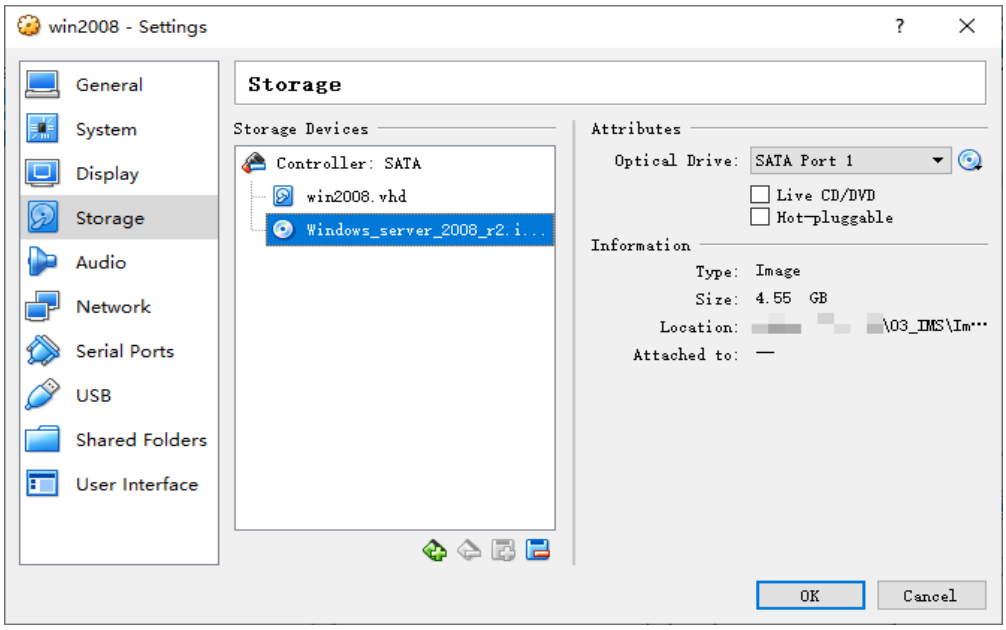
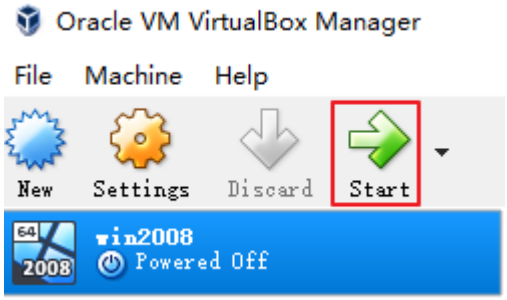


Figure 2-14 Selecting the mounted ISO file



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

2.4.1 Installing UVP VMTools

This section describes how to install UVP VMtools. This operation is mandatory. If UVP VMtools is not installed, the created image will be unavailable.

1. Click **here** to download UVP VMTools.
2. Decompress the UVP VMTools package to obtain **vmtools-windows.iso**.

   vmtools-windows.iso contains all the VMTools packages of applicable OSs. **Setup.exe** automatically identifies the OS type and executes the right VMTools package.
3. On the VirtualBox Windows VM, choose **Device** > **Allocate Drive** > **vmtools-windows.iso**.

4. Choose **Computer** > **CD Drive**.
5. Double-click **Setup.exe** to install UVP VMTools.

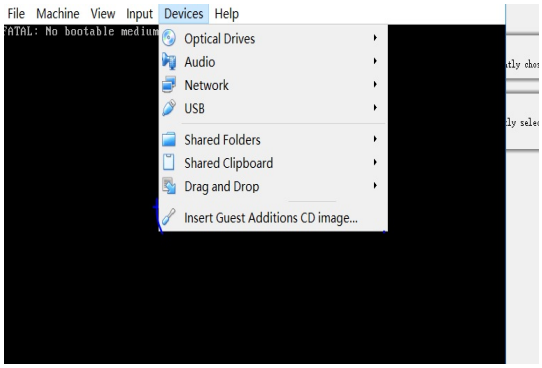
2.4.2 Installing VirtualBox Guest Additions on the Windows VM

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

Procedure

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

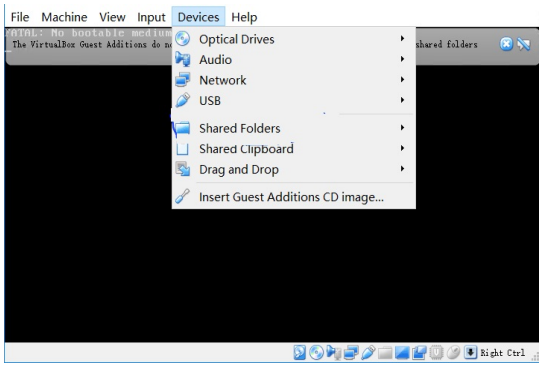
   Figure 2-16 Installing Guest Additions

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.

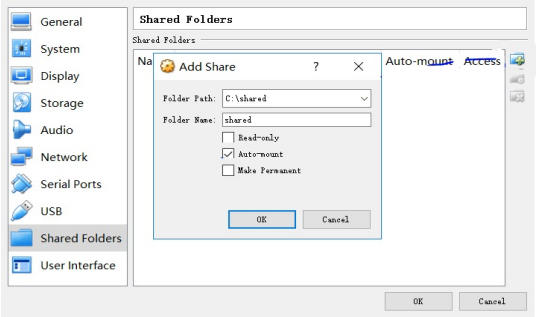
   Figure 2-17 Verifying the installation

4. Set the folder sharing mode.

   Select the folder path on the host where VirtualBox has been installed. After the folder is shared, you can access the folder on the VirtualBox VM.

Figure 2-18 Setting the folder sharing mode



2.4.3 (Optional) Installing Cloudbase-Init

To configure the ECS created from an image (for example, changing the ECS password), you are advised to install Cloudbase-Init. If you do not install it, the ECS cannot be configured and you can log in to the ECS only with the image password.

Install Cloudbase-Init

1. Download the Cloudbase-Init installation package.

   The version of Cloudbase-Init may vary depending on the OS bit. The downloaded package must be saved to a local shared folder (download path: **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 installation package to the newly created VM, and double-click the installation package.

   In this section, **CloudbaseInitSetup_0_9_11_x64** is used as an example.

Configure Cloudbase-Init

1. Edit configuration file **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf** in the Cloudbase-Init installation path.

   a. Add **netbios_host_name_compatibility=false** to the last line of the file so that the hostname supports a maximum of 63 characters.

   NOTE

   NetBIOS contains no more than 15 characters due to Windows system restrictions.

   b. Add **metadata_services=cloudbaseinit.metadata.services.httpservice.HttpService** to enable the agent to access the IaaS OpenStack data source.

   c. (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
   ```

   d. (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
   ```


e. **(Optional)** When the Cloudbase-Init version is 0.9.12 or later, you can customize the length of the password.

Change the value of **user_password_length** to customize the password length.

f. (Optional) Add configuration item **first_logon_behaviour=no** to the **cloudbase-init.conf** configuration file in the **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf** directory to disable the function of changing the password.

Add **first_logon_behaviour=no**.

2. Release the current DHCP address so that the created ECS can obtain the 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 ECS is 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 2-1 SAN policies

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

a. Execute **cmd.exe** and run the following command to query the current SAN policy of the ECS using DiskPart:

diskpart

b. Run the following command to view the SAN policy of the ECS:

san

- If the SAN policy is **OnlineAll**, run the **exit** command to exit DiskPart.
- If the SAN policy is not **OnlineAll**, go to **3.c**.

c. Run the following command to change the SAN policy of the ECS to **OnlineAll**:

san policy=onlineall

2.4.4 (Optional) Installing the One-Click Password Reset Plug-in

You are advised to install CloudResetPwdAgent on the ECS that is used to create an image. This plug-in allows you to reset the password of each ECS created from the image with a few clicks.

Procedure

1. Download package **CloudResetPwdAgent.zip**, which contains **CloudResetPwdAgent** and **CloudResetPwdUpdateAgent**.

   Decompress the package to a local shared folder after you download it from the following link:

   http://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip
2. Choose **Computer** > **Network** > **VBOXSVR** and 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 both the **CloudResetPwdAgent.Windows** and **CloudResetPwdUpdateAgent.Windows** folders.
   b. View **Task Manager** and check whether the installation is successful.

      If you can find **cloudResetPwdAgent** and **cloudResetPwdUpdateAgent** in the Task Manager, the installation is successful. Otherwise, the installation fails.

      NOTE

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

2.5 Exporting the Image File

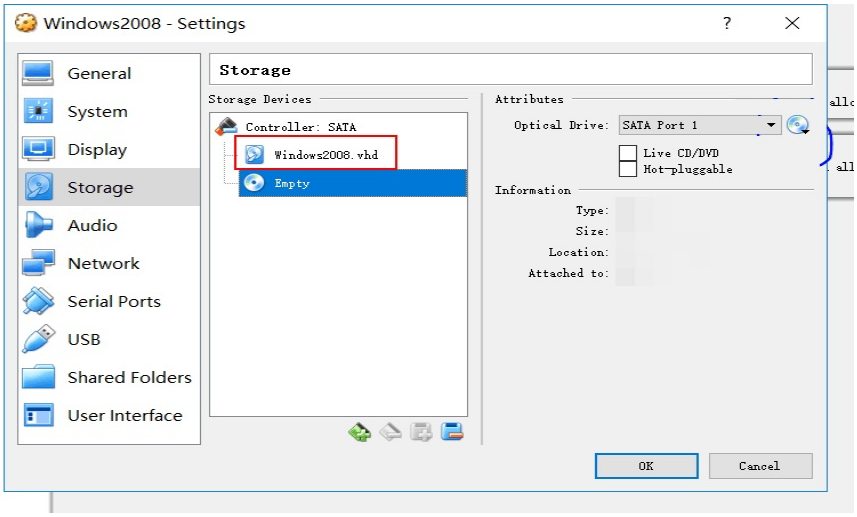
After the VM is configured, you can perform the following operations to obtain the Windows image file:

1. Open VirtualBox, select the newly created VM, choose **Settings** > **Storage**, and select **win2008.vhd**.

   win2008 is the VM name.
2. In the detailed information area on the right, view the storage location of the disk file.

   Enter the path to obtain the generated **win2008.vhd** image file.

Figure 2-19 Viewing the storage path of the disk file



2.6 Uploading and Registering the Image File

Upload the image file to the OBS bucket and register the image.

Constraints

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

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/en-us/browsertg-obs/obs_03_1003.html**.
2. Register the external image file as a private image. For details, see **Registering an Image File as a Private Image (Windows)**.

3 Creating a Linux Image Using VirtualBox and an ISO File

3.1 Introduction

VirtualBox

VirtualBox is a free and open-source hypervisor for x86 computers. Developed initially by InnoTek GmbH from Germany, it was acquired by Oracle Corporation and is now part of Oracle's xVM virtualization platform technology. VirtualBox is a virtualizer for x86 OSs based on the provided 32-bit or 64-bit Windows, Solaris, and Linux OSs. That is, users can install and run Solaris, Windows, DOS, Linux, OS/2 Warp, OpenBSD, and FreeBSD on VirtualBox as client OSs.

For more information about VirtualBox, visit the Oracle official website.

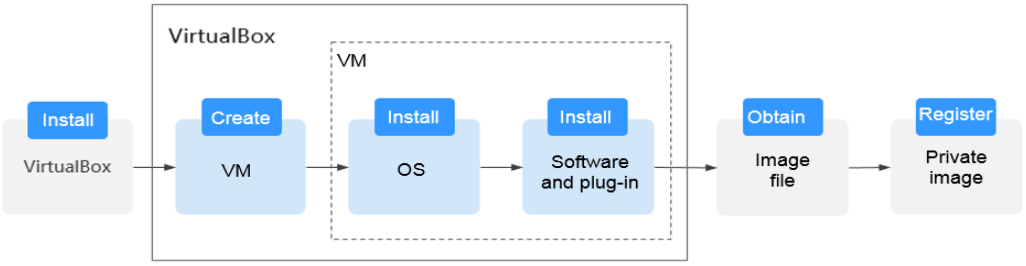
Download the installation package from **https://www.virtualbox.org/wiki/Downloads**.

Click **here** to see the OSs that can work with VirtualBox.

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 machine (64-bit Windows is recommended) and install VirtualBox on the host machine. For details about the preparations and installation process, see **Installing VirtualBox**.
2. Create a VM: Create an empty VM on VirtualBox as the image source. For details, see **Creating an Empty VM**.
3. Install the OS: Mount an ISO file to install an OS for the VM. The OS of the ISO file determines the OS of the image you want to create. For details, see **Installing a Linux OS on the VM**.
4. Install software and plug-ins: To ensure that the image to be created can be used to provision ECSs that 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 **Exporting the Image File**.
6. Register a private image: Upload the exported VHD image file to the OBS bucket and register it as a private image. Then you can use the private image to create ECSs. For details, see **Uploading and Registering the Image File**.

3.2 Installing VirtualBox

This section describes how to install VirtualBox.

Preparations

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

- The host runs a 64-bit Linux OS.
- The host has a memory of at least 4 GB and uses a dual-core processor. For example, the host specifications can be 8U16G.
- The available hard disk space is at least 20 GB.
- The host CPU supports hardware virtualization (Intel VT-x or AMD-V virtualization). For how to enable this, see **Host CPU Settings**.

  NOTE

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

Host CPU Settings

Perform the following operations to enable hardware virtualization on an Intel host:

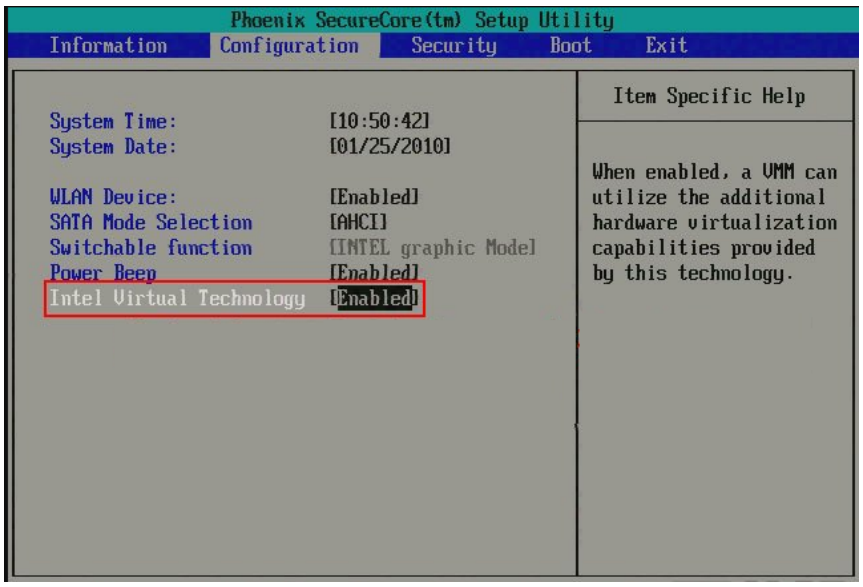
NOTE

The operations may differ depending on the host. You can enable hardware virtualization as prompted.

1. During startup, press the corresponding key to enter the BIOS.
2. Enter the BIOS, choose **Configuration** > **Intel Virtual Technology**, and press **Enter**.

3. Move the cursor to **Enabled** and press **Enter**. The value of **Intel Virtual Technology** will become **Enabled**.
4. Press **F10** to save the settings and exit. The hardware virtualization function is enabled.

