Image Management Service

User Guide

Issue	01
Date	2025-07-18

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Notice

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

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

Contents

1 Using IAM to Grant Access to IMS

1.1 Creating a User and Granting Permissions

Scenarios

This section describes how to use **Identity and Access Management** (IAM) to implement fine-grained permissions control over your images. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own identity credentials for accessing images.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or cloud service to perform professional and efficient O&M on your images.

If your account does not need individual IAM users for permissions management, you can skip this section.

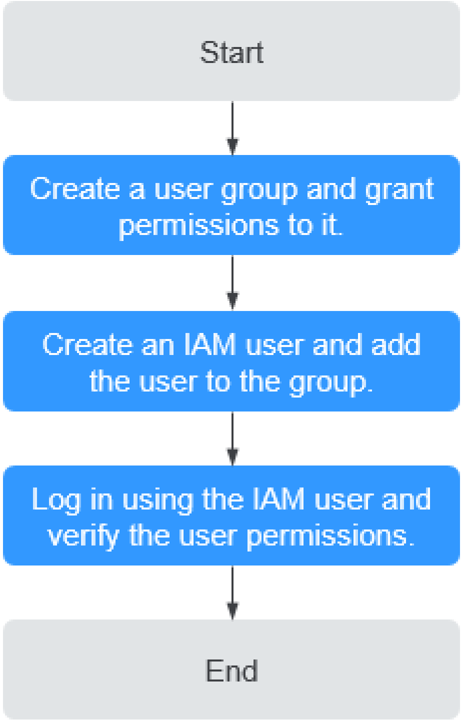
This section uses the **IMS ReadOnlyAccess** permission as an example to describe how to grant permissions to a user. **Figure 1-1** shows the process.

Prerequisites

Learn about the permissions (see **IMS Permissions**) supported by IMS. For the system permissions of other services, see **System Permissions**.

Process Flow

Figure 1-1 Process for granting IMS permissions


Start
Create a user group and grant permissions to it.
Create an IAM user and add the user to the group.
Log in using the IAM user and verify the user permissions.
End

1. **Create a user group and grant permissions to it**.

   Create a user group on the IAM console, and grant the read-only permission to the group by assigning the **IMS ReadOnlyAccess** permission.

2. **Create an IAM user and add it to the user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the management console using the IAM user, switch to a region where the permissions take effect, and verify the permissions (assume that the user has only the **IMS ReadOnlyAccess** permission).

   - In the **Service List**, choose **Image Management Service**. On the IMS console, perform operations except querying images, such as creating, modifying, and deleting an image.

     For example, click **Create Private Image** in the upper right corner. If you are prompted insufficient permissions, the **IMS ReadOnlyAccess** permission has taken effect.

   - Choose any other service in the **Service List**, such as **Virtual Private Cloud**. If a message appears indicating insufficient permissions to access the service, the **IMS ReadOnlyAccess** permission has taken effect.

1.2 Creating a Custom Policy

Scenarios

Custom policies can be created as a supplement to the system permissions of IMS. For the actions supported by custom policies, see **Permissions and Supported Actions**.

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. This section provides examples of common IMS custom policies.

Example Policies

- Example 1: Allowing users to create images

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ims:serverImages:create"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "KMS:*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:cloudServers:get",
                "ecs:servers:get",
                "ecs:serverVolumes:use",
                "ecs:cloudServers:list",
                "ecs:serverVolumeAttachments:list",
                "ecs:servers:list"

            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "bms:servers:list",
                "bms:servers:get",
                "bms:serverFlavors:get"
            ]
        },
       {
            "Effect": "Allow",
            "Action": [
                "evs:volumes:*"
            ]
        }
    ]
}
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "OBS:*:*"
            ]
        }
    ]
}
```

NOTE

The action required for creating an image is **ims:serverImages:create**. Others are dependent actions for creating an image.

- Example 2: Denying image deletion

  A deny policy must be used in conjunction with other policies to take effect. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

  The following method can be used if you need to assign the **IMS FullAccess** policy to a user but also forbid the user from deleting images. Create a custom policy for denying image deletion, and assign both the policies to the group the user belongs to. Then, the user can perform all operations on IMS except deleting images. The following is an example deny policy:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ims:images:delete"
            ]
        }
    ]
}
```

2 Preparations for Creating a Private Image

2.1 Overview

Before creating a private image, you need to configure the image source to initialize the private image and improve the image availability.

An image source can be an ECS, a BMS, or an image file. You can configure them as instructed in the following tables.

- **Table 2-1**
- **Table 2-2**
- **Table 2-3**
- **Table 2-4**

Image Source: ECS or Image File

Table 2-1 ECS configurations

OS	Configuration
Windows	• **Configuring DHCP** • **Enabling Remote Desktop Connection** • **Installing the One-Click Password Reset Plug-In** • **(Optional) Installing and Configuring Cloudbase-Init** • Installing Guest OS Drivers (**PV** and **VirtIO** Drivers) • **Running Sysprep**

OS	Configuration
Linux	- Configuring DHCP - Installing the One-Click Password Reset Plug-In - (Optional) Installing and Configuring Cloud-Init - Deleting Files from the Network Rule Directory - Changing Disk Identifiers in the GRUB File to UUID - Changing Disk Identifiers in the fstab File to UUID - Installing Native Xen and KVM Drivers on a Xen ECS - Installing Native KVM Drivers on a KVM ECS - Detaching Data Disks from an ECS

NOTE

- If the ECS was created from a public image, the one-click password reset plug-in and Cloud-Init have been installed in it by default.

Table 2-2 Image file configurations

OS	Configuration
Windows	- Configuring DHCP - Enabling Remote Desktop Connection - Installing the One-Click Password Reset Plug-In - (Optional) Installing and Configuring Cloudbase-Init - Installing Guest OS Drivers (PV and VirtIO Drivers) - (Optional) Enabling NIC Multi-Queue - (Optional) Configuring DHCPv6
Linux	- Deleting Files from the Network Rule Directory - Configuring DHCP - Deleting Files from the Network Rule Directory - Changing Disk Identifiers in the GRUB File to UUID - Changing Disk Identifiers in the fstab File to UUID - Installing Native Xen and KVM Drivers on a Xen ECS - Installing Native KVM Drivers on a KVM ECS - Configuring DHCP - (Optional) Enabling NIC Multi-Queue - (Optional) Configuring DHCPv6

NOTE

- To use an image file to create a private image, you are advised to perform the preceding operations on the VM where the image file is exported from.
- When you register a Windows image file as a private image, if you select **Enable automatic configuration**, the cloud platform will check the image file for Guest OS drivers. If no Guest OS drivers are found, the cloud platform will try to install them automatically.

Image Source: BMS or Image File

Table 2-3 BMS configurations

OS	Configuration	Reference
Windows	● Install the **bms-network-config** package. ● Install Cloudbase-Init. ● Delete residual files from the OS.	**Creating a Private Image from a BMS**
Linux	● Install the **bms-network-config** package. ● Install Cloud-Init. ● Delete residual files from the OS.	

Table 2-4 Image file configurations

OS	Configuration	Reference
Windows	● Install drivers for x86 V5 BMSs. ● Install Cloudbase-Init. ● Install the **bms-network-config** package. ● (Optional) Install the SDI iNIC driver. ● (Optional) Install the one-click password reset plug-in. ● Set the time zone. ● Set the virtual memory. ● (Optional) Configure automatic Windows update. ● Configure the SID.	**Private Image Creation Guide**

OS	Configuration	Reference
Linux	- Install and configure Cloud-Init. - Modify the hardware device driver that boots the OS. - Install the **bms-network-config** package. - (Optional) Install the SDI iNIC driver. - (Optional) Install the Hi1822 NIC driver. - (Optional) Install the IB driver. - (Optional) Install drivers for x86 V5 BMSs. - (Optional) Install the multipath software. - (Optional) Install the one-click password reset plug-in. - Perform security configuration. - Configure remote login to the BMS. - Configure the root partition to be automatically extended.	

2.2 Windows Private Images

2.2.1 Configuring DHCP

Scenarios

If a private image is created from an ECS or external image file and the VM where the ECS or external image file is located is configured with a static IP address, you need to configure DHCP so that the new ECSs created from the private image can dynamically obtain an IP address.

This section uses Windows Server 2008 R2 as an example to describe how to configure DHCP. For details about how to configure DHCP on ECSs running other OSs, see the relevant OS documentation.

NOTE

When registering an external image file as a private image, configure DHCP on the VM where the external image file is located. You are advised to configure DHCP on the VM and then export the image file.

Prerequisites

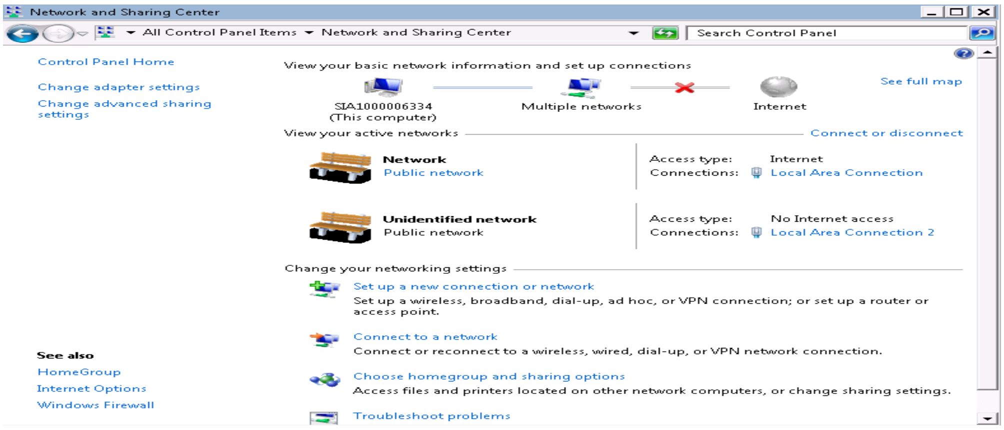
You have logged in to the ECS used to create a Windows private image.

For details about how to log in to an ECS, see **Login Overview**.

Procedure

1. On the ECS, choose **Start** > **Control Panel**.
2. Click **Network and Internet Connections**.
3. Click **Network and Sharing Center**.

Figure 2-1 Network and Sharing Center



View your basic network information and set up connections

View your active networks

Network
Public network
Access type: Internet
Connections: Local Area Connection

Unidentified network
Public network
Access type: No Internet access
Connections: Local Area Connection 2

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

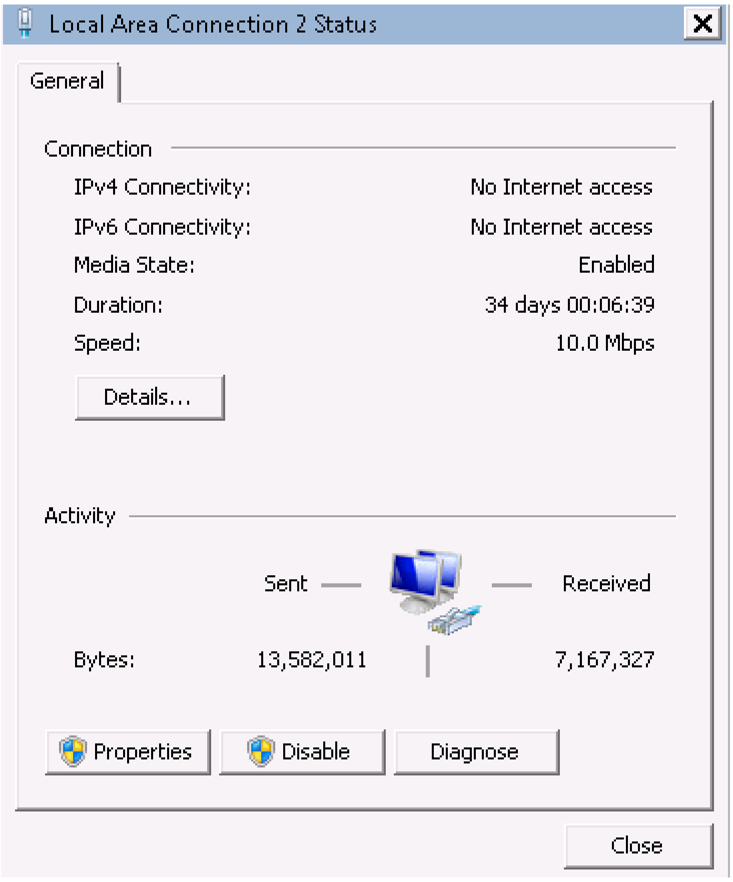
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems

4. Select the connection configured with the static IP address. For example, click **Local Area Connection 2**.

Figure 2-2 Local Area Connection 2 Status



Connection

IPv4 Connectivity: No Internet access

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 34 days 00:06:39

Speed: 10.0 Mbps

Activity

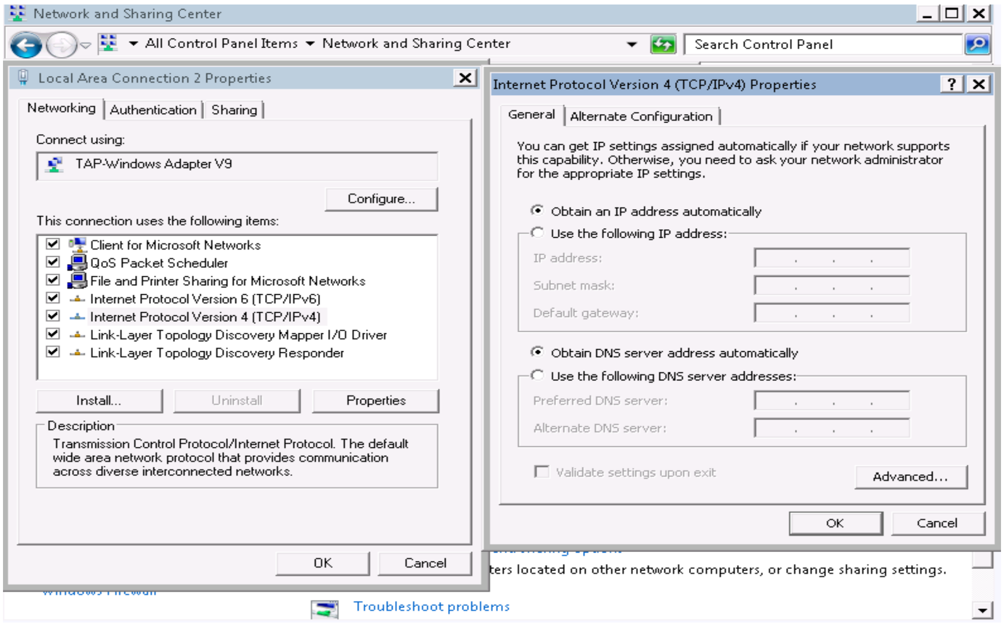
Bytes: 13,582,011 | 7,167,327

5. Click **Properties** and select the configured Internet protocol version.
6. On the **General** tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**, as shown in **Figure 2-3**. The system will automatically obtain an IP address.

NOTE

You are advised to record the original network information so that you can restore the network if necessary.

Figure 2-3 Configuring DHCP



Network and Sharing Center

All Control Panel Items ▸ Network and Sharing Center

Search Control Panel

Local Area Connection 2 Properties

Networking | Authentication | Sharing

Connect using:

TAP-Windows Adapter V9

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

OK | Cancel

ters located on other network computers, or change sharing settings.

Troubleshoot problems

2.2.2 Enabling Remote Desktop Connection

Scenarios

If you want to remotely access an ECS, enable remote desktop connection for the source ECS when creating a private image. This function must be enabled for GPU-accelerated ECSs.

NOTE

When registering an external image file as a private image, enable remote desktop connection on the VM where the external image file is located. You are advised to enable this function on the VM and then export the image file.

Prerequisites

You have logged in to the ECS used to create a Windows private image.

For details about how to log in to an ECS, see **Login Overview**.

Procedure

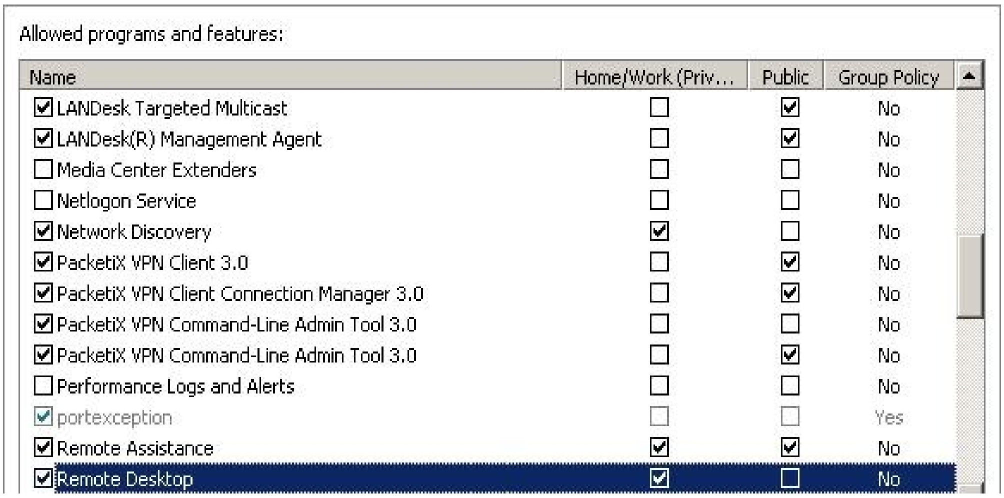
1. Before enabling this function, you are advised to set the resolution of the ECS to 1920×1080.

   On the ECS, choose **Start** > **Control Panel**. Under **Appearance and Personalization**, click **Adjust screen resolution**. Then select a proper value from the **Resolution** drop-down list box.

2. Choose **Start**, right-click **Computer**, and choose **Properties** from the shortcut menu.
3. Click **Remote settings**.

4. In the **Remote** tab, select **Allow connections from computers running any version of Remote Desktop (less secure)**.
5. Click **OK**.
6. Choose **Start** > **Control Panel** and navigate to **Windows Firewall**.
7. Choose **Allow a program or feature through Windows Firewall** in the left pane.
8. Select programs and features that are allowed by the Windows firewall for **Remote Desktop** based on your network requirements and click **OK** in the lower part.

Figure 2-4 Configuring remote desktop



Allowed programs and features:

Name	Home/Work (Priv...	Public	Group Policy
☑ LANDesk Targeted Multicast	□	☑	No
☑ LANDesk(R) Management Agent	□	☑	No
□ Media Center Extenders	□	□	No
□ Netlogon Service	□	□	No
☑ Network Discovery	☑	□	No
☑ PacketiX VPN Client 3.0	□	☑	No
☑ PacketiX VPN Client Connection Manager 3.0	□	☑	No
☑ PacketiX VPN Command-Line Admin Tool 3.0	□	□	No
☑ PacketiX VPN Command-Line Admin Tool 3.0	□	☑	No
□ Performance Logs and Alerts	□	□	No
☑ portexception	□	□	Yes
☑ Remote Assistance	☑	☑	No
☑ Remote Desktop	☑	□	No

2.2.3 (Optional) Installing and Configuring Cloudbase-Init

Scenarios

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

- If Cloudbase-Init is not installed, you cannot customize an ECS. Instead, you can only use the password in the image file to log in to the ECS.
- By default, ECSs created from a public image have Cloudbase-Init installed. You do not need to install or configure Cloudbase-Init on such ECSs.
- For ECSs created from external image files, install and configure Cloudbase-Init by performing the operations in this section.

NOTE

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

Prerequisites

- An EIP has been bound to the ECS.
- You have logged in to the ECS.

- The ECS uses DHCP to obtain IP addresses.
- The one-click password reset plug-in has been installed on the ECS.

  If you restart the ECS when installing Cloudbase-Init on it, the password may be changed to a random one. Therefore, you need to install the one-click password reset plug-in on the ECS. For details, see **Installing the One-Click Password Reset Plug-In**.

Install Cloudbase-Init

1. On the Windows **Start** menu, choose **Control Panel** > **Programs** > **Programs and Features** and check whether Cloudbase-Init 1.1.2 is installed.
   - If Cloudbase-Init 1.1.2 is installed, skip the subsequent steps and go to **Configure Cloudbase-Init**.
   - If Cloudbase-Init is installed but the version is not 1.1.2, uninstall Cloudbase-Init and go to the next step.
   - If Cloudbase-Init is not installed, go to the next step.
2. Check whether the OS is Windows desktop.
   - If yes, go to **3**.
   - If the OS is Windows Server, go to **4**.
3. Enable the administrator account (Windows 7 is used as an example).
   a. Click **Start** and choose **Control Panel** > **System and Security** > **Administrative Tools**.
   b. Double-click **Computer Management**.
   c. Choose **System Tools** > **Local Users and Groups** > **Users**.
   d. Right-click **Administrator** and select **Properties**.
   e. Deselect **Account is disabled**.
4. Download the Cloudbase-Init installation package.

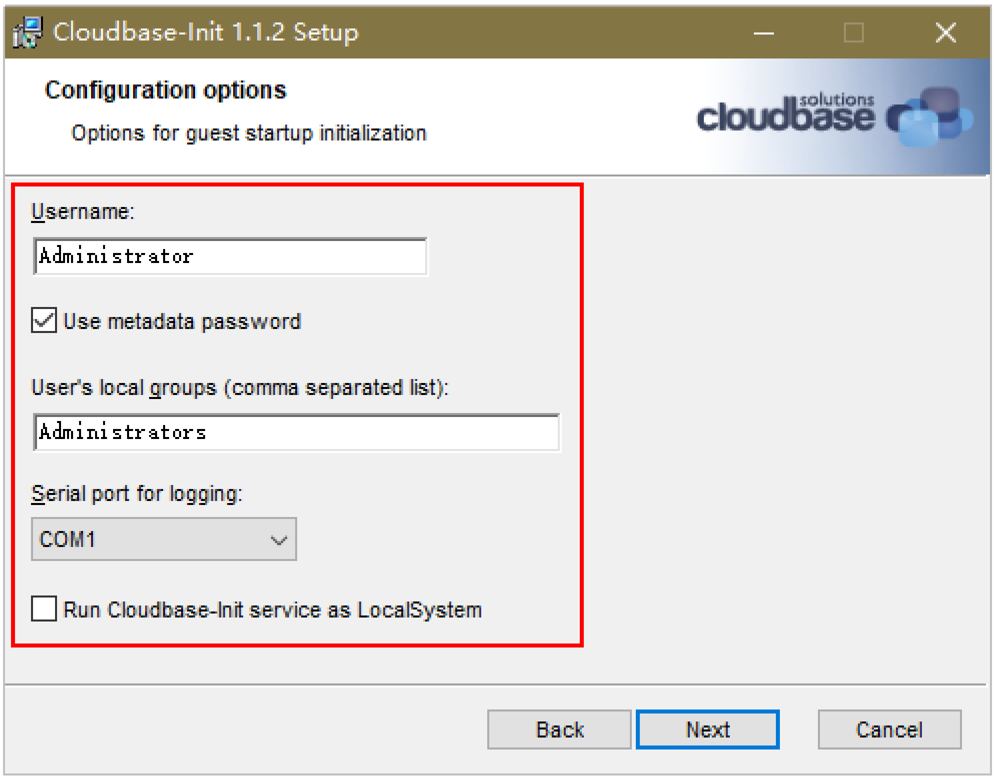
   Download the Cloudbase-Init installation package of the appropriate version based on the OS architecture from the Cloudbase-Init official website (**http://www.cloudbase.it/cloud-init-for-windows-instances/**).