Figure 3-2 Enabling the hardware virtualization function

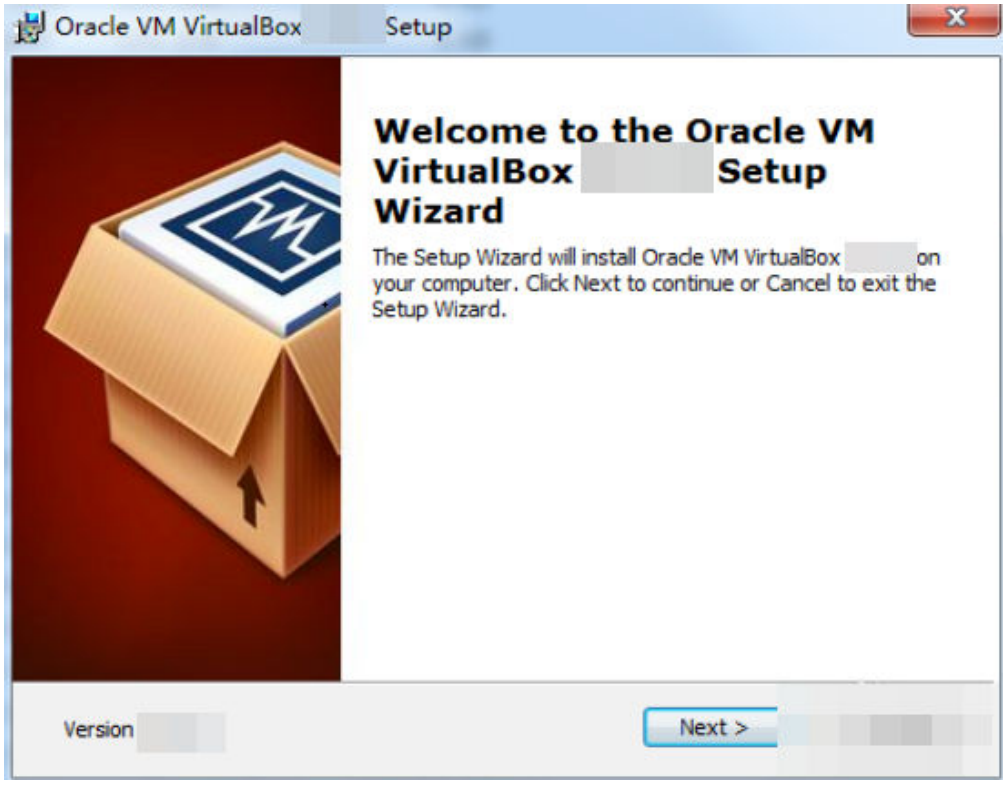


Procedure

1. Download the VirtualBox installation package.

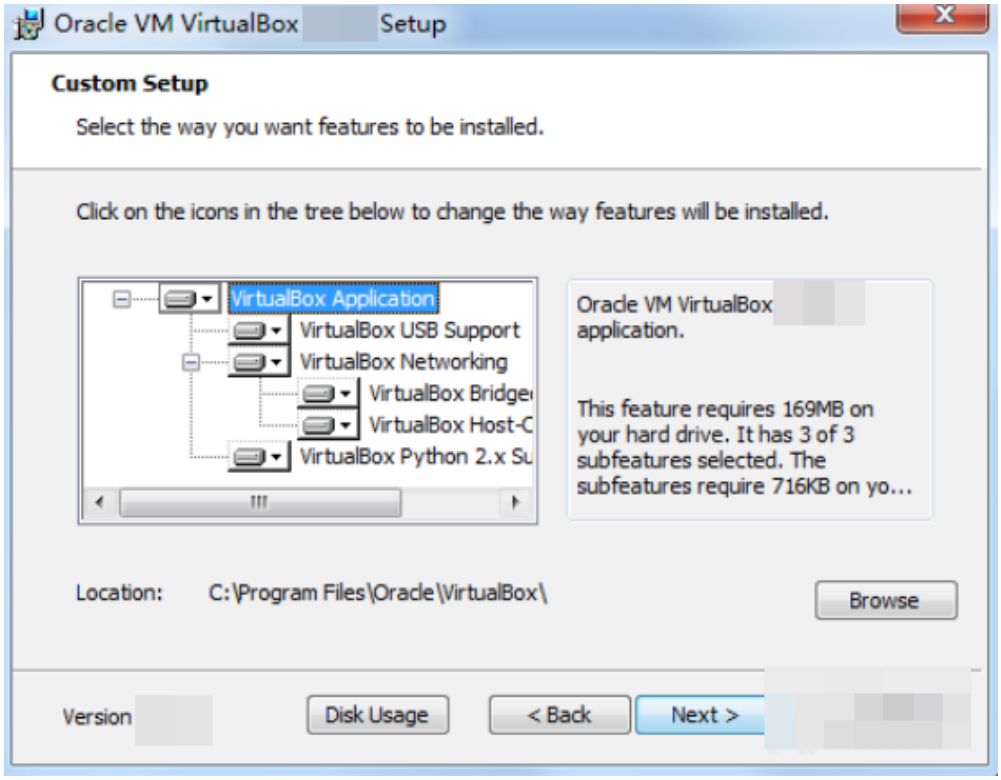
   Download the installation package from **https://www.virtualbox.org/wiki/Downloads**.
2. Decompress the installation package. Take VirtualBox-5.2.0 as an example. Right-click **VirtualBox-5.2.0-118431-Win.exe**, choose **Run as administrator**, and complete the installation as prompted.

Figure 3-3 Installing VirtualBox



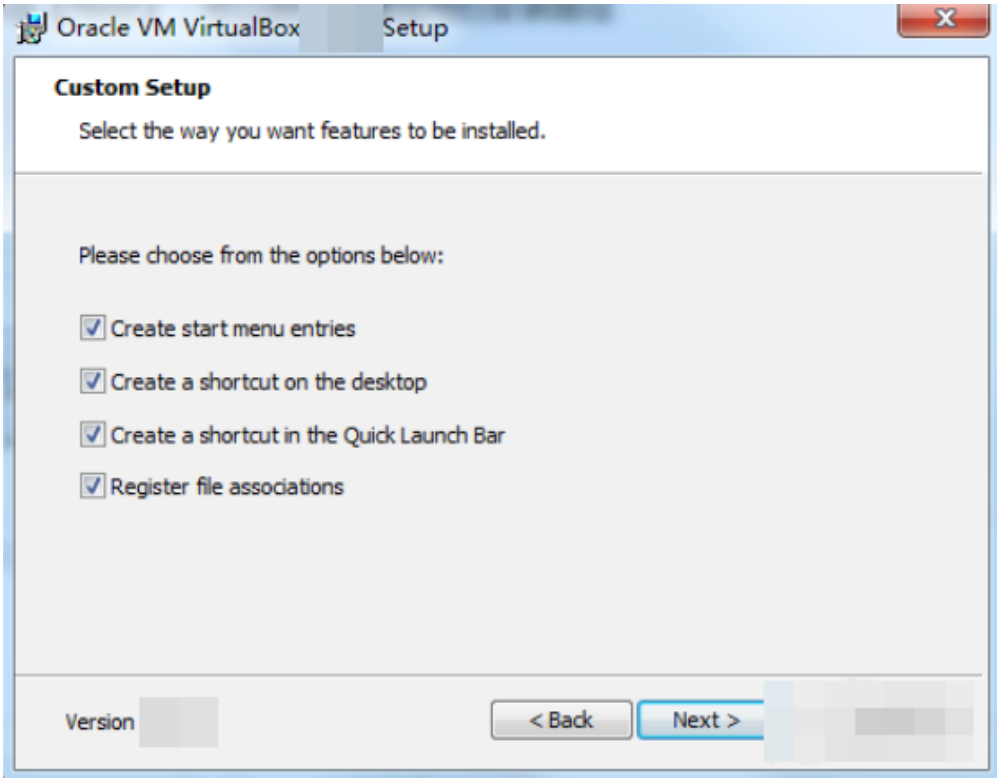
3. Select the VirtualBox installation path and click **Next**.

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 the OS

This section describes how to create an empty VM and install the OS on the VM after installing VirtualBox.

3.3.1 Creating an Empty VM

This section describes how to create an empty VM.

Prerequisites

VirtualBox has been installed.

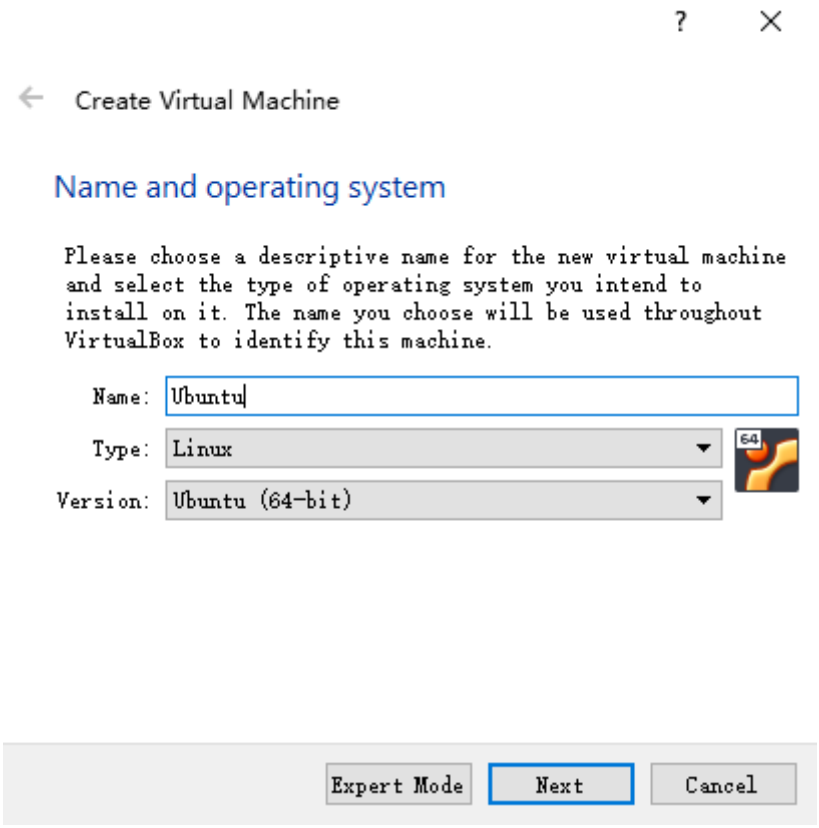
Procedure

1. Open VirtualBox and click **New**. In the displayed **Create Virtual Machine** dialog box, enter the VM name, select the 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 to be installed.

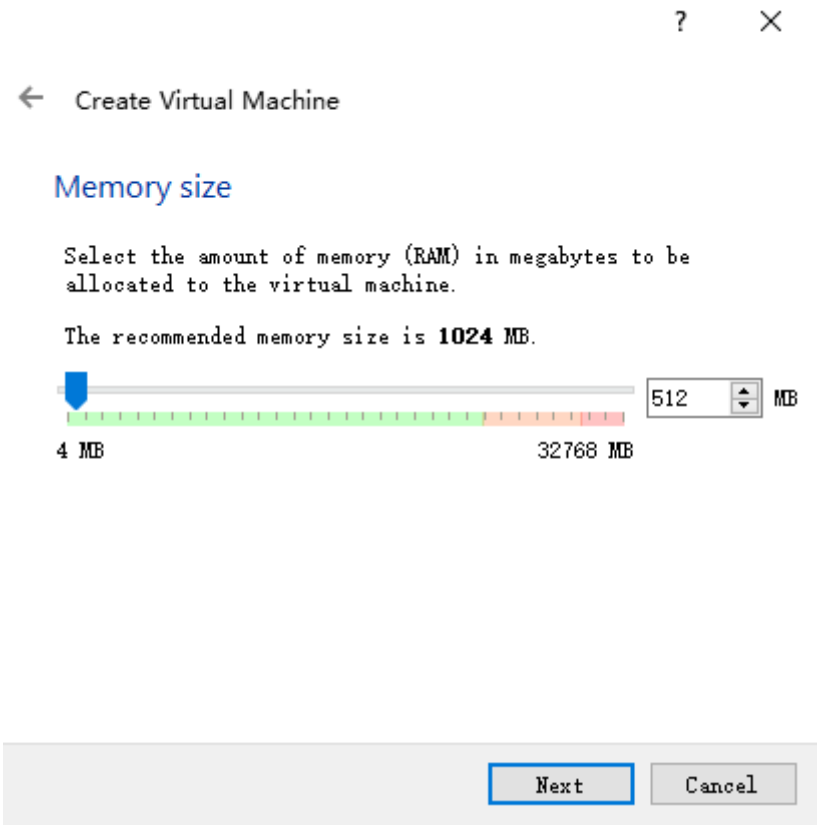
Figure 3-6 Creating a VM



2. In the **Memory size** dialog box, set the memory size and click **Next**.

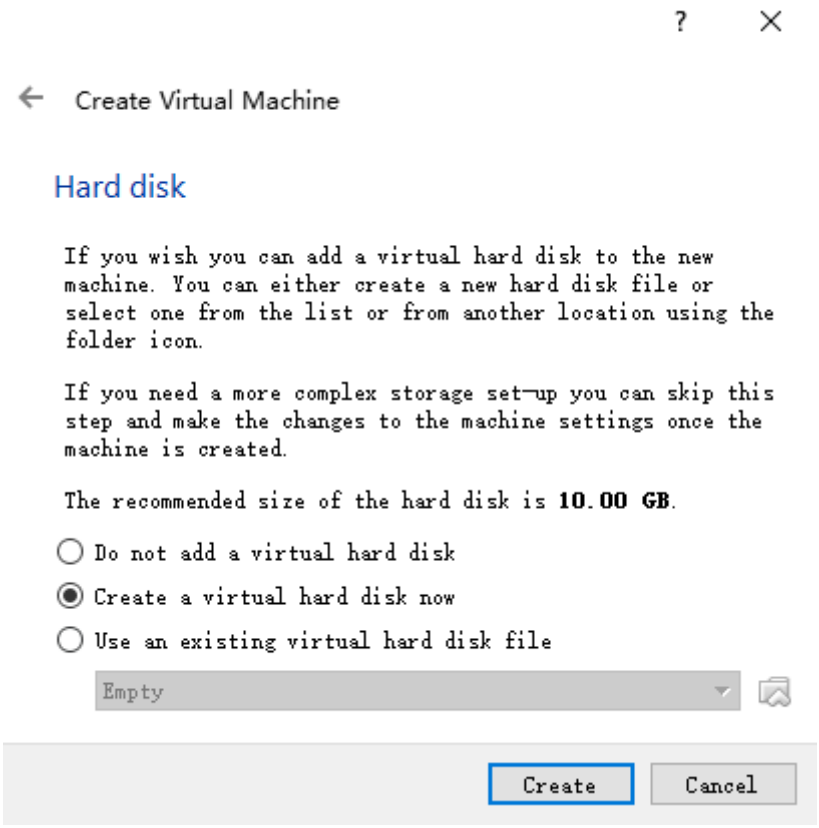
   For details about how to set the memory, see the VM configuration and official requirements for the OS. The default minimum size is 256 MB. This document uses 512 MB as an example.

Figure 3-7 Setting the memory size



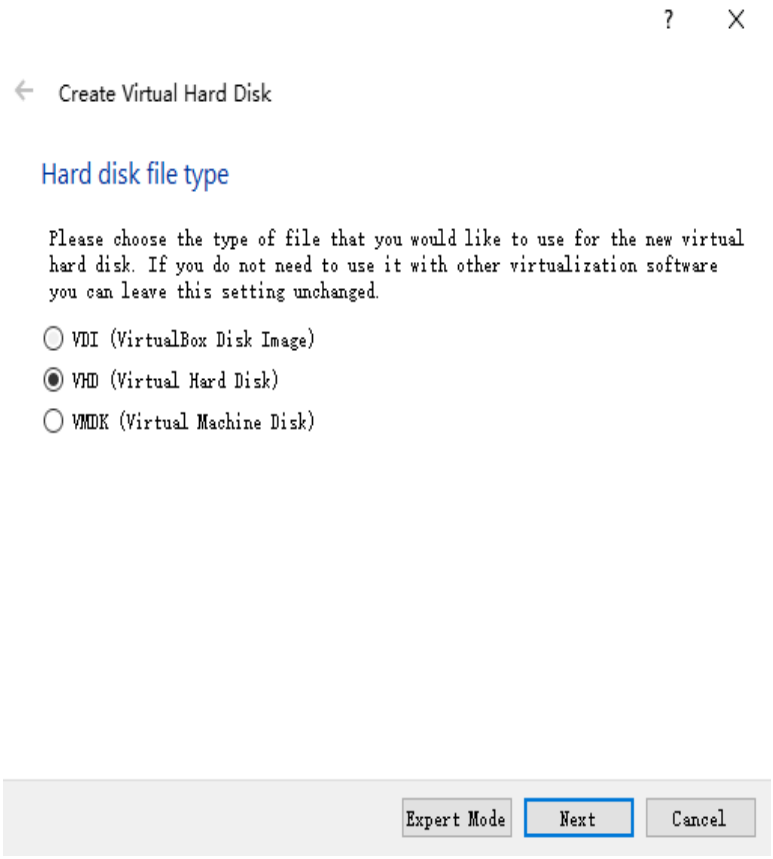
3. In the **Hard disk** dialog box, select **Create a virtual hard disk now** and click **Create**.