   To obtain the stable version, visit the following paths:
   - 64-bit: **https://www.cloudbase.it/downloads/CloudbaseInitSetup_Stable_x64.msi**
   - 32-bit: **https://www.cloudbase.it/downloads/CloudbaseInitSetup_Stable_x86.msi**
5. Double-click the Cloudbase-Init installation package.
6. Click **Next**.
7. Select **I accept the terms in the License Agreement** and click **Next**.
8. Retain the default path and click **Next**.
9. In the **Configuration options** window, enter **Administrator** for **Username**, select **COM1** for **Serial port for logging**, and deselect **Run Cloudbase-Init service as LocalSystem**.

   NOTE

   The version number shown in the figure is for reference only.

Figure 2-5 Configuring parameters



Configuration options

Options for guest startup initialization

Username:
Administrator

☑ Use metadata password

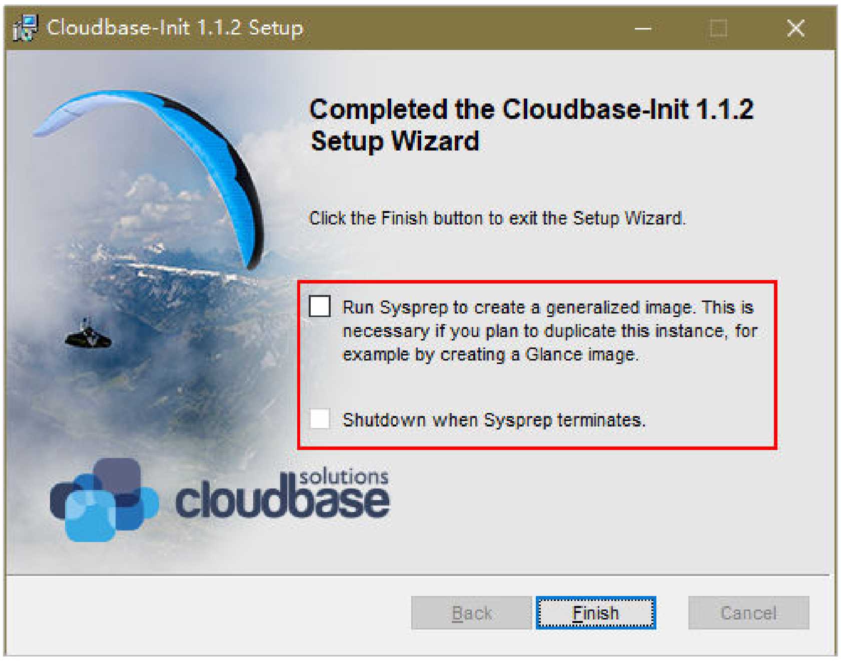
User's local groups (comma separated list):
Administrators

Serial port for logging:
COM1

□ Run Cloudbase-Init service as LocalSystem

10. Click **Next**.
11. Click **Install**.
12. In the **Files in Use** dialog box, select **Close the application and attempt to restart them** and click **OK**.
13. Check whether the version of the OS is Windows desktop.
    - If yes, go to **15**.
    - If no, go to **14**.
14. In the **Completed the Cloudbase-Init Setup Wizard** window, ensure that neither option is selected.

Figure 2-6 Completing the Cloudbase-Init installation



Cloudbase-Init 1.1.2 Setup

Completed the Cloudbase-Init 1.1.2 Setup Wizard

Click the Finish button to exit the Setup Wizard.

□ Run Sysprep to create a generalized image. This is necessary if you plan to duplicate this instance, for example by creating a Glance image.

□ Shutdown when Sysprep terminates.

NOTE

The version number shown in the figure is for reference only.

15. Click **Finish**.

Configure Cloudbase-Init

1. Edit the configuration file **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf** in the Cloudbase-Init installation path.
   a. Add **netbios_host_name_compatibility=false** to the last line of the file so that the hostname can have a maximum of 63 characters.

      NOTE

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

   b. Add **metadata_services=cloudbaseinit.metadata.services.httpservice.HttpService** to enable the agent to access the IaaS OpenStack data source.
   c. Add **plugins** to configure the plugins that will be loaded. Separate plugins with commas (,). The information in bold is the keyword of each plugin.
      - The following plugins are loaded by default. You can keep all or some of them as needed.

        ```
        plugins=cloudbaseinit.plugins.common.localscripts.LocalScriptsPlugin,cloudbaseinit.plugins.common.mtu.MTUPlugin,cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,cloudbaseinit.plugins.common.setuserpassword.SetUserPasswordPlugin,cloudbaseinit.plugins.common.sshpublickeys.SetUserSSHPublicKeysPlugin,cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin,cloudbaseinit.plugins.windows.extendvolumes.ExtendVolumesPlugin,cloudbaseinit.plugins.common.userdata.UserDataPlugin,cloudbaseinit.plugins.windows.licensing.WindowsLicensingPlugin
        ```

        Plugin functions:

  - **LocalScriptsPlugin** configures scripts.
  - **MTUPlugin** configures MTU network interfaces.
  - **CreateUserPlugin** creates a user.
  - **SetUserPasswordPlugin** configures a password.
  - **SetUserSSHPublicKeysPlugin** configures a key.
  - **SetHostNamePlugin** configures a hostname.
  - **ExtendVolumesPlugin** expands disk space.
  - **UserDataPlugin** injects user data.
  - **WindowsLicensingPlugin** activates Windows instances.

  NOTE

  If you need to change the hostname of ECSs after they are created from this image, and services on the ECSs are sensitive to hostname changes, you are not advised to configure the **SetHostNamePlugin** here.

- Optional plugins:

```
plugins=cloudbaseinit.plugins.windows.winrmlistener.ConfigWinRMListenerPlugin,cloudbaseinit.plugins.windows.winrmcertificateauth.ConfigWinRMCertificateAuthPlugin
```

  Plugin functions:

  - **ConfigWinRMListenerPlugin** configures listening to remote logins.
  - **ConfigWinRMCertificateAuthPlugin** configures remote logins without password authentication.

  ⚠ CAUTION

  The WinRM plug-ins use weak cryptographic algorithm, which may cause security risks. So, you are advised not to load these plug-ins.

d. (Optional) Add the following configuration items to configure the number of retry times and interval for obtaining metadata:

```
retry_count=40
retry_count_interval=5
```

e. (Optional) Add the following configuration item to prevent metadata network disconnections caused by the default route added by Windows:

```
[openstack]
add_metadata_private_ip_route=False
```

f. (Optional) If the Cloudbase-Init version is 0.9.12 or later, you can customize the password length.

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

g. (Optional) Add the following configuration item to disable password changing upon first login:

   first_logon_behaviour=no

h. (Optional) Add the following configuration item to ensure that time synchronization from BIOS persists through system restarts:

   real_time_clock_utc=true

NOTE

The registry entry **RealTimeIsUniversal=1** allows the system to synchronize time from BIOS. If **real_time_clock_utc=true** is not added, Cloudbase-Init will be set **RealTimeIsUniversal** back to **0**, causing the system to not synchronize time from BIOS after a restart.

2. Release the current DHCP address so that the created ECSs can obtain correct addresses.

   In the Windows command line, run the following command to release the current DHCP address:

   ipconfig /release

   NOTE

   This operation will interrupt network connection and adversely affect ECS use. The network will automatically recover after the ECSs are started again.

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

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

   Table 2-5 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

2.2.4 Installing the One-Click Password Reset Plug-In

Scenarios

You are advised to install the password reset plug-in CloudResetPwdAgent before creating a private image. In this way, you can reset the password of ECSs created from the image by a few clicks.

- ECSs created from a public image have this plug-in installed by default.
- For ECSs created from an external image file, install the plug-in by performing the operations in this section.

Precautions

- You can decide whether to install the CloudResetPwdAgent plug-in.
- The plug-in has been open-sourced in the GitHub open-source platform according to *GNU General Public License V2.0*.
- **Table 2-6** lists the OSs that support this plug-in.

Table 2-6 OSs that support the one-click password reset plug-in

OS Type	OS Version
Windows	Windows Server 2016 Datacenter 64bit Windows Server 2012 R2 Standard 64bit Windows Server 2012 R2 Datacenter 64bit Windows Server 2008 R2 Enterprise 64bit Windows Server 2008 SP2 Enterprise 64bit Windows Server 2008 R2 Datacenter 64bit Windows Server 2008 R2 Standard 64bit Windows Server 2008 R2 WEB 64bit

Prerequisites

- The ECS status is **Running**.
- The ECS must have a remaining space of more than 300 MB, and data can be written to its drive C.
- DHCP must be enabled for the VPC used by the ECS.
- Networks of the ECS are normal.
- The outbound security group rule of the ECS must meet the following requirements:
  - **Protocol**: **TCP**
  - **Port Range**: **80**
  - **Remote End**: **169.254.0.0/16**

  If you use the default outbound security group rule, preceding requirements can be met, and the ECS can be initialized. The default outbound security group rule is as follows:

- **Protocol**: **All**
- **Port Range**: **All**
- **Remote End**: **0.0.0.0/16**

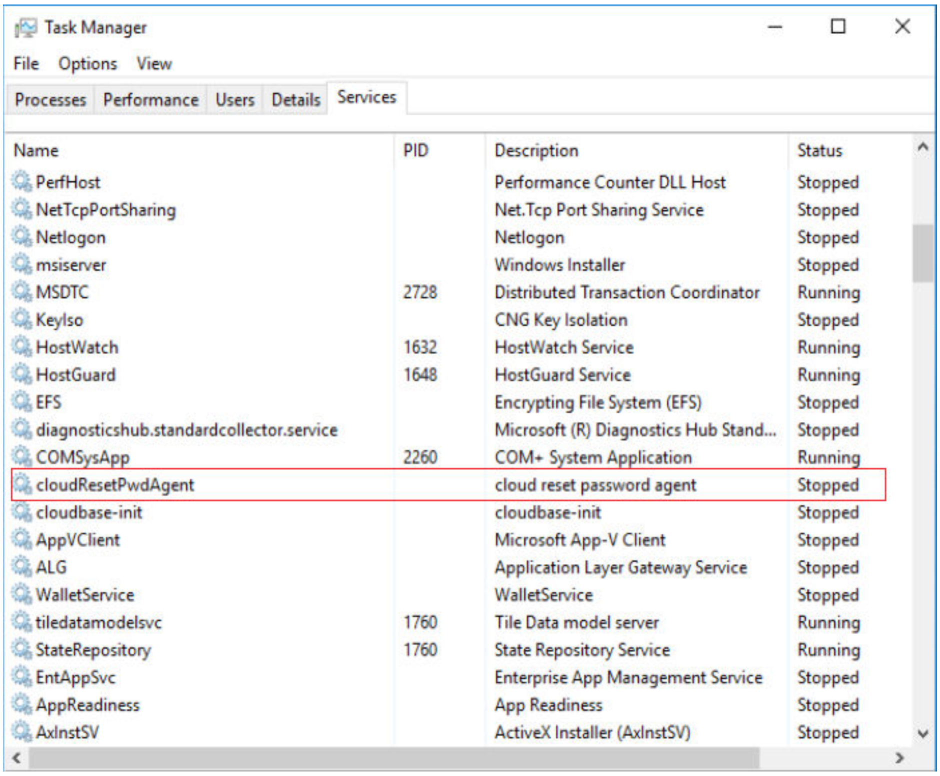
Procedure

Step 1 Log in to the ECS.

Step 2 Check whether the password reset plug-in CloudResetPwdAgent has been installed on the ECS.

Start the **Task Manager** and check whether **cloudResetPwdAgent** is displayed on the **Services** tab. As shown in **Figure 2-7**, the password reset plug-in has been installed on the ECS.