Figure 3-8 Creating a virtual hard disk



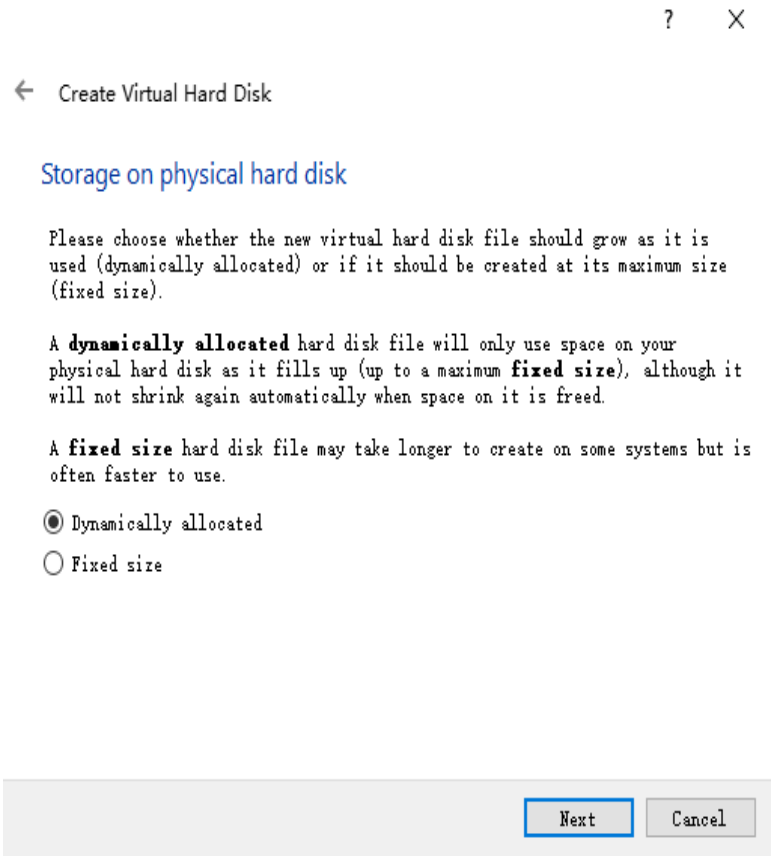
4. In the **Hard disk file type** dialog box, select **VHD** as the file type of the virtual hard disk and click **Next**.

Figure 3-9 Selecting the file type of the virtual hard disk



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

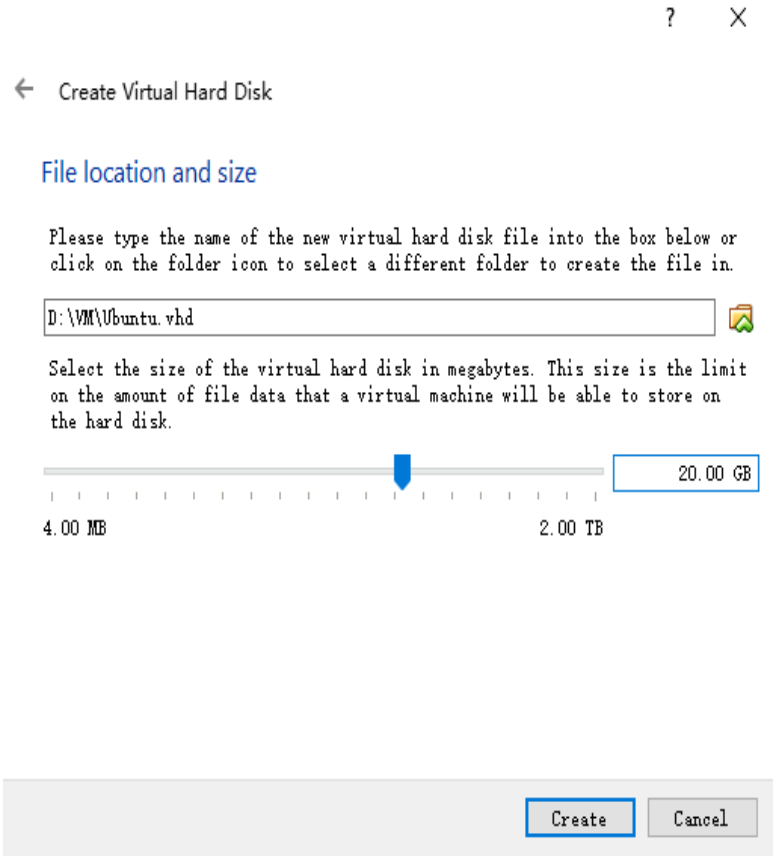
Figure 3-10 Selecting the disk allocation mode



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

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

Figure 3-11 In the **File location and size** dialog box, set the disk size and storage location.



7. Click **Create**.

3.3.2 Installing a Linux OS on the VM

The installation procedure varies depending on the image file you use. Install the OS as prompted. This section uses Ubuntu 14.04 as an example to describe how to install a Linux OS on the VM.

Prerequisites

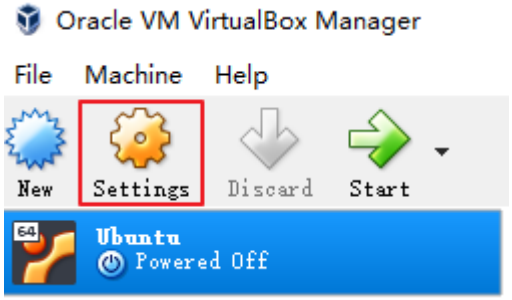
You have obtained the ISO image file, for example, **Ubuntu-14.04-server.iso**.

Procedure

Use the ISO file to install the OS for the newly created empty VM.

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

Figure 3-12 Configuring the VM



2. Choose **Storage** > **Empty**, click  in the **Attributes** area, and select the ISO image file **Ubuntu-14.04-server.iso**.

Figure 3-13 Selecting the ISO file to be mounted

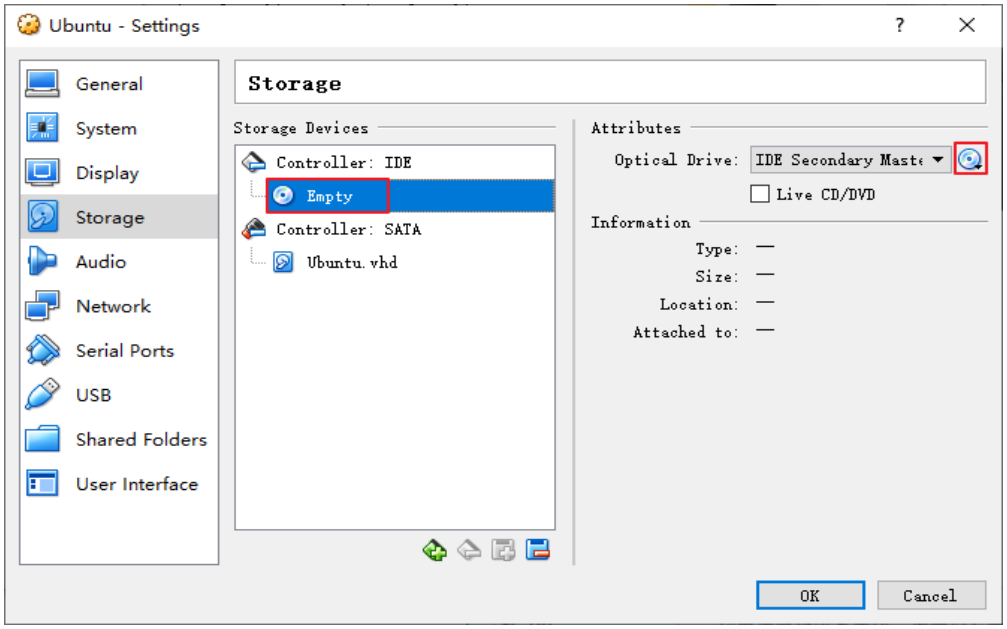
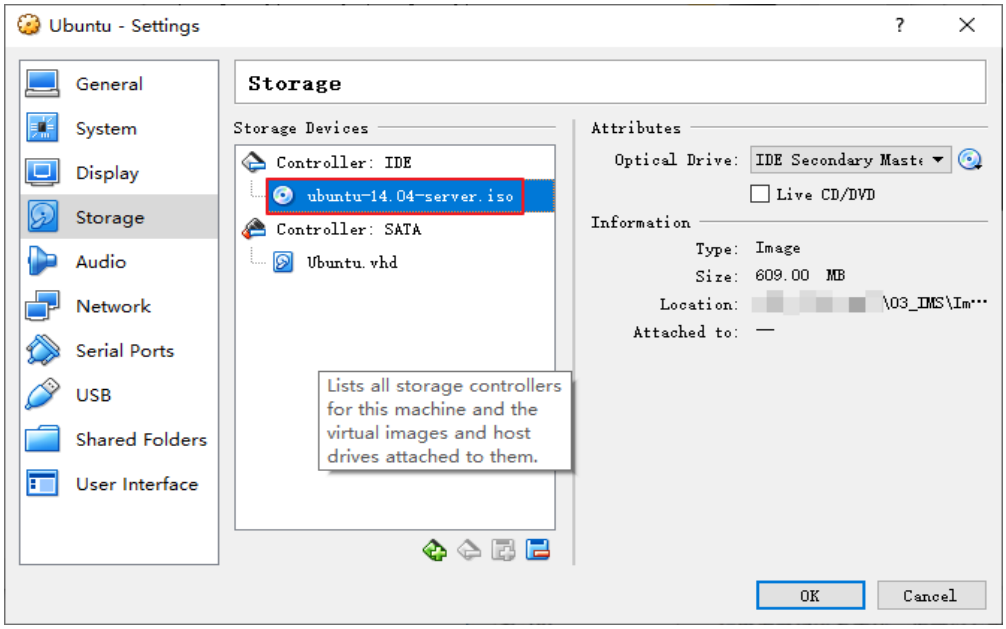
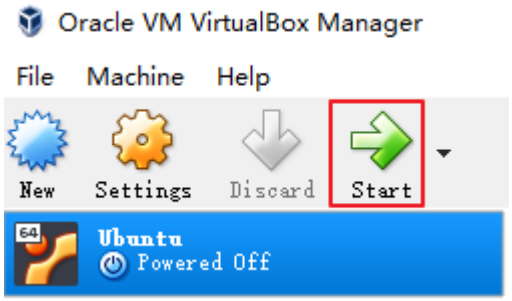


Figure 3-14 Selecting the mounted ISO file



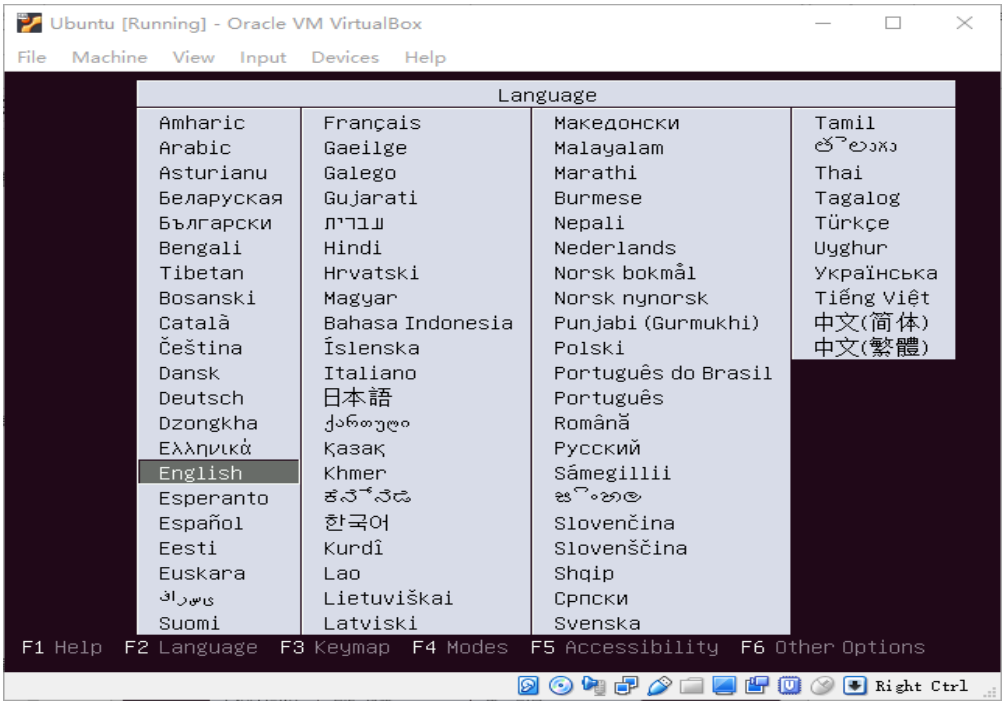
3. Click **OK**.
4. In VirtualBox Manager, select the new VM and click **Start**.

Figure 3-15 Starting the VM



5. Install the OS as prompted.

Figure 3-16 Installing the OS



NOTE

When installing the OS, you are advised to use only one partition, that is to say, the root partition.

When customizing the root partition, select **Standard Partition** and use file system ext3 or ext4 and partition table MSDOS. The root partition must be a primary partition.

3.4 Configuring the VM

3.4.1 Optimizing the VM

To ensure that ECSs created using a private image support both Xen and KVM virtualization, you must optimize the private image before its creation.

This section describes how to optimize a Linux VM that runs Ubuntu 14.04. For the optimization operations of other OSs, see **Optimization Process (Linux)**.

Installing Native Xen and KVM Drivers

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

   vi /etc/initramfs-tools/modules

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

```
[root@CTU10000xxxxx ~]#vi /etc/initramfs-tools/modules
...
# Examples:
#
```



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

3. Press **Esc**, enter **:wq**, and press **Enter** to save the settings and exit the vi editor.
4. Run the following command to generate initramfs again:

   update-initramfs -u

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

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

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

```
[root@ CTU10000xxxxx home]# lsinitramfs /boot/initrd.img-`uname -r` |grep xen
lib/modules/3.5.0-23-generic/kernel/drivers/net/ethernet/qlogic/netxen
lib/modules/3.5.0-23-generic/kernel/drivers/net/ethernet/qlogic/netxen/netxen_nic.ko
lib/modules/3.5.0-23-generic/kernel/drivers/net/xen-netback
lib/modules/3.5.0-23-generic/kernel/drivers/net/xen-netback/xen-netback.ko
lib/modules/3.5.0-23-generic/kernel/drivers/block/xen-blkback
lib/modules/3.5.0-23-generic/kernel/drivers/block/xen-blkback/xen-blkback.ko

[root@ CTU10000xxxxx 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, VM running will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the **lsinitrd** command. You can run the following commands to check whether the drivers are built-in ones in the kernel:

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

Changing the Disk Identifier in the GRUB Configuration File to UUID

Take Ubuntu 14.04 for example. Run **blkid** to obtain the UUID of the root partition. Modify the **/boot/grub/grub.cfg** file and use the UUID of the root partition to configure the boot item. If the root partition already uses UUID, no modification is required. The procedure is as follows:

1. Log in to the newly created VM as user **root**.
2. Run the following command to query all types of mounted file systems and the 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. Run the following command to query the **grub.cfg** file:

   cat /boot/grub/grub.cfg

   The following information is displayed:

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

4. Search for **root=/dev/xvda1** or **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34** is contained in the **/boot/grub/grub.cfg** configuration file.
   - If **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34** exists in the configuration file, the root partition is in the UUID format and requires no change.
   - If **root=/dev/xvda1** exists in the configuration file, the root partition is in the device name format. Go to step 5.
5. Obtain the UUID of the root partition based on **root=/dev/xvda1** and information obtained by running the **blkid** command.
6. Run the following command to open the **grub.cfg** file:

   vi /boot/grub/grub.cfg
7. Press **i** to enter editing mode. Use UUID to represent the root partition. 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. Run the following command to verify the change:

   cat /boot/grub/grub.cfg

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