Figure 2-7 Successful plug-in installation



Name	PID	Description	Status
PerfHost		Performance Counter DLL Host	Stopped
NetTcpPortSharing		Net.Tcp Port Sharing Service	Stopped
Netlogon		Netlogon	Stopped
msiserver		Windows Installer	Stopped
MSDTC	2728	Distributed Transaction Coordinator	Running
KeyIso		CNG Key Isolation	Stopped
HostWatch	1632	HostWatch Service	Running
HostGuard	1648	HostGuard Service	Running
EFS		Encrypting File System (EFS)	Stopped
diagnosticshub.standardcollector.service		Microsoft (R) Diagnostics Hub Stand...	Stopped
COMSysApp	2260	COM+ System Application	Running
cloudResetPwdAgent		cloud reset password agent	Stopped
cloudbase-init		cloudbase-init	Stopped
AppVClient		Microsoft App-V Client	Stopped
ALG		Application Layer Gateway Service	Stopped
WalletService		WalletService	Stopped
tiledatamodelsvc	1760	Tile Data model server	Running
StateRepository	1760	State Repository Service	Running
EntAppSvc		Enterprise App Management Service	Stopped
AppReadiness		App Readiness	Stopped
AxInstSV		ActiveX Installer (AxInstSV)	Stopped

- If the installation is successful, no further action is required.
- Otherwise, go to **3**.

Step 3 Download **CloudResetPwdAgent.zip** and verify its integrity by referring to **Obtaining the One-Click Password Reset Plug-in (Linux)**.

There is no special requirement for the directory that stores **CloudResetPwdAgent.zip**.

Step 4 Decompress **CloudResetPwdAgent.zip**.

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

Step 5 Install the plug-in.

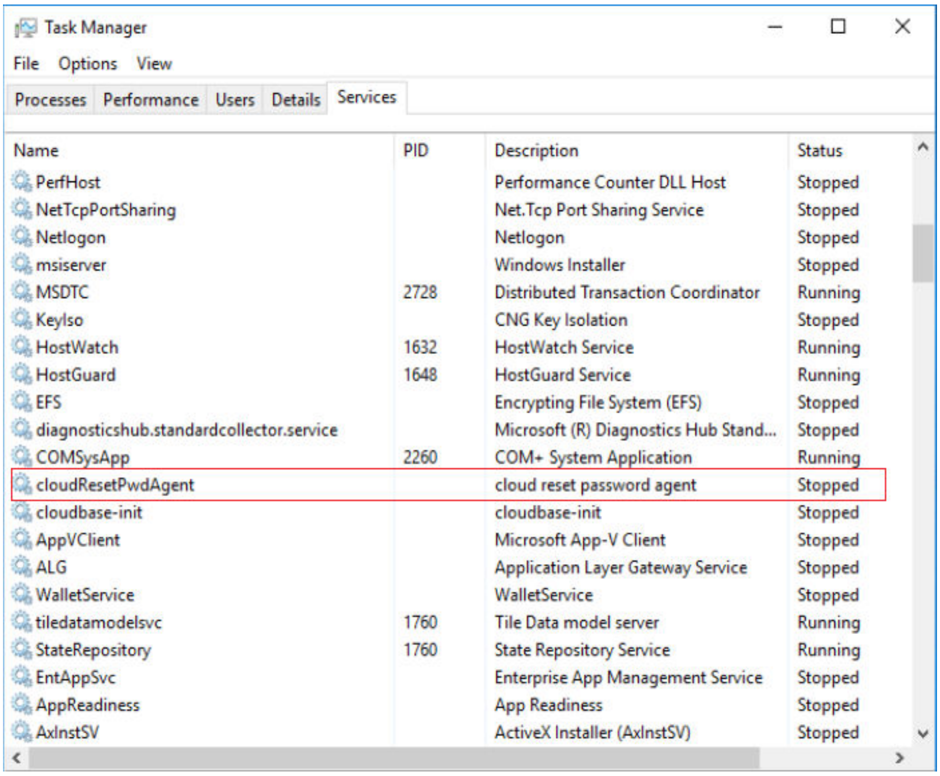
1. Double-click **setup.bat** in **CloudResetPwdAgent.Windows**.

   The password reset plug-in starts to be installed.

2. View the **Task Manager** and check whether the installation was successful.

   If **cloudResetPwdAgent** is displayed in the **Task Manager**, as shown in **Figure 2-8**, the installation was successful. Otherwise, the installation failed.

Figure 2-8 Successful plug-in installation



Name	PID	Description	Status
PerfHost		Performance Counter DLL Host	Stopped
NetTcpPortSharing		Net.Tcp Port Sharing Service	Stopped
Netlogon		Netlogon	Stopped
msiserver		Windows Installer	Stopped
MSDTC	2728	Distributed Transaction Coordinator	Running
KeyIso		CNG Key Isolation	Stopped
HostWatch	1632	HostWatch Service	Running
HostGuard	1648	HostGuard Service	Running
EFS		Encrypting File System (EFS)	Stopped
diagnosticshub.standardcollector.service		Microsoft (R) Diagnostics Hub Stand...	Stopped
COMSysApp	2260	COM+ System Application	Running
cloudResetPwdAgent		cloud reset password agent	Stopped
cloudbase-init		cloudbase-init	Stopped
AppVClient		Microsoft App-V Client	Stopped
ALG		Application Layer Gateway Service	Stopped
WalletService		WalletService	Stopped
tiledatamodelsvc	1760	Tile Data model server	Running
StateRepository	1760	State Repository Service	Running
EntAppSvc		Enterprise App Management Service	Stopped
AppReadiness		App Readiness	Stopped
AxInstSV		ActiveX Installer (AxInstSV)	Stopped

NOTE

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

----End

2.2.5 Running Sysprep

Scenarios

Running Sysprep ensures that an ECS has a unique SID after it is joined to a domain.

After installing Cloudbase-Init on an ECS, you need to decide whether the ECS needs to be added to a domain or whether it must have a unique SID. If yes, run Sysprep as instructed in this section.

Prerequisites

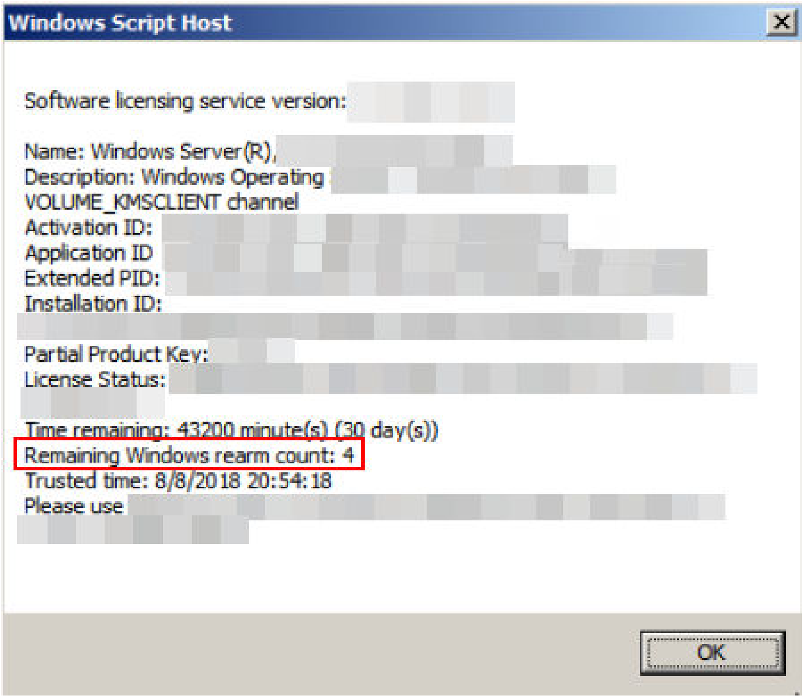
- Run Sysprep as the administrator.
- For a newly activated Windows ECS, you can run Sysprep only once at a time.
- If an ECS is created from an image file, only Sysprep provided by the image file can be used. In addition, Sysprep must always reside in the **%WINDIR%\system32\sysprep** directory.
- Windows must be in the activated state, and the remaining Windows rearm count must be greater than or equal to 1. Otherwise, the Sysprep encapsulation cannot be executed.

  Run the following command in the Windows command line and check how many times you can run Sysprep in the displayed **Windows Script Host** dialog box:

  slmgr.vbs /dlv

  If the value of **Remaining Windows rearm count** is **0**, you cannot run Sysprep.

  Figure 2-9 Windows Script Host



```
Software licensing service version: [redacted]

Name: Windows Server(R), [redacted]
Description: Windows Operating [redacted]
VOLUME_KMSCLIENT channel
Activation ID: [redacted]
Application ID [redacted]
Extended PID: [redacted]
Installation ID:
[redacted]
Partial Product Key: [redacted]
License Status: [redacted]
[redacted]

Time remaining: 43200 minute(s) (30 day(s))
Remaining Windows rearm count: 4
Trusted time: 8/8/2018 20:54:18
Please use [redacted]
[redacted]
```

Procedure

1. Enter the Cloudbase-Init installation directory.

   C:\Program Files\Cloudbase Solutions is used as an example of the Cloudbase-Init installation directory. Switch to the root directory of drive C and run the following command to enter the installation directory:

   cd C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf

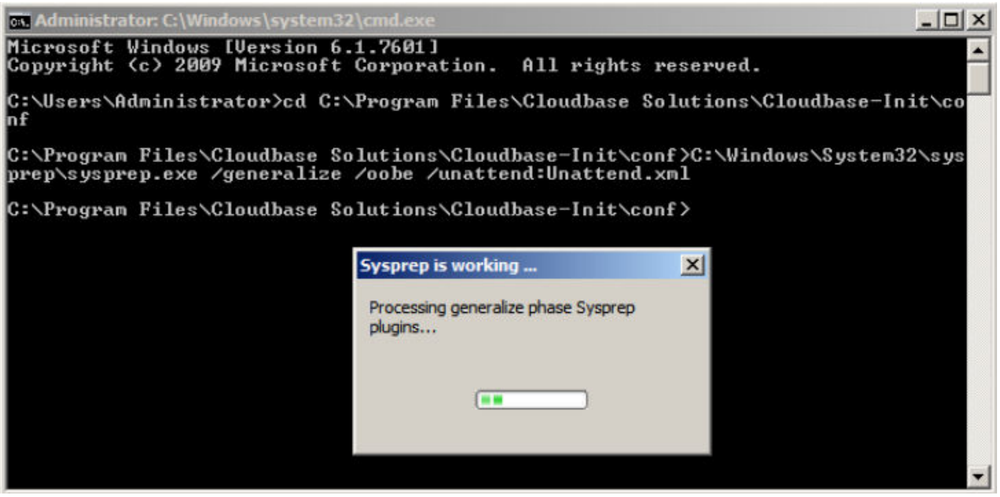
2. Run the following command to encapsulate Windows:

   C:\Windows\System32\sysprep\sysprep.exe /generalize /oobe /unattend:Unattend.xml

CAUTION

- Ensure that **/unattend:Unattend.xml** is contained in the preceding command. Otherwise, the username, password, and other important configuration information of the ECS will be reset, and you must configure the OS manually when you use ECSs created from the Windows private image.
- After this command is executed, the ECS will be automatically stopped. After the ECS is stopped, use the ECS to create an image. ECSs created using the image have unique SIDs. If you restart a Windows ECS on which Sysprep has been executed, Sysprep takes effect only for the current ECS. Before creating an image using the ECS, you must run Sysprep again.
- For Windows Server 2012 and Windows Server 2012 R2, the administrator password of the ECS will be deleted after Sysprep is executed on the ECS. You need to log in to the ECS and reset the administrator password. In this case, the administrator password set on the management console will be invalid. Keep the password you set secure.
- If a domain account is required for logins, run Sysprep on the ECS before using it to create a private image. For details about the impact of running Sysprep, see **Why Is Sysprep Required for Creating Private Images Using a Windows ECS?**
- The Cloudbase-Init account of a Windows ECS is an internal account of the Cloudbase-Init agent. This account is used for obtaining metadata and completing relevant configuration when the Windows ECS starts. If you modify or delete this account, or uninstall the Cloudbase-Init agent, you will be unable to inject initial custom information into an ECS created from a Windows private image. Therefore, you are not advised to modify or delete the Cloudbase-Init account.