```
......menuentry 'Ubuntu Linux, with Linux 3.13.0-24-generic' --class ubuntu --class gnu-linux --class
gnu --class os --unrestricted $menuentry_id_option '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
}
```

Changing the Disk Identifier in the fstab File to UUID

Take Ubuntu 14.04 for 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. Run the following command to query all types of mounted file systems and the 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. Run the following command to query the **fstab** file:

   cat /etc/fstab

   The following information is displayed:

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

3. Check whether the disk identifier in the **fstab** file is the device name.
   - If the disk is represented by UUID, no further operation is required.
   - If the disk is represented by the device name, go to step **4**.
4. Run the following command to open the **fstab** file:

   vi /etc/fstab

5. Press **i** to enter editing mode and change the disk identifier to UUID.
6. Press **Esc**, enter **:wq**, and press **Enter** to save the settings and exit the vi editor.

3.4.2 Installing Cloud-Init

Scenarios

To ensure that you can use the user data injection function to inject initial custom information into ECSs created from a private image (such as setting the ECS login password), install Cloud-Init on the ECS used to create the image.

- You need to download Cloud-Init from its official website. Therefore, you must bind an EIP to the ECS.
- If Cloud-Init is not installed, you cannot configure an ECS. As a result, you can only use the password in the image file to log in to the created ECSs.
- By default, ECSs created from a public image have Cloud-Init installed. You do not need to install or configure Cloud-Init on such ECSs.
- For ECSs created using an external image file, install and configure Cloud-Init by performing the operations in this section. For how to configure Cloud-Init, see **Configuring Cloud-Init**.

Prerequisites

- An EIP has been bound to the ECS.
- You have logged in to the ECS.
- The IP address obtaining mode of the ECS is DHCP.

Procedure

1. Check whether Cloud-Init has been installed.

   For details, see **Check Whether Cloud-Init Has Been Installed**.
2. Install Cloud-Init.

   You can install Cloud-Init in any of the following ways: **(Recommended) Install Cloud-Init Using the Official Installation Package**, **Install Cloud-Init Using the Official Source Code Package and pip**, and **Install Cloud-Init Using the Source Code**.

Check Whether Cloud-Init Has Been Installed

Perform the operations provided here to check whether Cloud-Init has been installed.

The methods of checking whether Cloud-Init is installed vary depending on the OSs. Take CentOS 6 as an example. Run the following command to check whether Cloud-Init is installed:

rpm -qa |grep 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 Cloud-Init has been installed, perform the following operations:

- Check whether to use the certificate in the ECS OS. If the certificate is no longer used, delete it.
  - If the certificate is stored in a directory of user **root**, for example, */$path/$to/$root*/**.ssh/authorized_keys**, run the following commands:

    cd /root/.ssh

    rm authorized_keys
  - If the certificate is not stored in a directory of user **root**, for example, */$path/$to/$none-root*/**.ssh/authorized_keys**, run the following commands:

    cd /home/centos/.ssh

    rm authorized_keys
- Run the following command to delete the cache generated by Cloud-Init and ensure that the ECS created from the private image can be logged in by using the certificate:

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

  NOTE

  Do not restart the ECS after performing the configuration. Otherwise, you need to configure it again.

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

The method of installing Cloud-Init on an ECS varies depending on the OS. Perform the installation operations as user **root**.

The following describes how to install Cloud-Init on an ECS running SUSE Linux, CentOS, Fedora, Debian, and Ubuntu. For other OS types, install the required type of Cloud-Init. For example, you need to install coreos-cloudinit on ECSs running CoreOS.

- SUSE Linux

  Paths for obtaining the Cloud-Init installation package for SUSE Linux

  http://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/

  http://download.opensuse.org/repositories/Cloud:/Tools/

  NOTE

  Select the required repo installation package in the provided paths.

  Take SUSE Enterprise Linux Server 12 as an example. Perform the following steps to install Cloud-Init:

  a. Log in to the ECS used to create a Linux private image.

  b. Run the following command to install the network installation source for SUSE Enterprise Linux Server 12:

     zypper ar http://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/SLE_12/Cloud:Tools.repo

  c. Run the following command to update the network installation source:

     zypper refresh

  d. Run the following command to install Cloud-Init:

     zypper install cloud-init

  e. Run the following commands to enable Cloud-Init to automatically start upon system boot:

     - SUSE 11

       chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config on; chkconfig cloud-final on

       service cloud-init-local status; service cloud-init status; service cloud-config status; service cloud-final status

     - SUSE 12 and openSUSE 12/13/42

       systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

       systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

CAUTION

For SUSE and openSUSE, perform the following steps to disable dynamic change of the ECS name:

1. Run the following command to open the **dhcp** file using the vi editor:

   vi etc/sysconfig/network/dhcp

2. Change the value of **DHCLIENT_SET_HOSTNAME** in the **dhcp** file to **no**.

- **CentOS**

  Table 3-1 lists the Cloud-Init installation paths for CentOS. Select the required installation package from the following addresses.

  Table 3-1 Cloud-Init installation package addresses

OS Type	Version	How to Obtain
CentOS	6 32-bit	https://dl.fedoraproject.org/pub/epel/6/i386/
	6 64-bit	https://dl.fedoraproject.org/pub/epel/6/x86_64/
	7 64-bit	https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-12.noarch.rpm

  Run the following commands to install Cloud-Init on an ECS running CentOS 6.5 64-bit (example):

  yum install https://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-*xx-xx*.noarch.rpm

  yum install cloud-init

  NOTE

  xx-xx indicates the version of Extra Packages for Enterprise Linux (EPEL) required by the current OS.

- Fedora

  Before installing Cloud-Init, ensure that the network installation source address has been configured for the OS by checking whether the **/etc/yum.repo.d/fedora.repo** file contains the installation source address of the software package. If the file does not contain the address, configure the address by following the instructions on the Fedora official website.

  Run the following command to install Cloud-Init:

  yum install cloud-init

- Debian and Ubuntu

  Before installing Cloud-Init, ensure that the network installation source address has been configured for the OS by checking whether the **/etc/apt/sources.list** file contains the installation source address of the software

package. If the file does not contain the address, configure the address by following the instructions on the Debian or Ubuntu official website.

Run the following commands to install Cloud-Init:

apt-get update

apt-get install cloud-init

Install Cloud-Init Using the Official Source Code Package and pip

The following operations use Cloud-Init 0.7.9 as an example to describe how to install Cloud-Init.

1. Download the **cloud-init-0.7.9.tar.gz** source code package (version 0.7.9 is recommended) and upload it to the **/home/** directory of the ECS.

   Download **cloud-init-0.7.9.tar.gz** from the following path:

   https://launchpad.net/cloud-init/trunk/0.7.9/+download/cloud-init-0.7.9.tar.gz

2. Create a **pip.conf** file in the **~/.pip/** directory and edit the following content:

   NOTE

   If the **~/.pip/** directory does not exist, run the **mkdir ~/.pip** command to create it.

   ```
   [global]
   index-url  = https://<$mirror>/simple/
   trusted-host = <$mirror>
   ```

   NOTE

   Replace *<$mirror>* with a public network PyPI source.

   Public network PyPI source: **https://pypi.python.org/**

3. Run the following command to install the downloaded Cloud-Init source code package (select **--upgrade** as needed during installation):

   pip install [--upgrade] /home/cloud-init-0.7.9.tar.gz

4. Run the **cloud-init -v** command. Cloud-Init is installed successfully if the following information is displayed:

   ```
   cloud-init 0.7.9
   ```

5. Enable Cloud-Init to automatically start upon system boot.
   - If the OS uses SysVinit to manage automatic start of services, run the following commands:

     chkconfig --add cloud-init-local; chkconfig --add cloud-init; chkconfig --add cloud-config; chkconfig --add cloud-final

     chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config on; chkconfig cloud-final on

     service cloud-init-local status; service cloud-init status; service cloud-config status; service cloud-final status
   - If the OS uses Systemd to manage automatic start of services, run the following commands:

     systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

     systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

CAUTION

If you install Cloud-Init using the official source code package and pip, pay attention to the following:

1. Add user **syslog** to the **adm** group during the installation. If user **syslog** exists, add it to the **adm** group. For some OSs (such as CentOS and SUSE), user **syslog** may not exist. Run the following commands to create user **syslog** and add it to the **adm** group:

   useradd syslog

   groupadd adm

2. Change the value of **distro** in **system_info** in the **/etc/cloud/cloud.cfg** file based on the OS release version, such as **distro: ubuntu**, **distro: sles**, **distro: debian**, and **distro: fedora**.

Install Cloud-Init Using the Source Code

The Cloud-Init configuration is included in the source code package. Therefore, you do not need to configure Cloud-Init after the installation. Perform the following steps to install Cloud-Init: You can obtain the Cloud-Init package from Github at **https://github.com/huaweicloud/huaweicloud-cloud-init**.

1. Run the following commands to download the Cloud-Init package and copy it to the **/tmp/CLOUD-INIT** folder:

   NOTE

   Download the Cloud-Init 0.7.6 package at https://github.com/huaweicloud/huaweicloud-cloud-init/archive/cloud-init-0.7.6.zip.

   Download the Cloud-Init 0.7.9 package at following website: https://github.com/huaweicloud/huaweicloud-cloud-init/archive/cloud-init-0.7.9.zip.

   wget https://github.com/huaweicloud/huaweicloud-cloud-init/archive/cloud-init-0.7.6.zip

   mkdir /tmp/CLOUD-INIT

   cp cloud-init-0.7.6.zip /tmp/CLOUD-INIT

   cd /tmp/CLOUD-INIT

2. Run the following command to decompress the package:

   unzip cloud-init-0.7.6.zip

3. Run the following command to enter the **cloud-init-0.7.6** folder:

   cd huaweicloud-cloud-init-cloud-init-0.7.6

4. Install the Cloud-Init package. The commands vary depending on the OS type.
   - For CentOS 6.x or SUSE 11.x, run the following commands:

     python setup.py build

     python setup.py install --init-system sysvinit
   - For CentOS 7.x or SUSE 12.x, run the following commands:

     python setup.py build

     python setup.py install --init-system systemd

NOTE

Add user **syslog** to the **adm** group during the installation. If user **syslog** exists, add it to the **adm** group. For some OSs (such as CentOS and SUSE), user **syslog** may not exist. Run the following commands to create user **syslog** and add it to the **adm** group:

useradd syslog

groupadd adm

5. Enable Cloud-Init to automatically start upon system boot.
   - If the OS uses SysVinit to manage automatic start of services, run the following commands:

     chkconfig --add cloud-init-local; chkconfig --add cloud-init; chkconfig --add cloud-config; chkconfig --add cloud-final

     chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config on; chkconfig cloud-final on

     service cloud-init-local status; service cloud-init status; service cloud-config status; service cloud-final status
   - If the OS uses Systemd to manage automatic start of services, run the following commands:

     systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

     systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
6. Run the following commands to check whether Cloud-Init has been installed:

   cloud-init -v

   cloud-init init --local

   Cloud-Init is successfully installed if the following information is displayed:

   ```
   cloud-init 0.7.6
   ```

3.4.3 Configuring Cloud-Init

Scenarios

You need to configure Cloud-Init after it is installed.

Prerequisites

- Cloud-Init has been installed.
- An EIP has been bound to the ECS.
- You have logged in to the ECS.
- The IP address obtaining mode of the ECS is DHCP.

Procedure

The following operations are required:

1. Configure Cloud-Init.

   For details, see **Configure Cloud-Init**.
2. Check whether Cloud-Init is successfully configured.

For details, see **Check the Cloud-Init Configuration**.

Configure Cloud-Init

1. Configure the user permissions for logging in to the ECS. If you select user **root**, enable the SSH permissions of user **root** and enable remote login to the ECS using a password.
   - If you inject a password, use it to log in to the ECS remotely using SSH or noVNC.
   - If you inject a private key, use it to log in to the ECS remotely using SSH.

   Run the following command to open the **/etc/cloud/cloud.cfg** file using the vi editor:

   vi /etc/cloud/cloud.cfg
2. Enable remote login using the password of user **root** and enable the SSH permissions of user **root**. Take CentOS 6.7 as an example. If the value of **disable_root** in the configuration file is **1**, the permissions are disabled. If the value is **0**, the permissions are enabled. (In some OSs, value **true** indicates that the permissions are disabled, and **false** indicates that the permissions are enabled). Set the value of **disable_root** to **0**, that of **ssh_pwauth** to **1**, and that of **lock_passwd** to **false** (indicating that user passwords are not locked).

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

   disable_root: 0
   ssh_pwauth: 1
   ```
3. Enable the hostname update. Do not comment or delete the **- update_hostname** statement.

   ```
   cloud_init_modules:
    - migrator
    - bootcmd
    - write-files
    - growpart
    - resizefs
    - set_hostname
    - update_hostname
    - update_etc_hosts
    - rsyslog
    - users-groups
    - ssh
   ```
4. Run the following command to open the **/etc/ssh/sshd_config** file using the vi editor:

   vi /etc/ssh/sshd_config
5. 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. Delete user **linux** and the **/home/linux** directory from the image template.

   userdel linux

   rm -fr /home/linux

7. Enable the agent to access the IaaS OpenStack data source.

   Add the following information to the last line of **/etc/cloud/cloud.cfg**:

   ```
   datasource_list: [ OpenStack ]
   datasource:
    OpenStack:
      metadata_urls: ['http://169.254.169.254']
      max_wait: 120
      timeout: 5
   ```

   NOTE

   - You can decide whether to set **max_wait** and **timeout**. The values of **max_wait** and **timeout** in the preceding command output are only for reference.
   - If the OS version is earlier than Debian 8 or CentOS 5, you cannot enable the agent to access the IaaS OpenStack data source.
   - The default zeroconf route must be disabled for CentOS and EulerOS ECSs for accurate access to the IaaS OpenStack data source.

     echo "NOZEROCONF=yes" >> /etc/sysconfig/network

8. Prevent Cloud-Init from taking over the network in **/etc/cloud/cloud.cfg**.

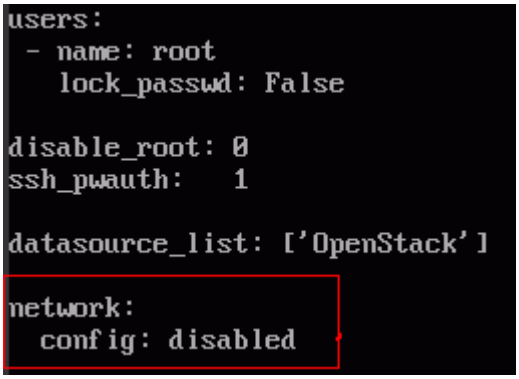
   If the Cloud-Init version is 0.7.9 or later, add the following content to **/etc/cloud/cloud.cfg**:

   ```
   network:
    config: disabled
   ```

   NOTE

   The added content must be in the YAML format.

   Figure 3-17 Preventing Cloud-Init from taking over the network

9. Add the following content to **/etc/cloud/cloud.cfg**:

   manage_etc_hosts: localhost

   This prevents the system from staying in the **Waiting for cloudResetPwdAgent** state for a long time during ECS startup.

Figure 3-18 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
```

10. Modify the **cloud_init_modules** configuration file.

    Move **ssh** from the bottom to the top to speed up the SSH login.

Figure 3-19 Speeding up the SSH login to the ECS

```
cloud_init_modules:
 - ssh
 - migrator
 - bootcmd
 - write-files
 - growpart
 - resizefs
 - set_hostname
 - update_hostname
 - update_etc_hosts
 - rsyslog
 - users-groups
```

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

    a. Run the following command to modify the **__init__.py** file:

    vi /usr/lib/python2.7/site-packages/cloudinit/sources/__init__.py

    Press **i** to enter editing mode. Search for **toks**. The following information is displayed:

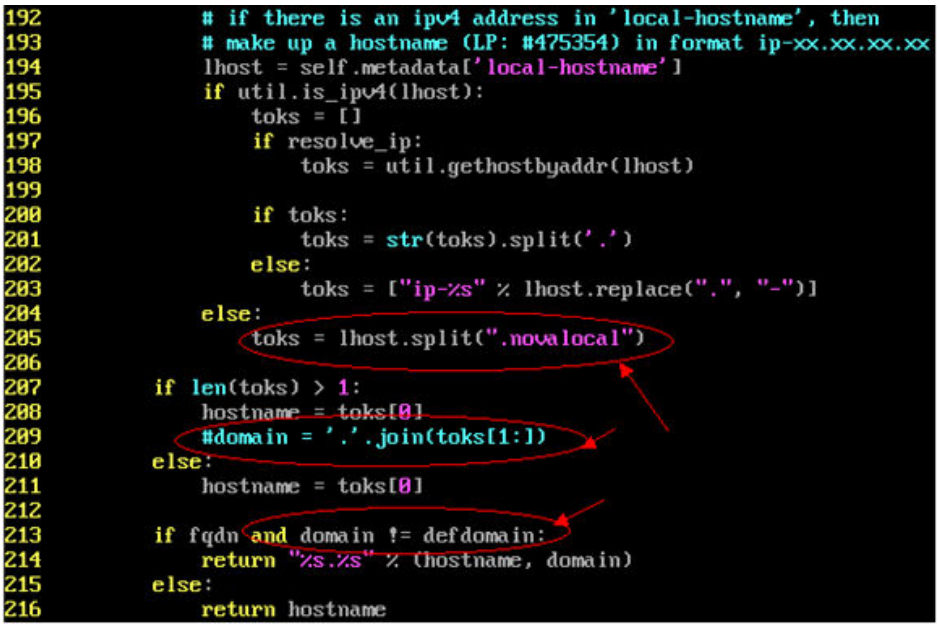
```
if toks:
    toks = str(toks).split('.')
else:
    toks = ["ip-%s" % lhost.replace(".", "-")]
else:
    toks = lhost.split(".novalocal")

if len(toks) > 1:
    hostname = toks[0]
    #domain = '.'.join(toks[1:])
else:
    hostname = toks[0]

if fqdn and domain != defdomain:
    return "%s.%s" % (hostname, domain)
else:
    return hostname
```

    After the modification is complete, press **Esc** to exit editing mode and enter **:wq!** to save the settings and exit.

Figure 3-20 Modifying the **__init__.py** file