Figure 2-10 Running Sysprep



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>cd C:\Program Files\Cloudbase Solutions\Cloudbase-Init\co
nf

C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf>C:\Windows\System32\sys
prep\sysprep.exe /generalize /oobe /unattend:Unattend.xml

C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf>
```

Sysprep is working ...

Processing generalize phase Sysprep plugins...

Follow-up Procedure

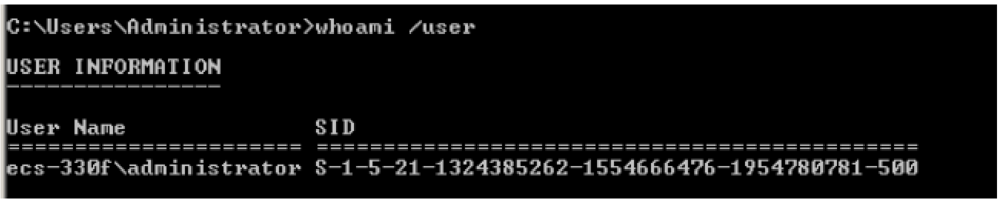
1. Use this ECS to create a private image. For details see **Creating a System Disk Image from an ECS**.

2. Use the image to create ECSs. Each ECS will have a unique SID.

   Run the following command to query the ECS SID:

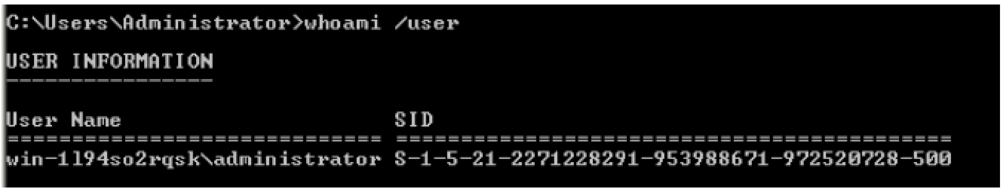
   whoami /user

   Figure 2-11 ECS SID before Sysprep is executed

```
C:\Users\Administrator>whoami /user

USER INFORMATION
----------------

User Name               SID
======================= =============================================
ecs-330f\administrator S-1-5-21-1324385262-1554666476-1954780781-500
```

   Figure 2-12 ECS SID after Sysprep is executed

```
C:\Users\Administrator>whoami /user

USER INFORMATION
----------------

User Name                      SID
============================== ===========================================
win-1194so2rqsk\administrator S-1-5-21-2271228291-953988671-972520728-500
```

2.2.6 Installing PV Drivers

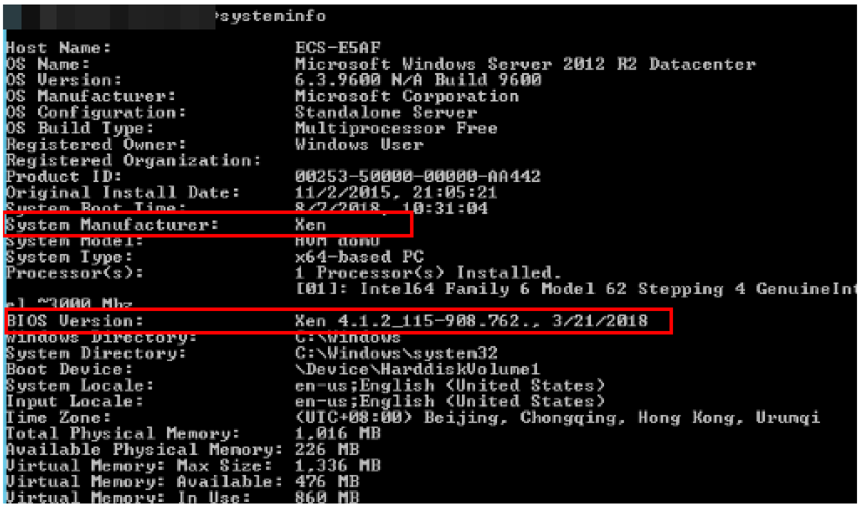
This section only applies to Xen ECSs, which have been discontinued and no longer been available for new users. For details, see **Discontinued ECS Specifications** If you are a new user or you are an existing user that will use this image to create a non-Xen ECS, skip this section.

Run the following command in the cmd window of an ECS to check its virtualization type:

systeminfo

In the command output, if the values of **System Manufacturer** and **BIOS Version** are **XEN**, the virtualization type is Xen.

Figure 2-13 Checking the virtualization type of a Windows ECS