```
192             # if there is an ipv4 address in 'local-hostname', then
193             # make up a hostname (LP: #475354) in format ip-xx.xx.xx.xx
194             lhost = self.metadata['local-hostname']
195             if util.is_ipv4(lhost):
196                 toks = []
197                 if resolve_ip:
198                     toks = util.gethostbyaddr(lhost)
199
200                 if toks:
201                     toks = str(toks).split('.')
202                 else:
203                     toks = ["ip-%s" % lhost.replace(".", "-")]
204             else:
205                 toks = lhost.split(".novalocal")
206
207         if len(toks) > 1:
208             hostname = toks[0]
209             #domain = '.'.join(toks[1:])
210         else:
211             hostname = toks[0]
212
213         if fqdn and domain != defdomain:
214             return "%s.%s" % (hostname, domain)
215         else:
216             return hostname
```

b. Run the following command to switch to the **cloudinit/sources** folder:

cd /usr/lib/python2.7/site-packages/cloudinit/sources/

c. Run the following commands to delete the **__init__.pyc** file and the optimized **__init__.pyo** file:

rm -rf __init__.pyc

rm -rf __init__.pyo

d. Run the following commands to clear the logs:

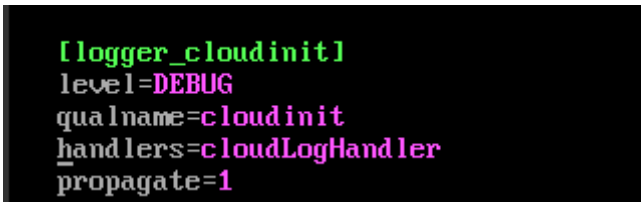
rm -rf /var/lib/cloud/*

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

12. Run the following command to edit the **/etc/cloud/cloud.cfg.d/05_logging.cfg** file to use cloudLogHandler to process logs:

vim /etc/cloud/cloud.cfg.d/05_logging.cfg

Figure 3-21 Setting the parameter value to **cloudLogHandler**



```
[logger_cloudinit]
level=DEBUG
qualname=cloudinit
handlers=cloudLogHandler
propagate=1
```

Check the Cloud-Init Configuration

Run the following command to check whether Cloud-Init has been properly configured:

cloud-init init --local

If Cloud-Init has been properly installed, the version information is displayed and no error occurs. For example, messages indicating lack of files will not be displayed.

NOTE

(Optional) Run the following command to set the password validity period to the maximum:

chage -M 99999 $user_name

user_name is a system user, such as user **root**.

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

3.4.4 (Optional) Installing the One-Click Password Reset Plug-in

You are advised to install CloudResetPwdAgent on the ECS that is used to create an image. This plug-in allows you to reset the password of each ECS created from the image with a few clicks.

Procedure

1. Download the CloudResetPwdAgent software package.

   NOTE

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

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

   For 32-bit OSs: **http://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip**

   For 64-bit OSs: **http://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip**

2. Run the following command to decompress **CloudResetPwdAgent.zip**.

   There is no special requirement for the directory that stores the decompressed **CloudResetPwdAgent.zip**. You can customize the directory.

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

   For example:

   If the decompressed directory is **/home/linux/test**, the command is as follows:

   unzip -o -d /home/linux/test CloudResetPwdAgent.zip

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

   a. Run the following command to open the **CloudResetPwdUpdateAgent.Linux** file:

      cd CloudResetPwdAgent/CloudResetPwdUpdateAgent.Linux

   b. Run the following command to add the execute permission for the **setup.sh** file:

      chmod +x setup.sh

   c. Run the following command to install the plug-in:

      sudo sh setup.sh

d. Run the following commands to check whether the installation is successful:

service cloudResetPwdAgent status

service cloudResetPwdUpdateAgent status

If the status of **CloudResetPwdAgent** and **CoudResetPwdUpdateAgent** is not **unrecognized service**, the installation is successful. Otherwise, the installation fails.

NOTE

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

3.4.5 Configuring NetworkManager

Linux OSs use NetworkManager to provide detection and configuration for systems to automatically connect to network. You are advised to use NetworkManager for new versions of OSs.

If you do not want to use NetworkManager, you can use the native network management service of the OS.

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

Perform the following operations to enable automatic network configuration for an ECS using NetworkManager:

1. Run the following command to install NetworkManager:

   yum install NetworkManager
2. Delete **ifcfg-eth1** to **ifcfg-eth11** from the **/etc/sysconfig/network-script/** directory and retain only **ifcfg-eth0**.
3. Run the following command to disable the network:

   service network stop
4. Run the following command to disable automatic start of the network:

   chkconfig network off
5. Run the following commands to restart messagebus and NetworkManager and enable NetworkManager to start automatically at startup:

   service messagebus restart

   service NetworkManager restart

   chkconfig NetworkManager on

Debian 9.0 or Later

Perform the following operations to enable automatic network configuration for an ECS using NetworkManager:

1. Run the following command to install NetworkManager:

   apt-get install network-manager
2. Change the value of **managed** in the **/etc/NetworkManager/NetworkManager.conf** file to **true**.

3. Modify **/etc/network/interfaces** and retain only **eth0**.
4. Run the following commands to disable the network, restart messagebus and NetworkManager, and enable NetworkManager to start automatically at startup:

   service network-manager restart

   chkconfig network-manager on

   service networking stop

   service messagebus restart

   service network-manager restart

Ubuntu 14 or Later

Perform the following operations to enable automatic network configuration for an ECS using NetworkManager:

1. Run the following command to install NetworkManager:

   apt-get install network-manager
2. Change the value of **managed** in the **/etc/NetworkManager/NetworkManager.conf** file to **true**.
3. Modify **/etc/network/interfaces** and retain only **eth0**.
4. Run the following command to disable the network:

   service networking stop
5. Run the following command to disable automatic start of the network:

   chkconfig network off
6. Run the following commands to restart D-Bus and NetworkManager:

   service dbus restart

   service network-manager restart

SUSE 11 SP3 and openSUSE 13 or Later

Perform the following operations to enable automatic network configuration for an ECS using NetworkManager:

1. Delete **ifcfg-eth1** to **ifcfg-eth11** from the **/etc/sysconfig/network-script/** directory and retain only **ifcfg-eth0**.
2. Run the following command to 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 Exporting the Image File

After the VM is configured, you can perform the following operations to obtain the Linux image file:

1. Open VirtualBox, select the newly created VM, choose **Settings** > **Storage**, and select **Linux.vhd**.

   Linux is the VM name.

2. In the detailed information area on the right, view the storage location of the disk file.

   Enter the path to obtain the generated Linux image file.

3.6 Uploading and Registering the Image File

Upload the image file to the OBS bucket and register the image.

Restrictions

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

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/en-us/browsertg-obs/obs_03_1003.html**.

2. Register the external image file as a private image. For details, see **Registering an Image File as a Private Image (Linux)**.

4 Cleaning Up the Disk Space of a Windows ECS

Scenarios

This section describes how to clean up the disk space of a Windows ECS.

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, which deteriorates the I/O performance. Therefore, you can disable virtual memory to release the disk space of the Windows OS.

In the following operations, 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 the 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 initiali size to *xxx* shown in the warning. The partition for storing paging files must have sufficient space. If the disk resources are insufficient, the virtual memory is insufficient. You only need to set the 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 4-1**. Click **Yes** and then click **Apply**.

Figure 4-1 Warning

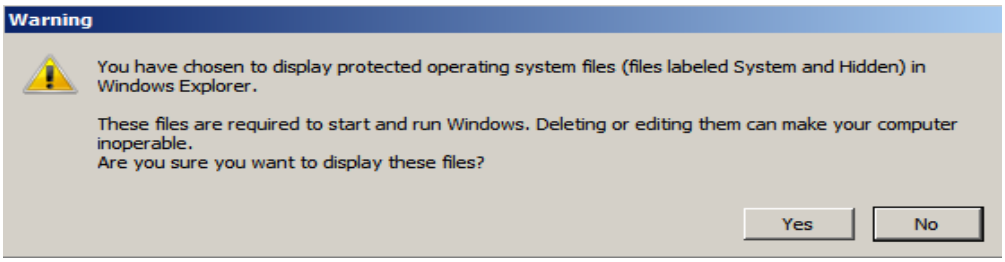
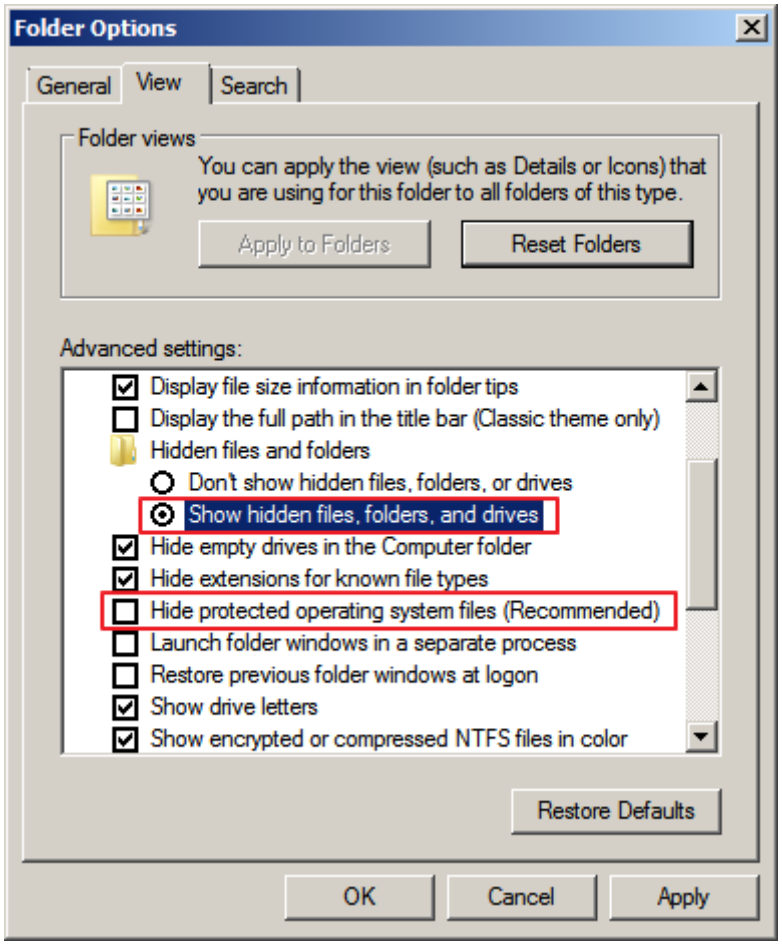


Figure 4-2 Showing hidden files



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

Disable Hibernation

In the following operations, 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 the hibernation function file of the Windows OS and occupies large system disk space. It saves memory data and sessions to disks so that the memory image file required for sessions can be quickly restored after the computer is restarted. Perform the following steps to delete the **Hiberfil.sys** file to release some disk space:

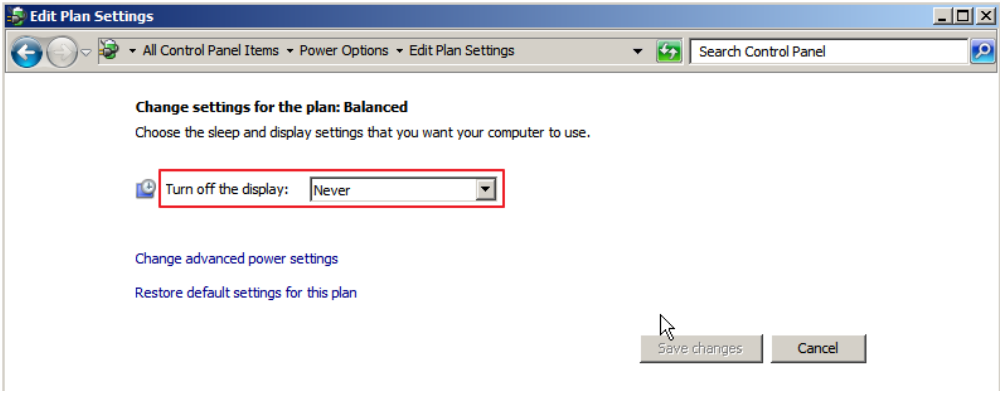
1. Run **cmd.exe** as an administrator to open the command line interface (CLI).
2. Run the following command to disable hibernation (**Hiberfil.sys** file is automatically deleted):

   powercfg -h off

Method 2: Disable hibernation.

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

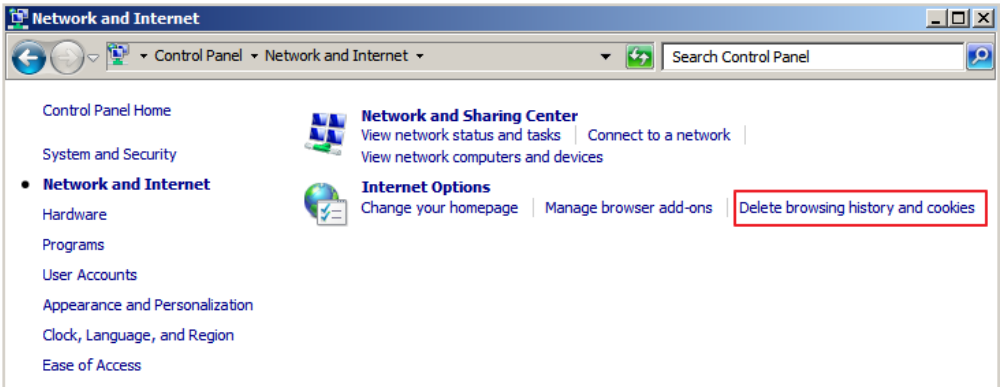


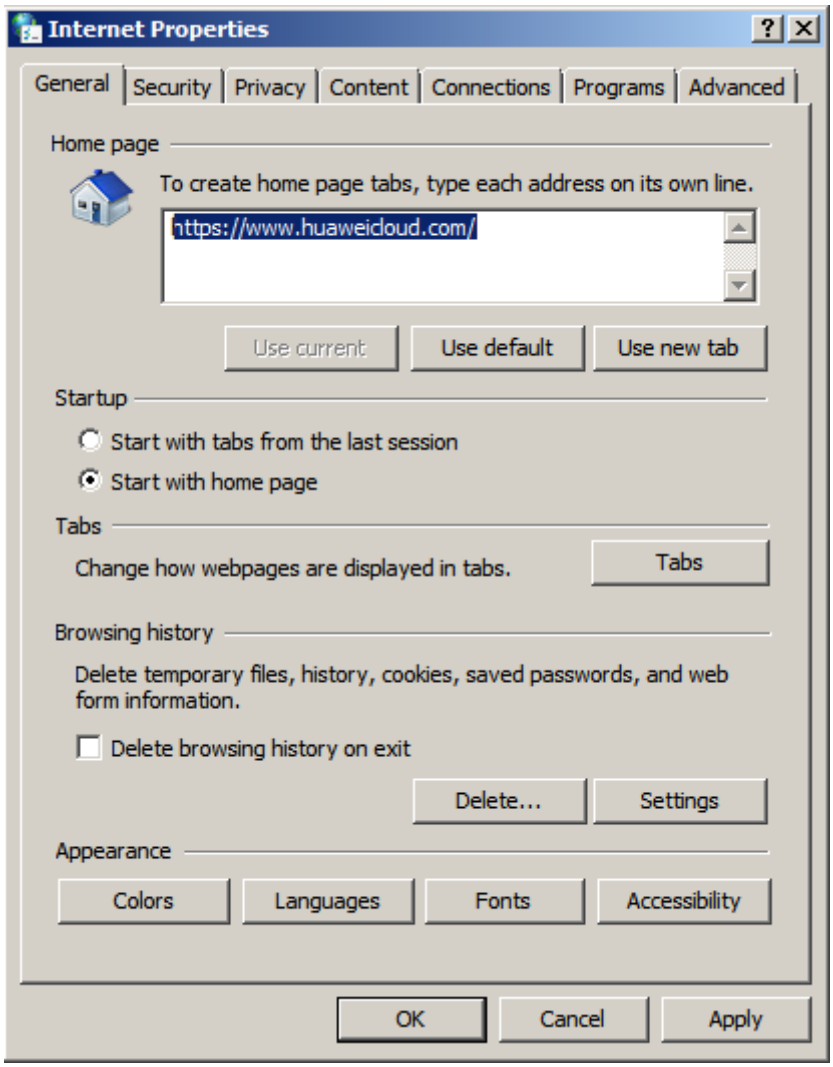
Deleting Internet Explorer Temporary Files

In the following operations, 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.

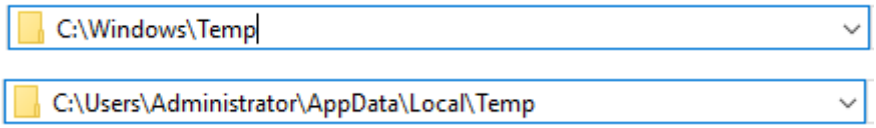
Internet Explorer stores all information about Internet access in a specified folder, including Internet Explorer cache files, cookies files, recent browsing history, visited websites, URLs in the address bar, and Internet Explorer tables/passwords. Perform the following steps to delete temporary files 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 in them. (The folders store visited websites and other temporary information.



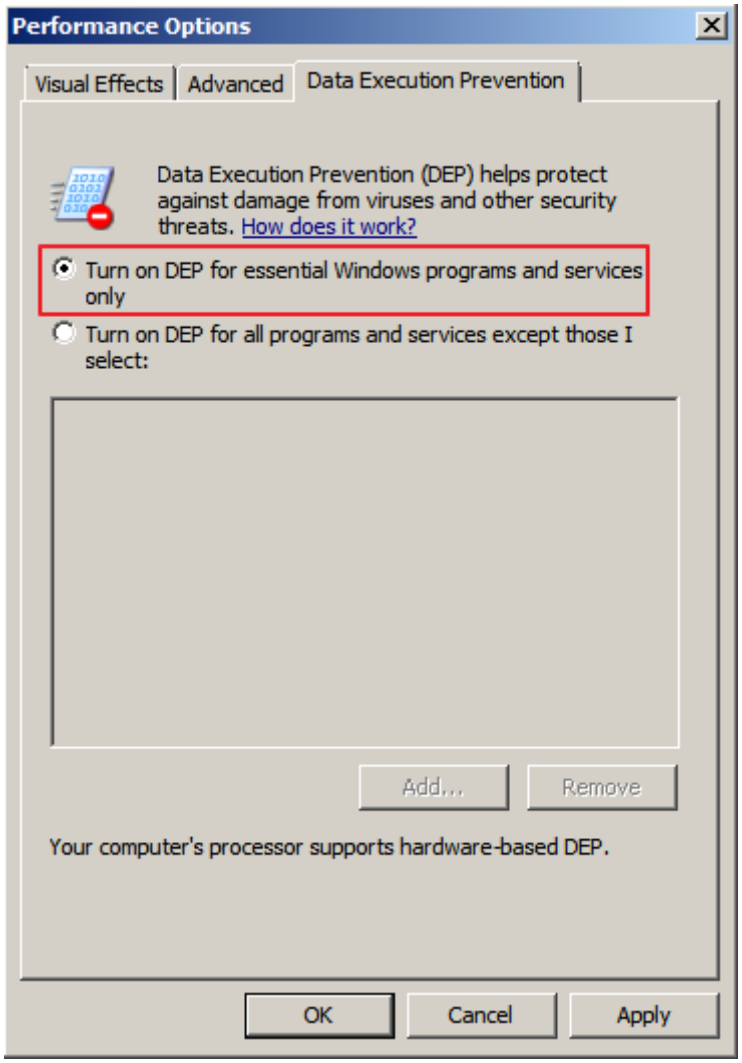
Disable Data Execution Prevention (DEP)

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.

In the following operations, 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 the system startup and file reading. However, the number of files increases with time. Deleting redundant files can release disk space in Windows.

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

Clean Up Disks

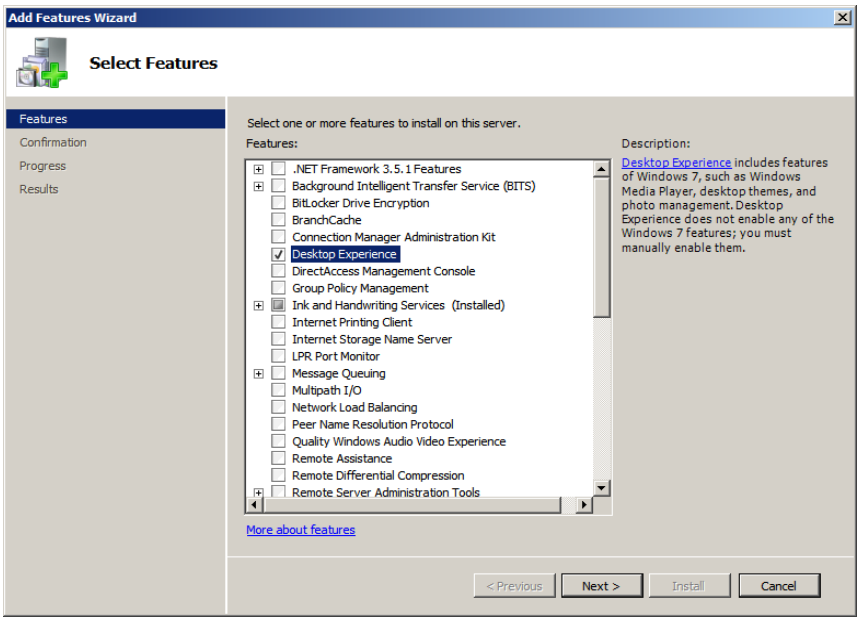
You can use **Disk Cleanup** of ECSs to delete temporary files, empty the recycle bin, and delete redundant system files and other files.

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 released. 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. In the following operations, an ECS running Windows Server 2008 R2 Standard 64bit is used as an example to describe how to install desktop experience.

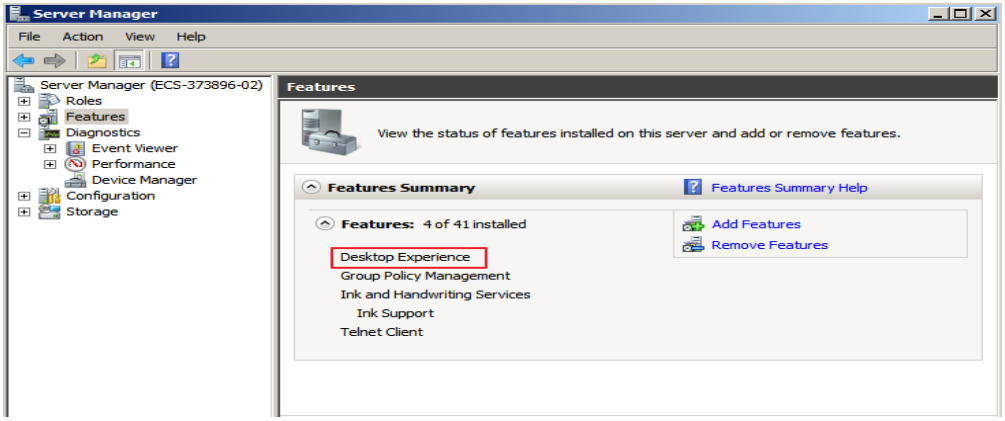
1. Choose **Start** > **All Programs** > **Administrative Tools** > **Server Manager**. In the navigation pane, click **Features**.
2. Click **Add Features**.
3. In the **Select Features** dialog box, select **Desktop Experience** and click **Next**.

   Figure 4-3 Adding 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 4-4 Successful installation of desktop experience



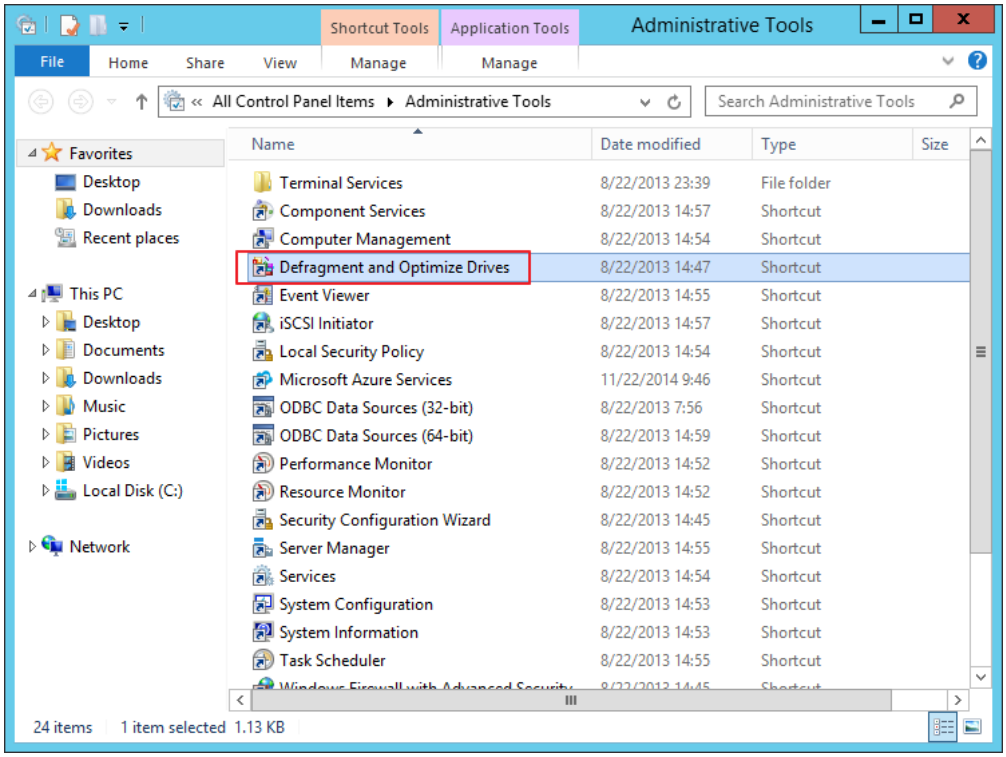
7. Choose **Start** > **All Programs** > **Accessories** > **System Tools** > **Disk Cleanup** to start the disk cleanup tool.

Defragment and Optimize Drives

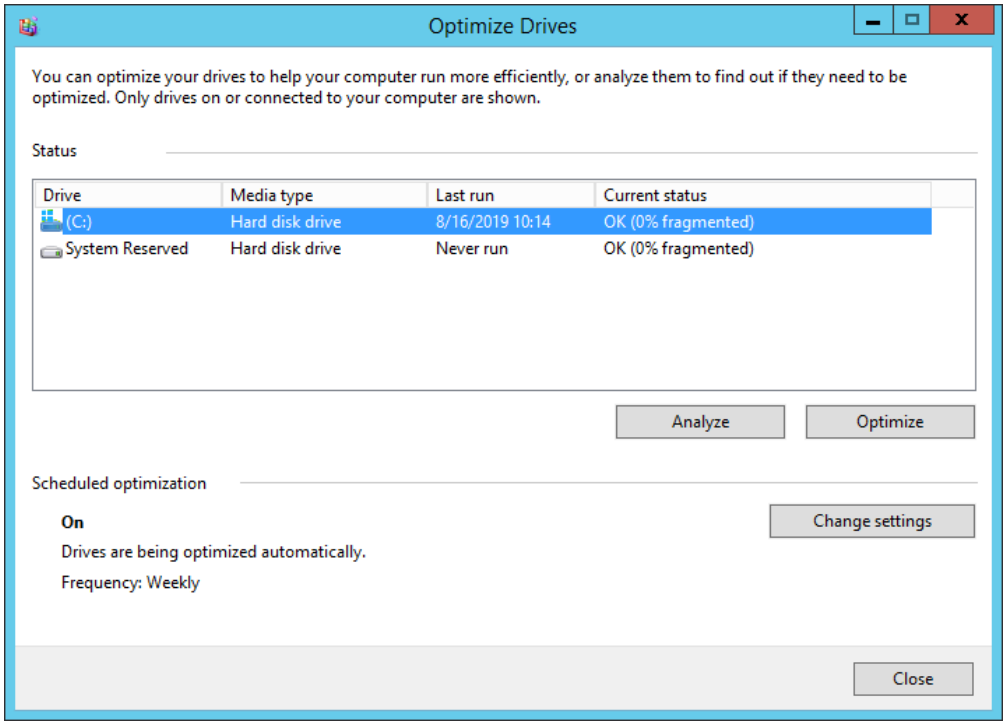
Disk defragmentation is a process in which system software or professional disk defragmentation software is used to organize the fragments generated during the long-term use of disks into the smallest number of contiguous fragments, improving the performance and running speed of the computer.

In the following operations, 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 on disk C to release 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.

In the following operations, 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. Run the following command to 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. Run the following command to 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

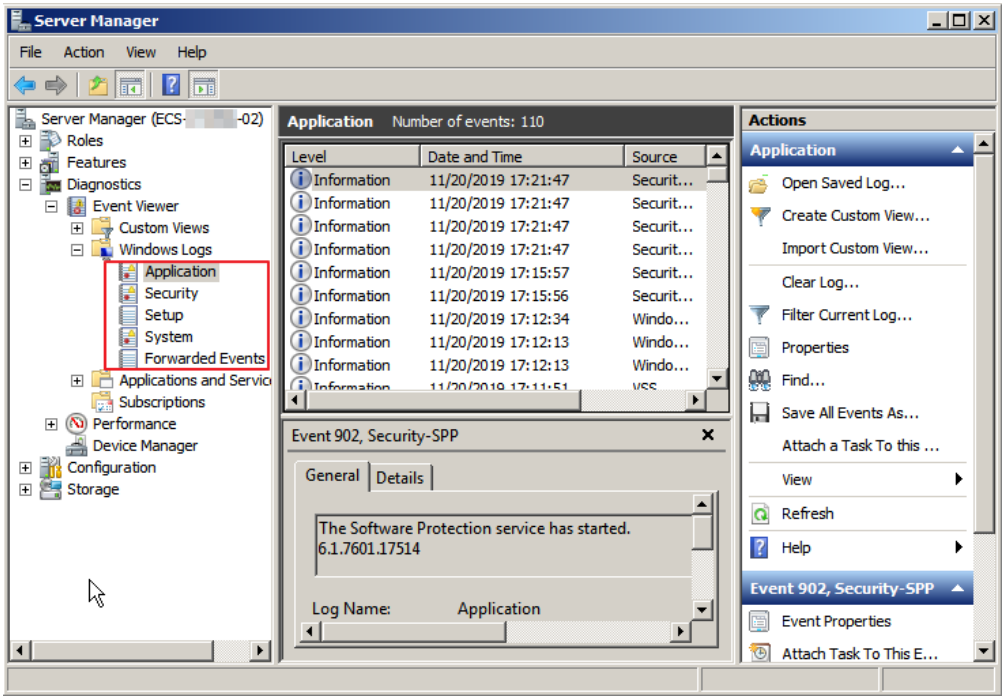
System logs record hardware and software information and system problems and can be used to monitor system events. You can use the logs to locate error causes or track attacker actions. System logs include application logs, security logs, startup logs, and event forwarding logs. The **System32** > **LogFiles**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

In the following operations, 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 in it.

1. Chose **Start**, right-click **Computer**, and choose **Manage** in 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**.



5 Converting the Image Format

5.1 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.

Background

- **qemu-img** supports the mutual conversion of image formats VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, and QED.
- ZVHD and ZVHD2 are 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 the command to convert the format of VHD image files, use VPC to replace VHD. Otherwise, qemu-img cannot identify the image format.

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

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

Windows

1. Install qemu-img.
   a. Download the qemu-img installation 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. Run the following command to 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. Run the following command to 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

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. Run the following command to 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_cach]
   ```
3. Convert the image format. For example, perform the following steps to convert a VMDK image file running CentOS 7 to a QCOW2 image file:
   a. Run the following command to 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 pat following **-O** (which must be in upper case) is the converted image format + source image file name + target image file name.