```
[redacted]>systeminfo

Host Name:                 ECS-E5AF
OS Name:                   Microsoft Windows Server 2012 R2 Datacenter
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00253-50000-00000-AA442
Original Install Date:     11/2/2015, 21:05:21
System Boot Time:          8/7/2018, 10:31:04
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 62 Stepping 4 GenuineInt
el ~3000 Mhz
BIOS Version:              Xen 4.1.2_115-908.762., 3/21/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Total Physical Memory:     1,016 MB
Available Physical Memory: 226 MB
Virtual Memory: Max Size:  1,336 MB
Virtual Memory: Available: 476 MB
Virtual Memory: In Use:    860 MB
```

Scenarios

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

NOTICE

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

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

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

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

- If the PV driver version is later than 2.5, you do not need to install new PV drivers.
- If the PV driver version is not displayed or the version is 2.5 or earlier, perform operations in **Installing PV Drivers** or **Installing the PV Driver Upgrade Package**.

Prerequisites

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

Obtaining the PV Driver Package

Table 2-7 lists the PV driver packages required for optimizing Windows private images.

Table 2-7 PV driver packages

Software Package	OS	How to Obtain
pvdriver-win2008R2-64bit.zip	Windows Server 2008 R2 64bit	**https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2008R2-64bit.zip**
pvdriver-win2012-64bit.zip	Windows Server 2012 64bit	**https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2012-64bit.zip**
pvdriver-win2012R2-64bit.zip	Windows Server 2012 R2 64bit	**https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2012R2-64bit.zip**
pvdriver-win2016-64bit.zip	Windows Server 2016 64bit	**https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2016-64bit.zip**
pvdriver-win2019-64bit.zip	Windows Server 2019 64bit	**https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2019-64bit.zip**

Installing PV Drivers

1. Log in to the Windows ECS using VNC.

   For details about how to log in to an ECS, see **Login Overview**.

   NOTE

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

2. On the ECS, choose **Start** > **Control Panel**.
3. Click **Uninstall a program**.
4. Uninstall **GPL PV drivers for Windows** *x.x.x.xx* as prompted.
5. Download PV drivers of the required version based on the ECS OS and instructions in **Obtaining the PV Driver Package**.
6. Decompress the PV driver package.
7. Right-click **GPL PV Drivers for Windows** *x.x.x.xx*, select **Run as administrator**, and complete the installation as prompted.
8. Restart the ECS as prompted to make the PV drivers take effect.

   ECSs running Windows Server 2008 must be restarted twice.

NOTE

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

Installing the PV Driver Upgrade Package

1. Log in to the Windows ECS using VNC.

   For details about how to log in to an ECS, see **Login Overview**.

   NOTE

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

2. On the ECS, choose **Start** > **Control Panel**.
3. Choose **Programs** > **Uninstall a program**, find PV drivers, and uninstall them.
4. After the uninstallation is complete, restart the ECS to clear the environment.
5. Download **pvdriver-windows.zip** from the following link:

   https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-windows.zip

6. Download **pvdriver-windows.zip** from the following link:
7. Click **Setup.exe** to install new PV drivers. The package will automatically adapt to the OS version.
8. Restart the ECS as prompted to make the PV drivers take effect.

   ECSs running Windows Server 2008 must be restarted twice.

   NOTE

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

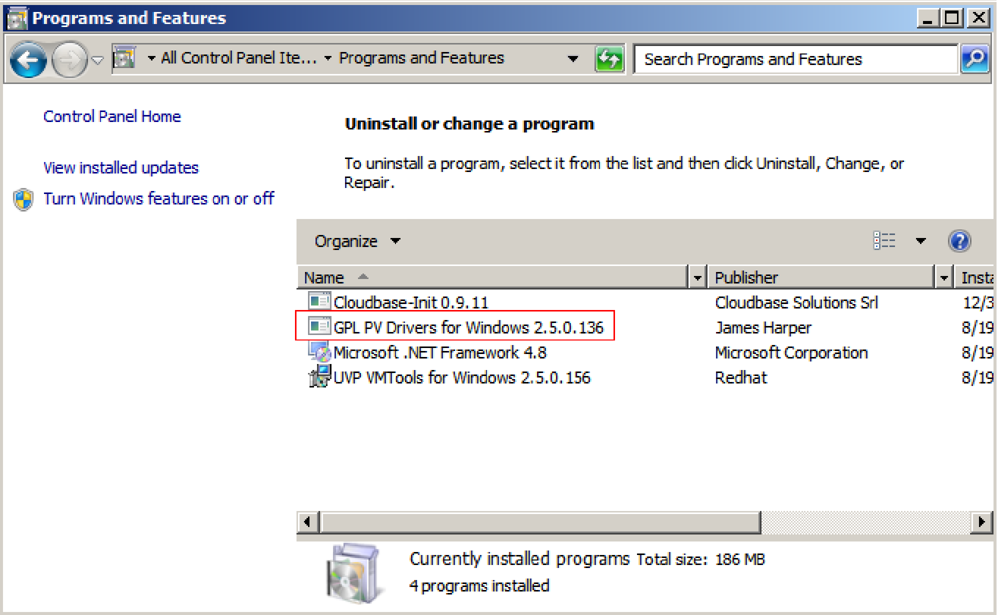
Verifying the Installation

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

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

   If PV drivers for Windows exist, the installation is successful, as shown in **Figure 2-14**.

Figure 2-14 Verifying the installation



Programs and Features
All Control Panel Ite... ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Insta
Cloudbase-Init 0.9.11	Cloudbase Solutions Srl	12/3
GPL PV Drivers for Windows 2.5.0.136	James Harper	8/19
Microsoft .NET Framework 4.8	Microsoft Corporation	8/19
UVP VMTools for Windows 2.5.0.156	Redhat	8/19

Currently installed programs Total size: 186 MB
4 programs installed

2.2.7 Installing VirtIO Drivers

Scenarios

VirtIO is a standard interface for VMs to access host devices. It is used to improve the I/O performance between VMs and hosts. For details about VirtIO, see **VirtIO**. For details about open source code of virtio-win/kvm-guest-drivers-windows, see **https://github.com/virtio-win/kvm-guest-drivers-windows**.

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

This section describes how to install VirtIO drivers on a KVM ECS.

NOTICE

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

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

Prerequisites

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

Installing VirtIO Drivers

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

1. Log in to the Windows ECS using VNC.

   For details about how to log in to an ECS, see **Login Overview**.

   NOTE

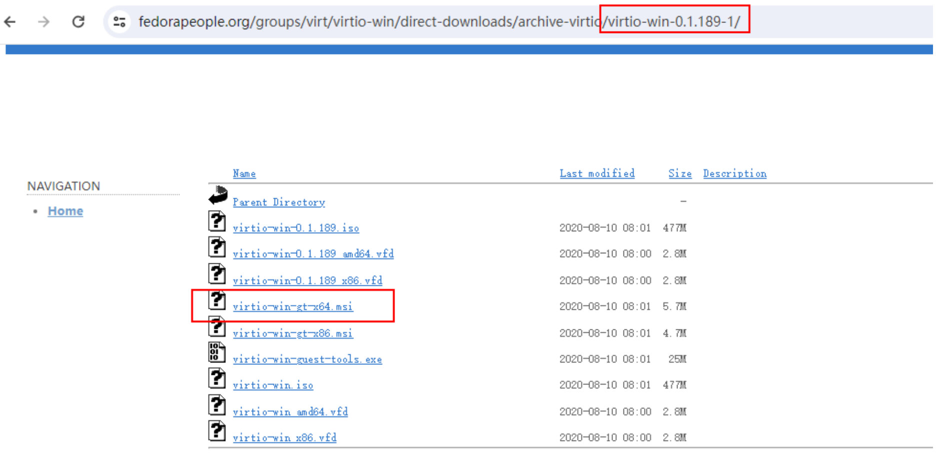
   You must log in to the ECS using VNC. Remote desktop connection is not allowed because the NIC driver needs to be updated during the installation but the NIC is in use for the remote desktop connection. As a result, the installation will fail.

2. Download VirtIO drivers.

   Download path:

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

   Figure 2-15 Downloading a driver package



fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/virtio-win-0.1.189-1/

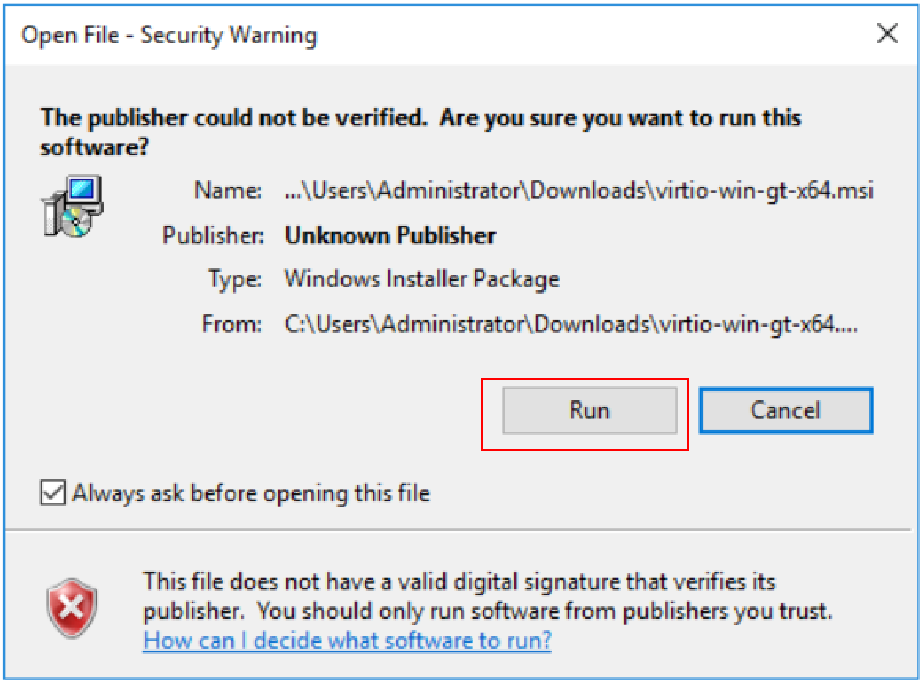
NAVIGATION

- Home

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

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

   Figure 2-16 Starting the installation



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: ...\Users\Administrator\Downloads\virtio-win-gt-x64.msi

Publisher: **Unknown Publisher**

Type: Windows Installer Package

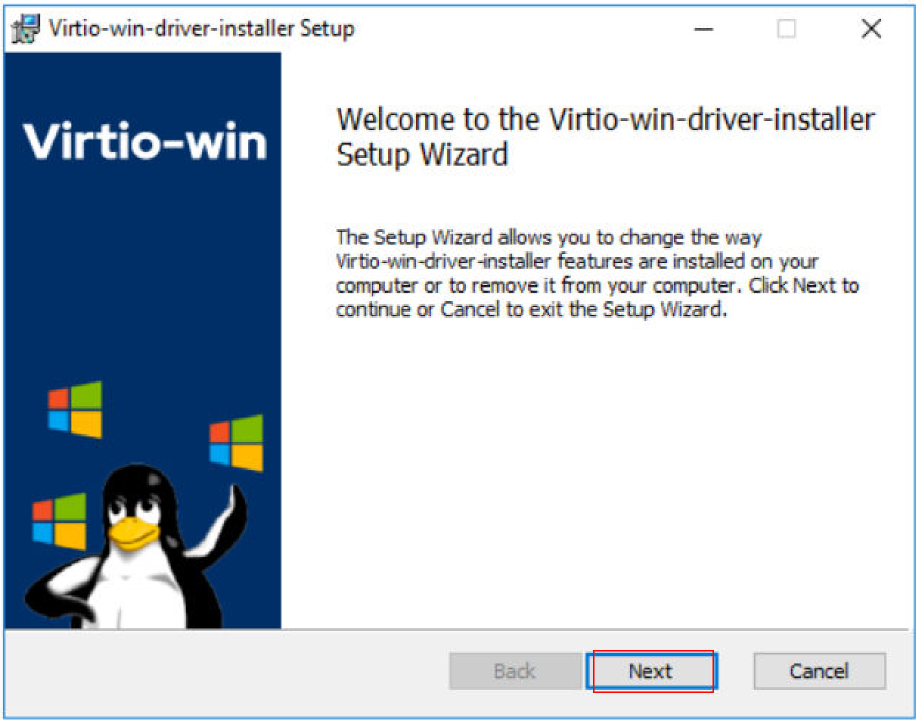
From: C:\Users\Administrator\Downloads\virtio-win-gt-x64....

Run | Cancel

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Figure 2-17 Installation wizard

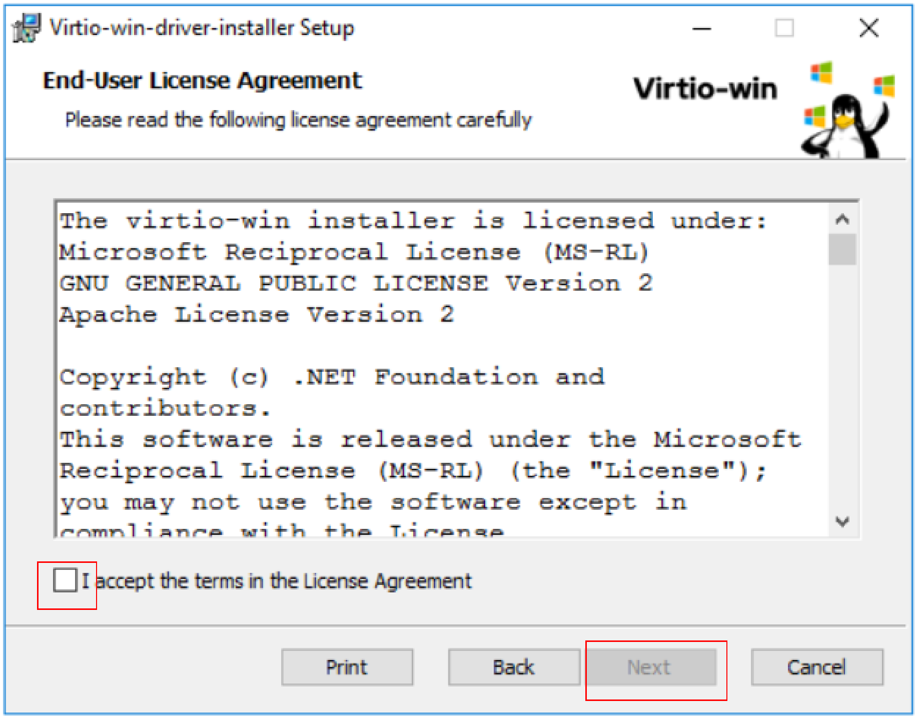


Virtio-win-driver-installer Setup

Welcome to the Virtio-win-driver-installer Setup Wizard

The Setup Wizard allows you to change the way Virtio-win-driver-installer features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 2-18 Accepting the agreement



Virtio-win-driver-installer Setup

End-User License Agreement

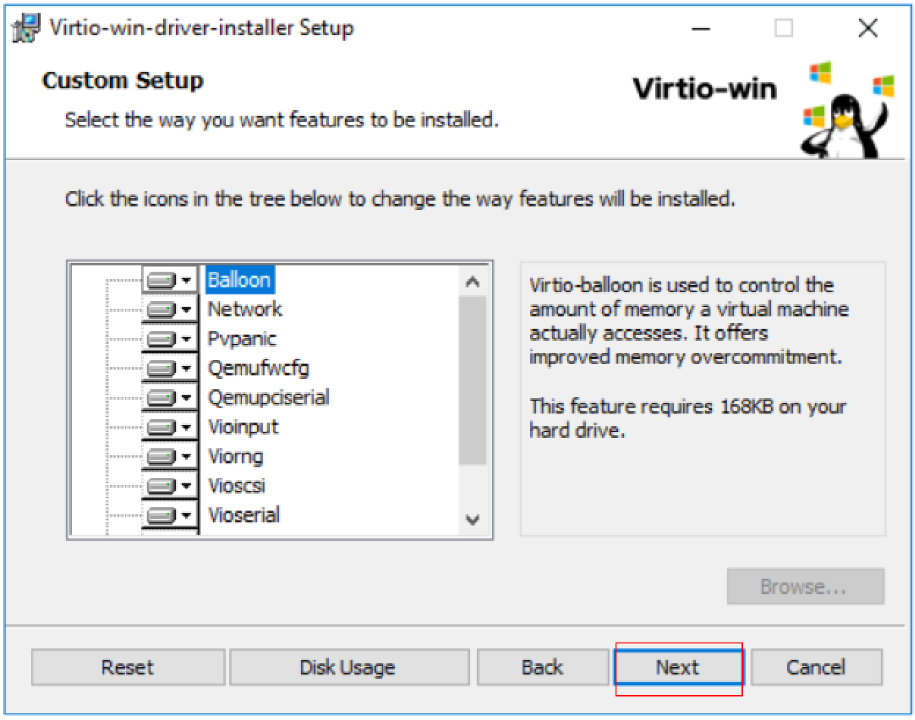
Please read the following license agreement carefully

```
The virtio-win installer is licensed under:
Microsoft Reciprocal License (MS-RL)
GNU GENERAL PUBLIC LICENSE Version 2
Apache License Version 2