      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. Run the following command to 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

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 file 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 image 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.

1. Run the following commands to query the 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. Run the following command to query the configuration of the pre-allocated image file:

   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. Run the following command to query details about the converted image 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
```

5.2 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 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 self-developed tool **qemu-img-hw**. This section describes how to use **qemu-img-hw** to convert an image file to ZVHD2.

Background

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 an EulerOS ECS as an example.

Procedure

1. Upload the image file to be converted to the ECS.
   - If the local host runs a Linux OS, run the **scp** command.

     For example, to upload **image01.qcow2** to the **/usr/** directory on the ECS, run the following command:

scp /var/image01.qcow2 root@*xxx.xxx.xx.xxx*:/usr/

xxx.xxx.xx.xxx indicates the EIP bound to the ECS.

- If the local host 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** software package, upload it to the ECS, and then decompress the package.

Table 5-1 qemu-img-hw package

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

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. Run the following command to change file permissions:

   chmod +x qemu-img-hw

   c. Run the **qemu-img-hw** command 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 Errors During qemu-img-hw Running

- Symptom:

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

  ```
  ./qemu-img-hw: /lib64/libc.so.6: version `GLIBC_2.14' not found (required by ./qemu-img-hw)
  ```

  Solution:

  Run the **strings /lib64/libc.so.6 | grep glibc** command to check the glibc version. If the version is too early, install the latest version. Run the following commands in sequence:

  wget http://ftp.gnu.org/gnu/glibc/glibc-2.15.tar.gz

  wget http://ftp.gnu.org/gnu/glibc/glibc-ports-2.15.tar.gz

  tar -xvf glibc-2.15.tar.gz

  tar -xvf glibc-ports-2.15.tar.gz

  mv glibc-ports-2.15 glibc-2.15/ports

  mkdir glibc-build-2.15

  cd glibc-build-2.15

  ../glibc-2.15/configure --prefix=/usr --disable-profile --enable-add-ons --with-headers=/usr/include --with-binutils=/usr/bin

  NOTE

  If **configure: error: no acceptable C compiler found in $PATH** is displayed, run the **yum -y install gcc** command.

  make

  make install

- Symptom:

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

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

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

6 Creating a Private Image Using Packer

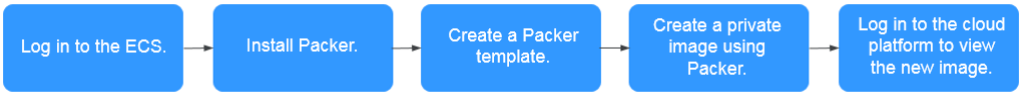
Packer is an open-source tool that can be used to create custom images. It consists of three components, builder, provisioner, and post-processor. The components can be flexibly combined using a JSON template to automatically create image files. Packer simplifies private image creation by changing the image creation process to a form in which management code can be configured. In this way, users can flexibly customize images and switch images between different cloud platforms.

This section describes how to create a Ubuntu 16.04 Server 64-bit private image from a CentOS 7.4 64-bit ECS using Packer and upload the created image to the public cloud platform.

Constraints

Full-ECS images cannot be used to create private images using Packer.

Procedure



Installing Packer

1. Log in to the management console, create an ECS (for example, an ECS running CentOS 7.4 64-bit), and bind an EIP to the ECS.
2. Log in to the ECSs.
3. On the **Packer download page**, select the Packer version corresponding to the ECS OS and architecture type. You are advised to select a version ranging from 1.2.3 to 1.4.2.
4. Run the following command to install Packer (**packer_1.4.2_linux_amd64.zip** is used as an example):

   wget --no-check-certificate https://releases.hashicorp.com/packer/1.4.2/packer_1.4.2_linux_amd64.zip

NOTE

- You need to bind an EIP to the ECS in advance so that the ECS can access the Internet.
- If message "command not found" is displayed, the wget tool is not installed. Run the **yum install wget** command to install the wget tool.

5. Run the following command to decompress the Packer installation package:

   unzip packer_1.4.2_linux_amd64.zip

6. Run the following command to move the Packer installation 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 installation package to another directory that has been added to environment variables.

7. Run the following command to query the Packer version number and check whether Packer is installed successfully:

   packer -v

   - If the command output contains the Packer version number, Packer is installed successfully.
   - If "command not found" is displayed, the Packer installation fails. Check whether the directory where Packer resides has been added to environment variables.

     NOTE

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

     If the PATH does not contain the Packer installation directory, run the following commands to add the Packer installation directory to PATH:

     1. Run the following command to open the **profile** file:

        vim /etc/profile

     2. Press **i** to enter editing mode and add **export PATH=$PATH:/usr/local/bin** to the end of the file.

        Replace **/usr/local/bin** with the actual directory where Packer is installed.

     3. Press **Esc** to exit 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

Creating a Packer Template

To create an image using Packer, you need a template in JSON format. You need to specify a **builder**, **provisioner**, and post-processor in the template. In the Builder, you can specify any operation on the source image, specify the installation software, and modify configuration. 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 from each builder based on the manifest output. For details about the builder, provisioner, and post-processor, see the **official Packer documents**.

This section uses the Shell provisioner as an example.

1. Run the following command to create the **hwcloud.json** file:

   touch hwcloud.json

2. Run the following command to open the **hwcloud.json** file:

   vim hwcloud.json

3. Press **i** to enter editing mode and edit the template based on the site requirements. The following content is for reference only. For the parameter descriptions, see **Table 6-1**.

```
{
  "builders": [{
    "type": "openstack",
    "identity_endpoint": "https://iam.xxx.com/v3",
    "tenant_name": "xxx",
    "domain_name": "domain_name",
    "username": "username",
    "password": "password",
    "ssh_username": "root",
    "region": "xxx",
    "image_name": "Ubuntu-image-updating-powered-by-Packer",
    "instance_name": "Ubuntu-image-updating-powered-by-Packer",
    "source_image": "f1dd2272-7041-479e-9663-646632b6ac00",
    "availability_zone": "xxx",
    "flavor": "s3.medium.2",
    "use_blockstorage_volume": true,
    "networks": ["11d661c4-e41f-487f-a6f6-9b88d623dd5d"],
    "floating_ip": "8f686f9a-3408-4fdd-be75-ea768065800c"
  }],
  "provisioners": [{
    "inline": [
      "apt-get update -y"
    ],
    "inline_shebang": "/bin/sh -x",
    "type": "shell",
    "skip_clean": true
  }],
  "post-processors": [{
    "strip_path": true,
    "output": "packer-template-ubuntu-updating-result.log",
    "type": "manifest"
  }]
}
```

NOTE

In **Table 6-1**, **tenant_name**, **region**, **availability_zone**, **flavor**, **networks**, and **floating_ip** are the attributes of the ECS used to create the private image.

Table 6-1 Packer template parameters

Parameter	Description	Mandatory
type	Specifies the type. Retain the default value **openstack**.	Yes

Parameter	Description	Mandatory
identity_endpoint	Specifies the address of the identity authentication node. The format is https://*IAM endpoint*/v3. Obtain the IAM endpoint from **Regions and Endpoints**.	Yes
tenant_name	Specifies the project name. To obtain the project name, perform the following operations: 1. On the management console, move the cursor to the username in the upper right corner and choose **My Credentials**. 2. On the **API Credentials** page, obtain the project name (value in the **Project Name** column).	Yes
domain_name	Specifies the domain name. To obtain the domain name, perform the following operations: 1. On the management console, move the cursor to the username in the upper right corner and choose **My Credentials**. 2. On the **API Credentials** page, obtain the domain name.	Yes

Parameter	Description	Mandatory
username	Specifies the IAM username. To obtain the IAM username, perform the following operations: 1. On the management console, move the cursor to the username in the upper right corner and choose **My Credentials**. 2. On the **API Credentials** page, obtain the IAM username. **NOTE** If you use an account to log in to the HUAWEI CLOUD console, the IAM username and account name are the same.	Yes
password	Specifies the password for logging in to the management console.	Yes
ssh_username	Specifies the SSH login username of the private image to be created.	Yes
region	Specifies the region name. Obtain the region name from **Regions and Endpoints**.	Yes
image_name	Specifies the name of the private image to be created.	Yes
instance_name	Specifies the name of the temporary instance generated during the private image creation. If you do not set this parameter, the system uses a random value.	No

Parameter	Description	Mandatory
source_image	Specifies the ID of the source image, which can be obtained from the public image list on the IMS console. If you already have a Ubuntu 16.04 Server 64-bit private image and want to reconstruct the image using Packer, you can enter the ID of the private image.	Yes
availability_zone	Specifies the AZ. Obtain the AZ from **Regions and Endpoints**.	Yes
flavor	Specifies the ECS flavor.	Yes
use_blockstorage_volume	Specifies whether the system disk rather than the whole ECS is used to create an image.	Yes. The value must be **true**.
networks	Specifies the ID of the VPC subnet.	Yes
floating_ip	Specifies the EIP ID.	This parameter is mandatory if the image instance created using Packer needs to access the Internet.
provisioners	Specifies the type of the Packer provisioner used to create the private image. For details, see **Packer Provisioners**.	Yes
post-processors	Specifies the type of the Packer post-processor used to create the private image.	No

Creating a Private Image Using Packer

1. After the Packer template is created, run the following command to create an image:

   packer build hwcloud.json

   The command output is as follows:

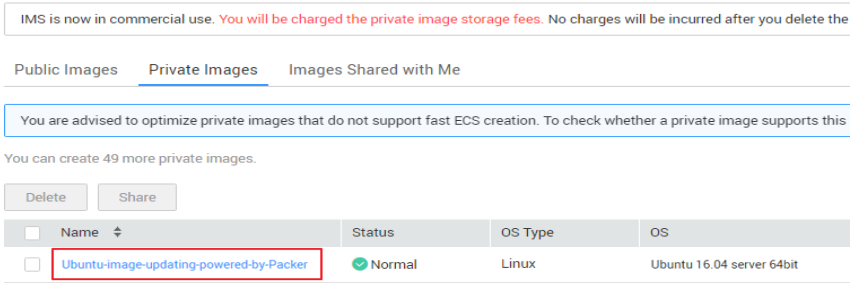
```
openstack output will be in this color.

==> openstack: Loading flavor: s3.small.1
    openstack: Verified flavor. ID: s3.small.1
==> openstack: Creating temporary keypair: packer_5be8d358-2cc6-66a4-f1b5-31e8587c7bfa ...
==> openstack: Created temporary keypair: packer_5be8d358-2cc6-66a4-f1b5-31e8587c7bfa
==> openstack: Launching server...
==> openstack: Launching server...
    openstack: Server ID: fcf2014e-2f70-46c5-80d5-870ae0d1e659
==> openstack: Waiting for server to become ready...
    openstack: Selected floating IP: '8f686f9a-3408-4fdd-be75-ea768065800c' (119.3.67.11)
==> openstack: Associating floating IP '8f686f9a-3408-4fdd-be75-ea768065800c' (119.3.67.11) with
instance port...
    openstack: Added floating IP '8f686f9a-3408-4fdd-be75-ea768065800c' (119.3.67.11) to instance!
==> openstack: Using ssh communicator to connect: 119.3.67.11
==> openstack: Waiting for SSH to become available...
==> openstack: Connected to SSH!
==> openstack: Provisioning with shell script: /tmp/packer-shell133419321
    openstack: + apt-get update -y
    openstack: Hit:1 http://archive.ubuntu.com/ubuntu xenial InRelease
          ......
    openstack: Fetched 7,088 kB in 9s (778 kB/s)
    openstack: Reading package lists...
==> openstack: Stopping server: fcf2014e-2f70-46c5-80d5-870ae0d1e659 ...
    openstack: Waiting for server to stop: fcf2014e-2f70-46c5-80d5-870ae0d1e659 ...
==> openstack: Creating the image: CentOS-image-updating-powered-by-Packer
    openstack: Image: 9eccbb17-9aed-4beb-bf44-1e8c80448ba3
==> openstack: Waiting for image CentOS-image-updating-powered-by-Packer (image id:
9eccbb17-9aed-4beb-bf44-1e8c80448ba3) to become ready...
==> openstack: Terminating the source server: fcf2014e-2f70-46c5-80d5-870ae0d1e659 ...
==> openstack: Deleting temporary keypair: packer_5be8d358-2cc6-66a4-f1b5-31e8587c7bfa ...
==> openstack: Running post-processor: manifest
Build 'openstack' finished.