Copyright (c) .NET Foundation and
contributors.
This software is released under the Microsoft
Reciprocal License (MS-RL) (the "License");
you may not use the software except in
compliance with the License
```

□ I accept the terms in the License Agreement

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

Figure 2-19 Selecting VirtIO drivers to install



Virtio-win-driver-installer Setup

Custom Setup

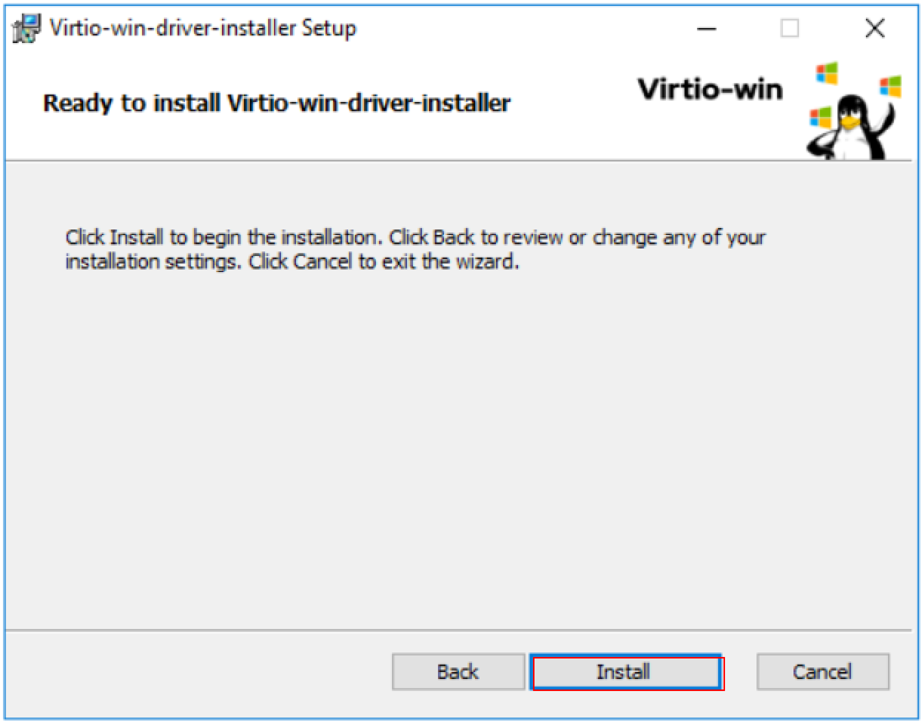
Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

Virtio-balloon is used to control the amount of memory a virtual machine actually accesses. It offers improved memory overcommitment.

This feature requires 168KB on your hard drive.

Figure 2-20 Proceeding with the installation.



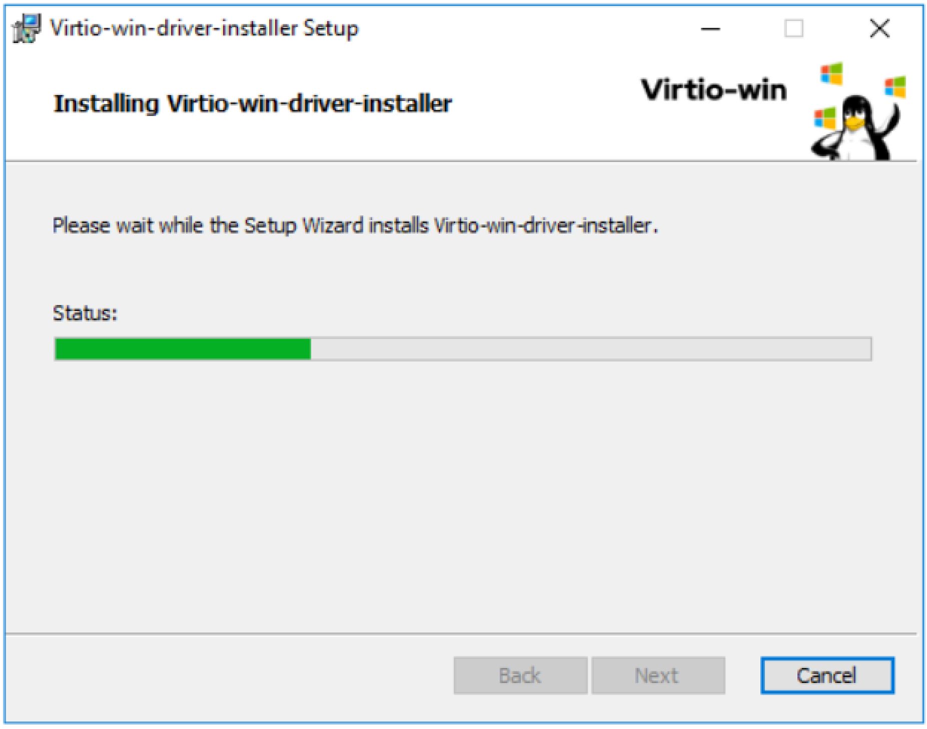
Virtio-win-driver-installer Setup

Ready to install Virtio-win-driver-installer

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

4. Wait until the installation is complete.

Figure 2-21 Installation in process



Virtio-win-driver-installer Setup

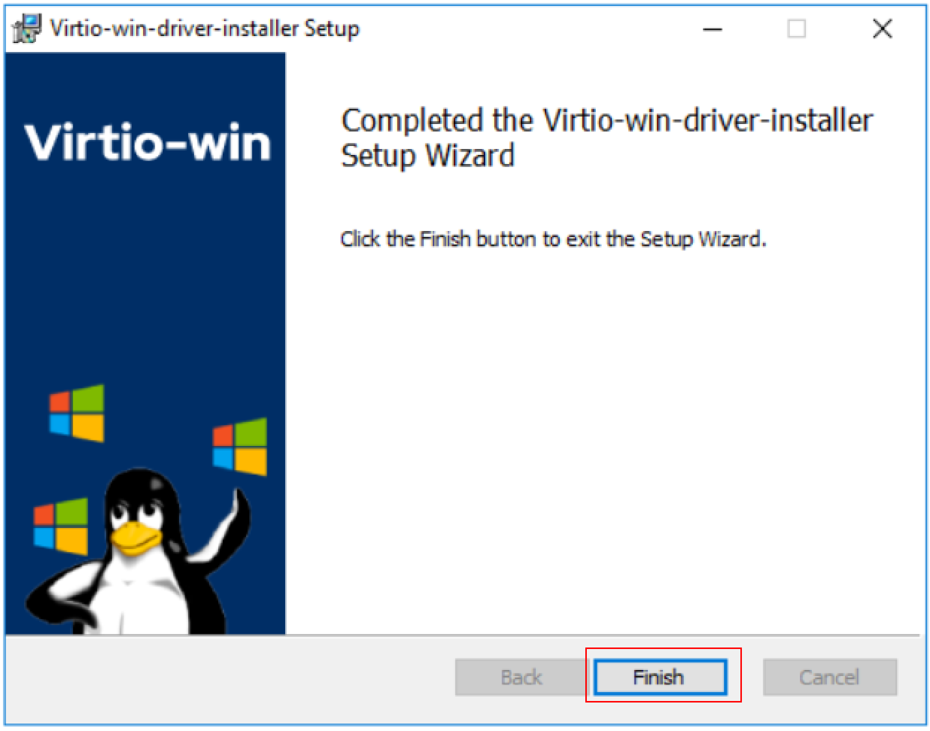
Installing Virtio-win-driver-installer

Please wait while the Setup Wizard installs Virtio-win-driver-installer.

Status:

5. Restart the ECS after the installation is complete.

Figure 2-22 Installation completed

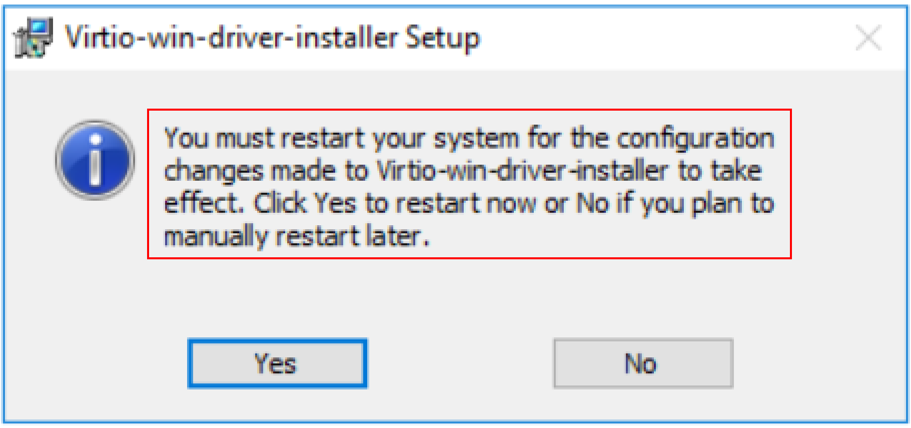


Virtio-win-driver-installer Setup

Completed the Virtio-win-driver-installer Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 2-23 Restart prompt



You must restart your system for the configuration changes made to Virtio-win-driver-installer to take effect. Click Yes to restart now or No if you plan to manually restart later.

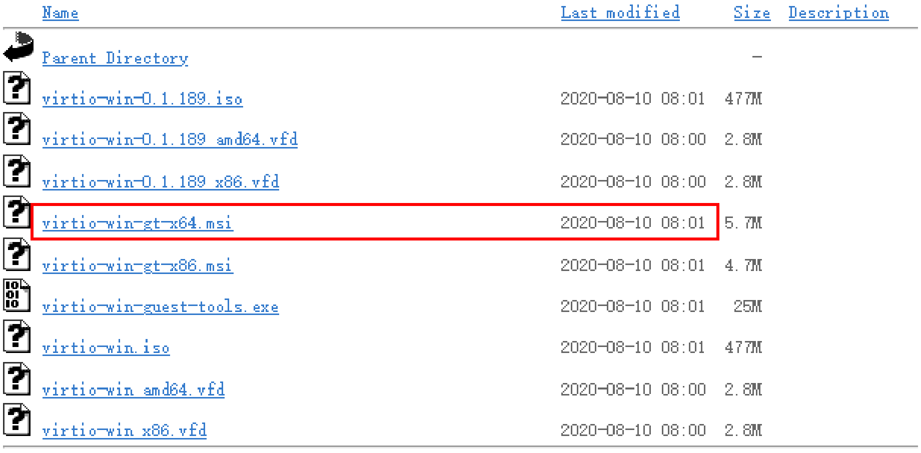
6. After the restart, perform the operations in **Verifying the Installation** to verify that the VirtIO drivers have been successfully installed.

Verifying the Installation

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

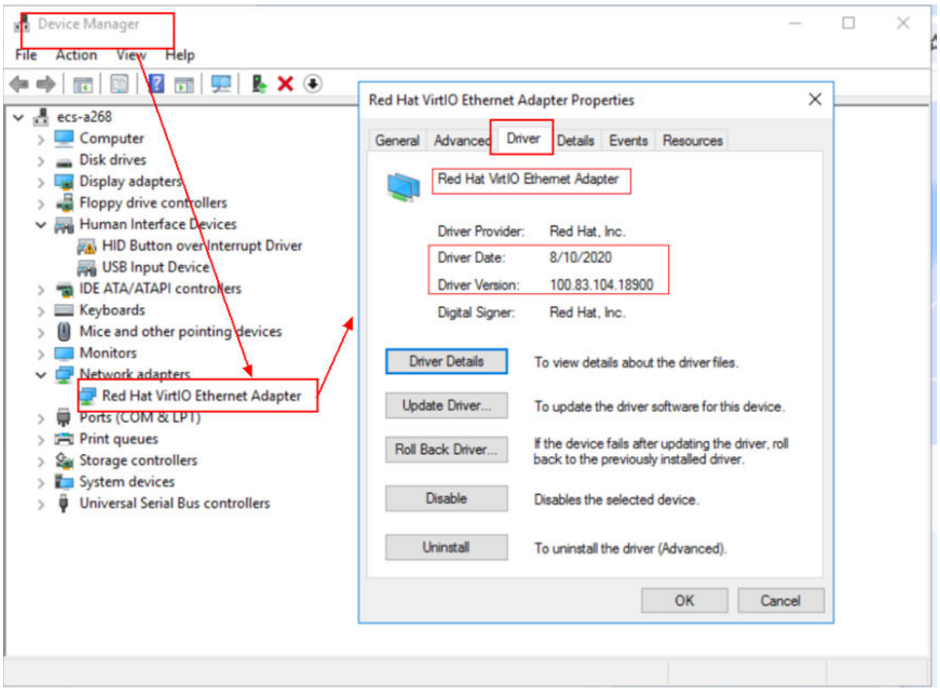
1. Open **Device Manager** and search for VirtIO drivers.
2. Check whether the VirtIO driver version and date displayed in **Device Manager** are the same as those of the VirtIO drivers you downloaded. If they are the same, the VirtIO drivers have been installed successfully.

Figure 2-24 Version and date of downloaded drivers



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

Figure 2-25 Version and date of drivers in Device Manager



Red Hat VirtIO Ethernet Adapter Properties

Red Hat VirtIO Ethernet Adapter

Driver Provider: Red Hat, Inc.

Driver Date: 8/10/2020

Driver Version: 100.83.104.18900

Digital Signer: Red Hat, Inc.

Driver Details: To view details about the driver files.

Update Driver...: To update the driver software for this device.

Roll Back Driver...: If the device fails after updating the driver, roll back to the previously installed driver.

Disable: Disables the selected device.

Uninstall: To uninstall the driver (Advanced).

Follow-up Procedure

1. On the ECS, choose **Control Panel** > **Power Options**. Click **Choose when to turn off the display**, select **Never** for **Turn off the display**, and save the changes.
2. After the installation of VirtIO drivers is complete, perform the following operations to clear system logs:
   a. For Windows Server 2008 and Windows Server 2012, right-click **Computer** and select **Manage**.
   b. In the displayed dialog box, choose **System Tools** > **Event Viewer** > **Windows Logs** and delete logs of five items.
   c. Stop the ECS.

2.3 Linux Private Images

2.3.1 Configuring DHCP

Scenarios

If a private image is created from an ECS or external image file and the VM where the ECS or external image file is located is configured with a static IP address, you need to configure DHCP so that the new ECSs created from the private image can dynamically obtain an IP address.

The configuration method varies depending on OSs.

NOTE

When registering an external image file as a private image, configure DHCP on the VM where the external image file is located. You are advised to configure DHCP on the VM and then export the image file.

Prerequisites

You have logged in to the ECS used to create a Windows private image.

For details about how to log in to an ECS, see **Login Overview**.

Ubuntu 18 or Later

1. Run **vi /etc/netplan/01-netcfg.yaml** on the ECS to open the **/etc/netplan/01-netcfg.yaml** file, and check whether the value of **dhcp4** is **true**.
   - If **dhcp4** is set to **true**, enter **:q** to exit the editor. No further action will be required.
     ```
     network:
       version:2
       renderer:NetworkManager
       ethernets:
         eth0:
           dhcp4: true
     ```
   - If **dhcp4** is set to **no** and a static IP address is configured, go to the next step.
     ```
     network:
       version:2
       renderer:NetworkManager
       ethernets:
         eth0:
           dhcp4: no
           addresses: [192.168.1.109/24]
           gateway4: 192.168.1.1
           nameservers:
             addresses: [8.8.8.8,114.114.114.114]
     ```
2. Press **i** to enter the editing mode.

   Delete the static IP address settings and set **dhcp4** to **true**. You can also use a number sign (#) to comment out the static IP address settings.
   ```
   network:
     version:2
     renderer:NetworkManager
     ethernets:
       eth0:
         dhcp4: true   # Set dhcp4 to true.
         #dhcp4: no    # Delete or comment out the static IP address settings.
         #addresses: [192.168.1.109]
         #gateway4: 192.168.1.1
         #nameservers:
         # addresses: [8.8.8.8,114.114.114.114]
   ```
3. If your ECS has more than one NIC, configure DHCP for all of them.
   ```
   network:
     version:2
     renderer:NetworkManager
     ethernets:
       eth0:
         dhcp4: true
       eth1:
         dhcp4: true
       eth2:
         dhcp4: true
   ```