==> Builds finished. The artifacts of successful builds are:
--> openstack: An image was created: 9eccbb17-9aed-4beb-bf44-1e8c80448ba3
--> openstack:
```

2. Log in to the management console and click **Image Management Service** under **Computing**.
3. Click the **Private Images** tab and view the image created using Packer. **Figure 6-1** shows the created image.

   Figure 6-1 Viewing the private image created using Packer



Helpful Links

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

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

Configuring 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 **.repo** 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

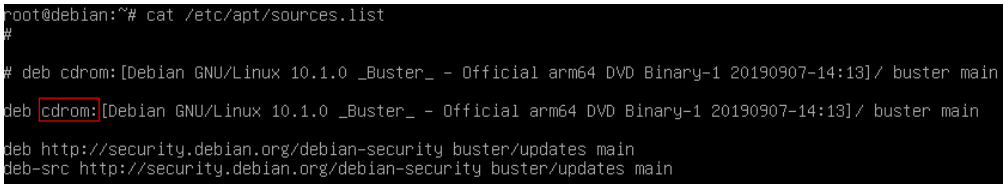
Examples

The operations in **Configuring a Local Image Source** may be different depending on the OS version. Basically, you need to add the source and refresh it. The following uses Debian 10.1.0 and CentOS 8.0 as examples to describe how to add a local source.

- Debian 10.1.0

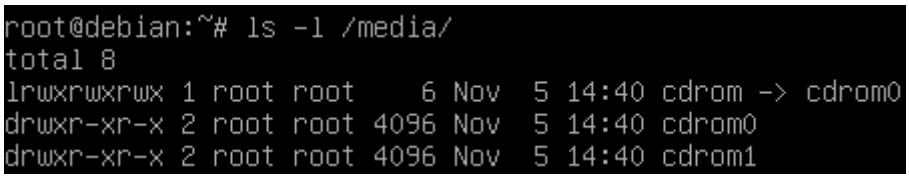
Run the **cat /etc/apt/sources.list** command to check whether the **sources.list** file contains a default cdrom source.

Figure 7-1 Viewing the source



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**.

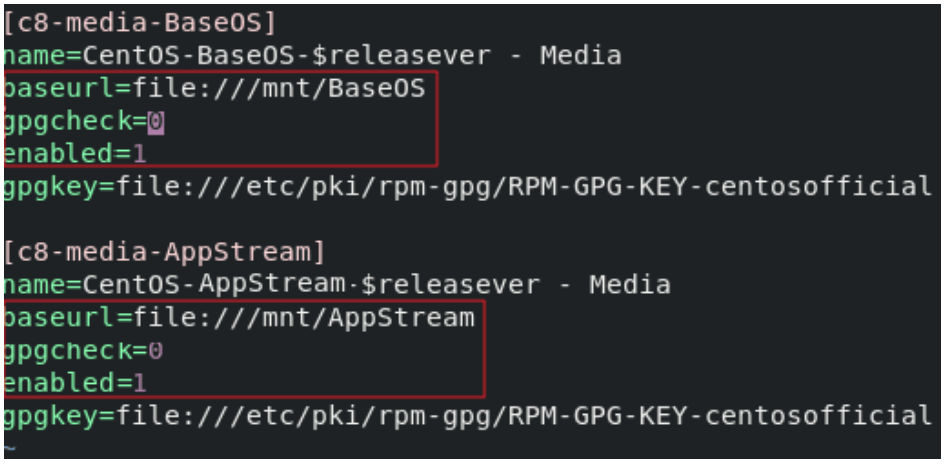
Figure 7-2 Checking the media directory



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



  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. Otherwise, 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 in different regions, you are advised to use IMS to implement the migration.

Table 8-1 ECS migration methods

Migration Method	Description	Characteristics	Constraints
Deploying 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, which consumes manpower, materials, and time.

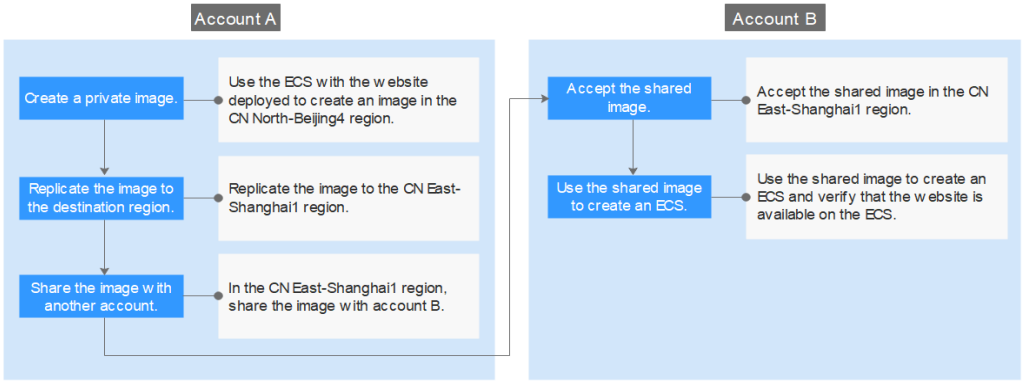
Migration Method	Description	Characteristics	Constraints
Server Migration Service (SMS)	The SMS supports physical to virtual (P2V) and virtual to virtual (V2V) migrations, enabling you to migrate x86 physical servers or VMs in private or public clouds to HUAWEI CLOUD.	• You only need to install and configure the migration Agent on the source server and create the migration task on SMS. SMS will complete the migration. • Services are not interrupted during the migration. Resumable data transfer is supported.	The ECS to be migrated must be able to access the public network.
Image Management Service (IMS)	Migrate an ECS from an on-premises IDC, private cloud, or other public clouds to HUAWEI CLOUD, or migrate an ECS between HUAWEI CLOUD accounts in different regions by importing private images, replicating images cross regions, and sharing images.	• Only image files in VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, QED, ZVHD, or ZVHD2 format can be imported. • Mainstream OSs, such as SUSE, Oracle Linux, Red Hat, Ubuntu, openSUSE, CentOS, Debian, Fedora, and EulerOS are compatible. • 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.	Local storage space is occupied 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 in 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 desired account.

For example, if a website is set up on an ECS in the CN North-Beijing4 region and you want to migrate the ECS to another account in the CN East-Shanghai1 region, 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 desired account**
4. **Accept the shared image**
5. **Use the shared image to create an ECS**

Step 1: Create a Private Image

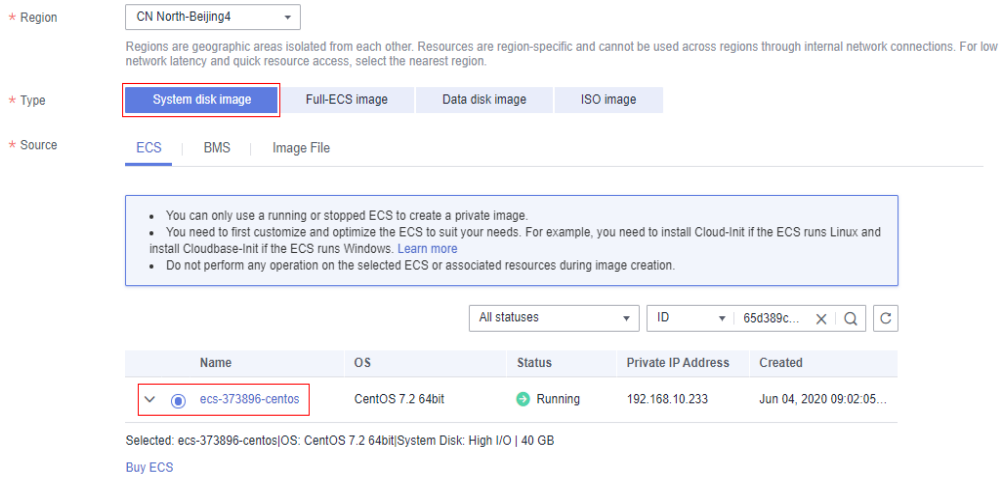
Use the ECS with the website deployed to create an image in the CN North-Beijing4 region. Assume that the web access address of the ECS is http://121.36.*xxx.xxx*/index.html.

1. Log in to the management console and switch to the CN North-Beijing4 region.
2. Under **Service List**, choose **Computing** > **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/Disk** > **Create Image** in the **Operation** column.

   The **Create Image** page is displayed.
4. Set parameters.

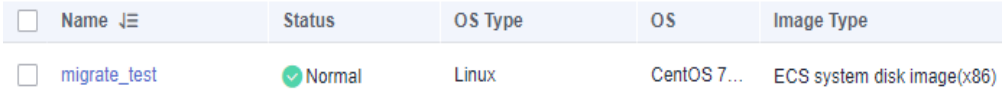
Figure 8-2 Creating a private image



- **Type**: Select **System disk image**.
- **Source**: Select **ECS** and 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

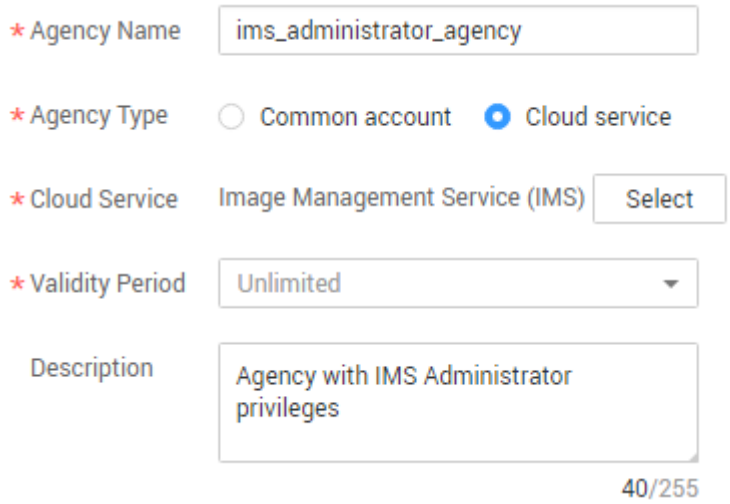


Step 2: Replicate the Image to the Destination Region

Replicate the private image created in **Step 1: Create a Private Image** to the CN East-Shanghai1 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_administrator_agency**.

Figure 8-4 Creating an agency

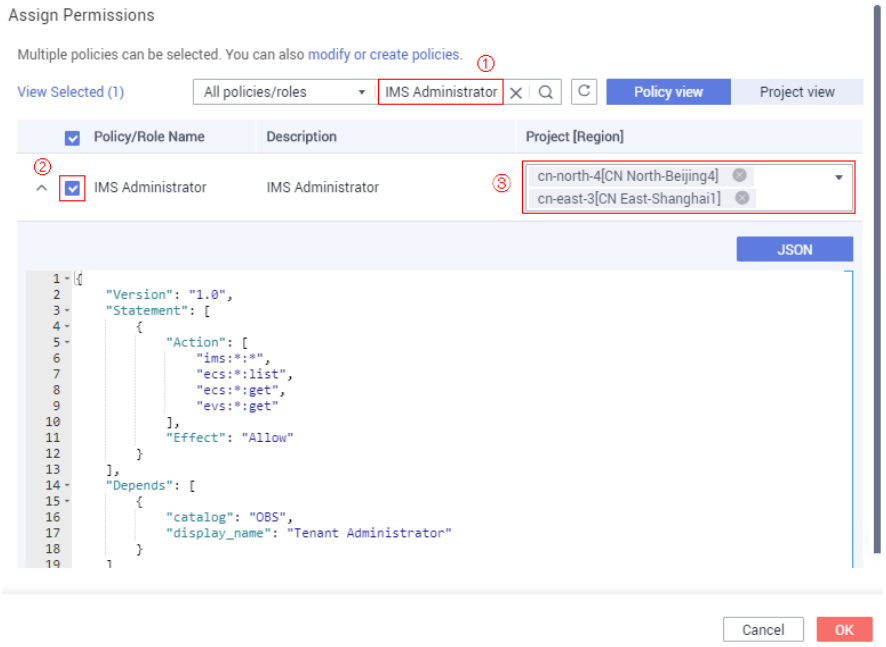


- **Agency Type**: Select **Cloud service**.
- **Cloud Service**: This parameter is available if you select **Cloud service** for **Agency Type**. Click **Select**. In the displayed **Select Cloud Service** dialog box, select **Image Management Service (IMS)** and click **OK**.
- **Validity Period**: 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 North-Beijing4** and **CN East-Shanghai1** in the **Project [Region]** column, and click **OK**.

CAUTION

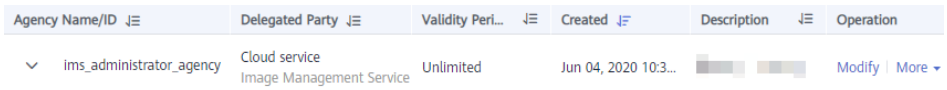
Do not select **All projects** in the **Project [Region]** column. Otherwise, the created agency will be invalid.

Figure 8-5 Configuring permissions



e. Click **OK**.

Figure 8-6 Viewing agencies



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

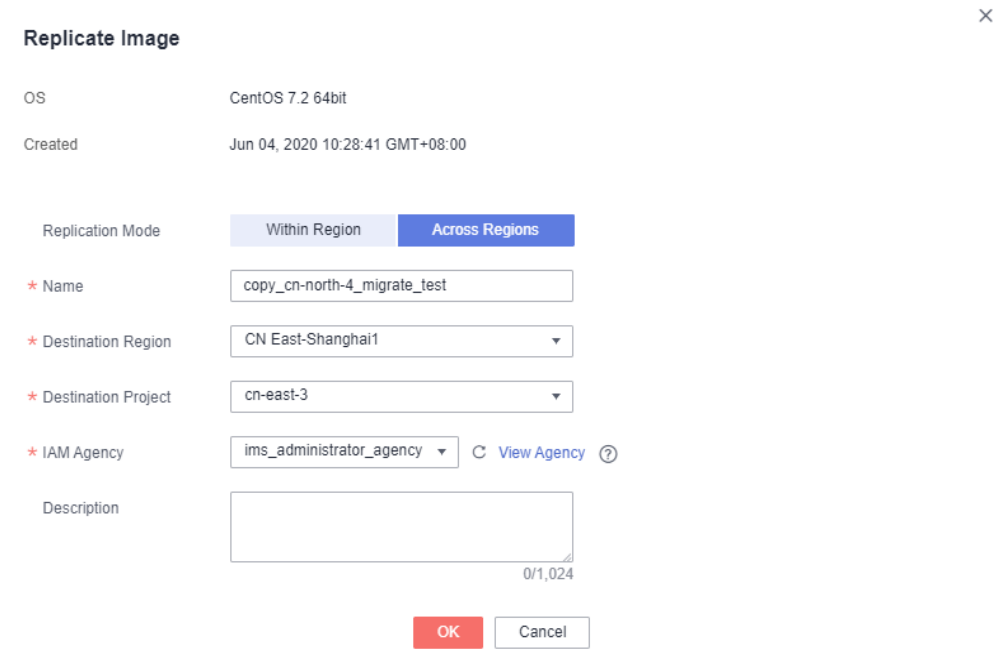
   The **Private Images** page is displayed.

3. Locate the row that contains the **migrate_test** image, anc choose **More** > **Replicate** in the **Operation**.

   The **Replicate Image** dialog box is displayed.

4. Set parameters.

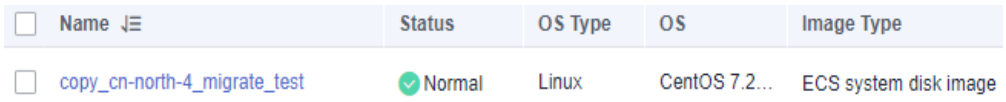
Figure 8-7 Replicating an image



- **Name**: Retain the default value **copy_cn-north-4_migrate_test**.
- **Destination Region**: Select **CN East-Shanghai1**.
- **Destination Project**: Select **cn-east-3**.
- **IAM Agency**: Select **ims_administrator_agency** created in **1**.

5. Click **OK**.
6. Switch to the CN East-Shanghai1 region. Wait for several minutes and check whether the image is successfully replicated.

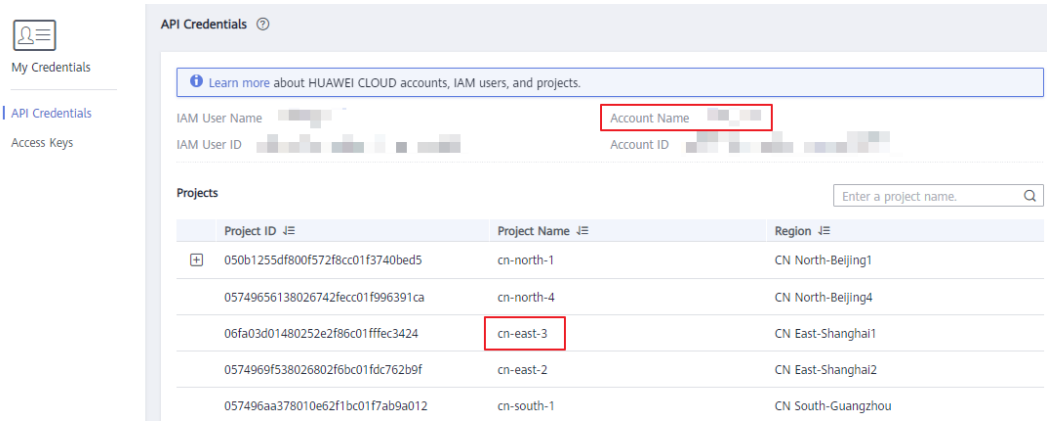
Figure 8-8 Viewing private images



Step 3: Share the Image with the Desired Account

In the CN East-Shanghai1 region, share the image with the desired account. Before the image sharing, obtain the desired account name. If it is an account of a DeC or multi-project user, you also need to obtain its project name. (You can obtain the project name from **My Credentials**. For details, see **Figure 8-9**.)

Figure 8-9 Obtaining the account name and project name



1. In the CN East-Shanghai1 region, choose **Service List** > **Computing** > **Image Management Service** and click the **Private Images** tab.

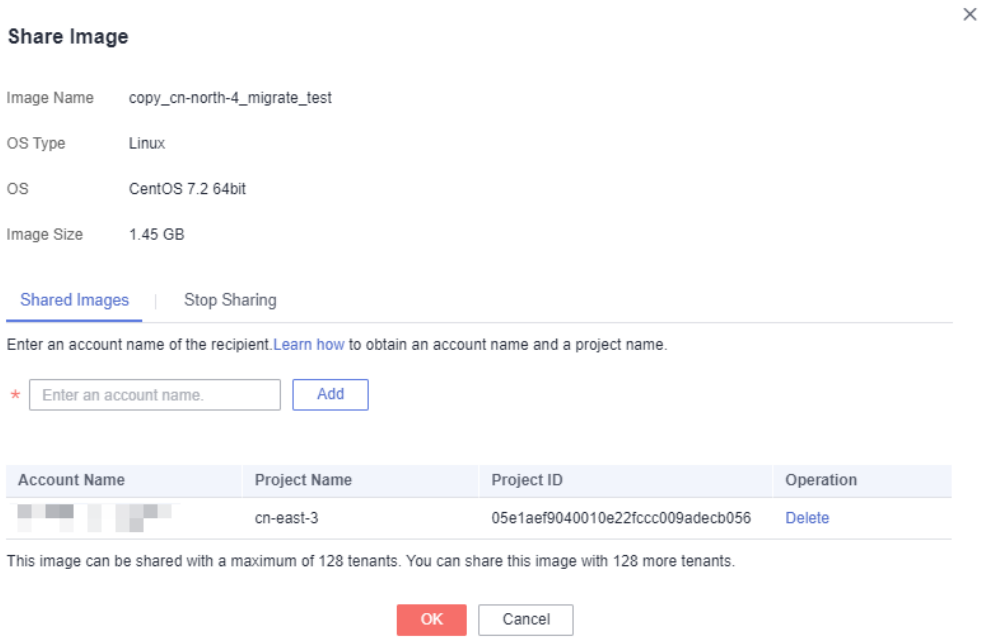
   The **Private Images** page is displayed.

2. Locate the row that contains the **copy_cn-north-4_migrate_test** private image. Choose **More** > **Share** in the **Operation** column.

   The **Share Image** dialog box is displayed.

3. Click the **Shared Images** tab, enter the desired account name, and click **Add**.

   Figure 8-10 Sharing an image



4. Click **OK**.

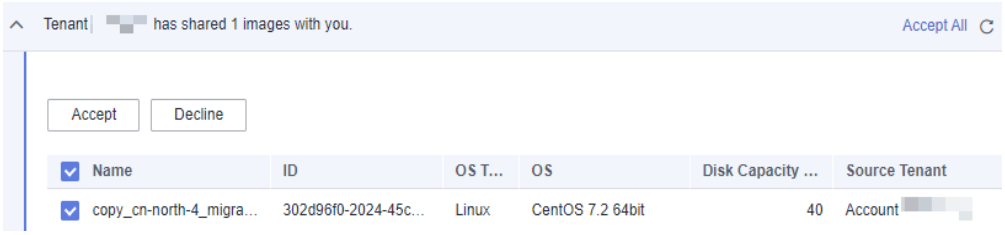
Step 4: Accept the Shared Image

Accept the shared image in the CN East-Shanghai1 region.

1. Log in to the management console using the account the image is shared with and switch to the CN East-Shanghai1 region.

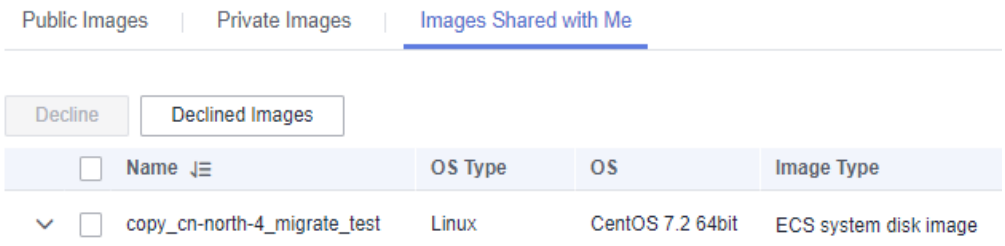
2. Under **Service List**, choose **Computing** > **Image Management Service**. Then, click the **Images Shared with Me** tab.
3. In the displayed dialog box, select **copy_cn-north-4_migrate_test** and click **Accept**.

Figure 8-11 Accepting a shared image



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

Figure 8-12 Viewing shared images



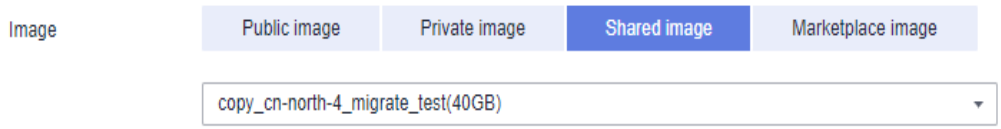
Step 5: Use the Shared Image to Create an ECS

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_cn-north-4_migrate_test**, and click **Apply for Server** in the **Operation** column.

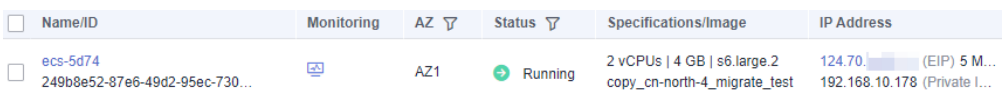
   The page for purchasing ECSs is displayed.
2. Set the billing mode, AZ, specifications, and network as needed to create an ECS. Retain the default value for **Image**.

Figure 8-13 Selecting an image



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

Figure 8-14 Viewing ECSs



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 8-15 Verifying the website

A Change History

Released On	Description
2020-06-04	This issue is the fifth official release. Added the following content: **Converting the Image Format Using qemu-img-hw**
2019-12-30	This issue is the fourth official release. Added **Configuring an ISO File as a Local Image Source**.
2019-11-30	This issue is the third official release. Optimized operations in **Cleaning Up the Disk Space of a Windows ECS**.
2019-07-30	This issue is the second official release. • Added the description of the image creation process in **Introduction** and **Introduction**. • Optimized operations in **Creating a Private Image Using Packer**.
2019-04-03	This issue is the first official release.