```
    eth3:
      dhcp4: true
```

4. Press **Esc**, enter **:wq**, and press **Enter** to save the settings and exit the vi editor.
5. Run the **netplan apply** command to make the settings take effect.

Ubuntu 16.04

1. Run the following command on the ECS to open the **/etc/network/interfaces** file:

   vi /etc/network/interfaces

   - If DHCP has been configured for all NICs, enter **:q** to exit the vi editor.
     ```
     auto lo
     iface lo inet loopback
     auto eth0
     iface eth0 inet dhcp

     auto eth1
     iface eth1 inet dhcp
     ```
   - If static IP addresses are set on the NICs, go to **2**.
     ```
     auto lo
     iface lo inet loopback
     auto eth0
     #iface eth0 inet dhcp
     iface eth0 inet static
     address 192.168.1.109
     netmask 255.255.255.0
     gateway 192.168.1.1
     ```
2. Press **i** to enter the editing mode.
3. Delete the static IP address settings and configure DHCP for the NICs.

   You can also use a number sign (#) to comment out the static IP address settings.
   ```
   auto lo
   iface lo inet loopback
   auto eth0
   iface eth0 inet dhcp
   ```
   If the ECS has multiple NICs, you must configure DHCP for all the NICs.
   ```
   auto lo
   iface lo inet loopback
   auto eth0
   iface eth0 inet dhcp
   auto eth1
   iface eth1 inet dhcp
   ```
4. Press **Esc**, enter **:wq**, and press **Enter**.

   The system saves the settings and exits the vi editor.

Related Operations

Configure DHCP to enable the ECS to obtain IP addresses continuously.

- For CentOS and EulerOS, use the vi editor to add **PERSISTENT_DHCLIENT="y"** to configuration file **/etc/sysconfig/network-scripts/ifcfg-ethX**.
- For SUSE Linux Enterprise, use the vi editor to set **DHCLIENT_USE_LAST_LEASE** to **no** in the configuration file **/etc/sysconfig/network/dhcp**.

- For Ubuntu 12.04 or later, upgrade dhclient to ISC dhclient 4.2.4 so that the NIC can consistently obtain IP addresses from the DHCP server. To perform the upgrade, you need to install isc-dhcp-server first.

2.3.2 Deleting Files from the Network Rule Directory

Scenarios

To prevent NIC name drift when you use a private image to create ECSs, you need to delete files from the network rule directory of the VM where the ECS or image file is located during the private image creation.

NOTE

When registering an external image file as a private image, delete files from the network rule directory on the VM where the external image file is located. You are advised to delete the files on the VM and then export the image file.

Prerequisites

An OS and VirtIO drivers have been installed on the ECS.

Procedure

1. Run the following command to query files in the network rule directory:

   ls -l /etc/udev/rules.d

2. Run the following commands to delete the files whose names contain **persistent** and **net** from the network rule directory:

   Example:

   rm /etc/udev/rules.d/*30***-net_persistent***-names***.rules**

   rm /etc/udev/rules.d/*70***-persistent-net.rules**

   The italic content in the commands varies depending on your environment.

   NOTE

   For CentOS 6 images, to prevent NIC name drift, you need to create an empty rules configuration file.

   Example:

   touch /etc/udev/rules.d/*75***-persistent-net-generator.rules** //Replace *75* with the actual value in the environment.

3. Delete network rules.
   - If the OS uses the initrd system image, perform the following operations:
     i. Run the following command to check whether the initrd image file whose name starts with **initrd** and ends with **default** contains the **persistent** and **net** network device rule files (replace the italic content in the following command with the actual OS version):

        lsinitrd /boot/initrd-*2.6.32.12-0.7***-default |grep persistent|grep net**

        ○ If no, no further action is required.

        ○ If yes, go to 3.ii.

ii. Run the following command to back up the initrd image files (replace the italic part in the following command with the actual OS version):

cp /boot/initrd-*2.6.32.12-0.7***-default /boot/initrd-***2.6.32.12-0.7-***default_bak**

iii. Run the following command to generate the initrd file again:

mkinitrd

– If the OS uses the initramfs system image (such as Ubuntu), perform the following operations:

i. Run the following command to check whether the initramfs image file whose name starts with **initrd** and ends with **generic** contains persistent and net rule files.

lsinitramfs /boot/initrd.img-3.19.0-25-generic|grep persistent|grep net

- ○ If no, no further action is required.
- ○ If yes, go to 3.ii.

ii. Run the following command to back up the initrd image files:

cp /boot/initrd.img-3.19.0-25-generic /boot/initrd.img-3.19.0-25-generic_bak

iii. Run the following command to generate the initramfs image files again:

update-initramfs -u

2.3.3 (Optional) Installing and Configuring 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.

- 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.
- 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.

NOTE

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

Prerequisites

- An EIP has been bound to the ECS.

- You have logged in to the ECS.
- The ECS uses DHCP to obtain IP addresses.

Procedure

1. Check whether Cloud-Init has been installed.

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

2. Install Cloud-Init.

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

Check Whether Cloud-Init Has Been Installed

Perform the operations provided here to check whether Cloud-Init has been installed. The methods of checking whether Cloud-Init is installed vary depending on the OSs.

- If you are in a Python 3 environment, run the following command to check whether Cloud-Init is installed (Ubuntu 22.0.4 is used as an example):

  which cloud-init

  – If information similar to the following is displayed, Cloud-Init has been installed:

  ```
  /usr/bin/cloud-init
  ```

  – If information similar to the following is displayed, Cloud-Init is not installed:

  ```
  /usr/bin/which: no cloud-init in (/usr/local/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/
  sbin:/usr/bin)
  ```

- If you are in a Python 2 environment, run the following command to check whether Cloud-Init is installed (CentOS 6 is used as an example):

  which cloud-init

  – If information similar to the following is displayed, Cloud-Init has been installed:

  ```
  cloud-init-0.7.5-10.el6.centos.2.x86_64
  ```

  – If no information is returned, Cloud-Init is not installed.

  NOTE

  To confirm Cloud-Init is really not installed, you are advised to run **rpm -qa |grep cloud-init** to check again. If either of **which cloud-init** and **rpm -qa |grep cloud-init** shows that Cloud-Init has been installed, Cloud-Init is installed.

If Cloud-Init has been installed, perform the following operations:

- Determine whether to continue to use the SSH certificate in the OS of this ECS. If no, delete it.

  – If the certificate is stored in a directory of user **root**, for example, */$path/$to/$root/***.ssh/authorized_keys**, run the following commands:

  cd /root/.ssh

  rm authorized_keys

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

    cd /home/centos/.ssh

    rm authorized_keys

- Delete the cache data generated by Cloud-Init to ensure that ECSs created from the private image can be logged in by using an SSH certificate:

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

NOTE

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

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

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

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

- SUSE Linux

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

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

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

  NOTE

  Select the required repo installation package in the provided paths.

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

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

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

     zypper ar https://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/SLE_12_SP3/Cloud:Tools.repo

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

     zypper refresh

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

     zypper install cloud-init

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

     ▪ SUSE 11

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

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

  - SUSE 12 and openSUSE 12/13/42

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

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

⚠ CAUTION

For SUSE and openSUSE, perform the following steps to prevent DHCP from changing the hostname:

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 2-8 lists the Cloud-Init installation paths for CentOS. Select an epel-release installation package matching your OS.

Table 2-8 Cloud-Init installation package addresses

OS Type	Version	How to Obtain
CentOS	6 32-bit	https://archives.fedoraproject.org/pub/archive/epel/6/i386/
	6 64-bit	https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/
	7 64-bit	https://archives.fedoraproject.org/pub/archive/epel/7/x86_64/Packages/e/

a. Run the following commands to install Cloud-Init:

   yum install *Cloud-Init installation package address*/**epel-release-***x-y***.noarch.rpm**

   yum install cloud-init

NOTE

Cloud-Init installation package address indicates the address of the Cloud-Init epel-release installation package, and *x-y* indicates the version of the Cloud-Init epel-release required by the current OS. Replace them with the actual values according to **Table 2-8**.

- Take CentOS 6 64-bit as an example. If the version is 6.8, the command is as follows:

  yum install https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/epel-release-6-8.noarch.rpm

- Take CentOS 7 64-bit as an example. If the version is 7.14, the command is as follows:

  yum install https://archives.fedoraproject.org/pub/archive/epel/7/x86_64/Packages/e/epel-release-7-14.noarch.rpm

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

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

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

- Fedora

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

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

  yum install cloud-init

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

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

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

- Debian and Ubuntu

  Before installing Cloud-Init, ensure that the network installation source address has been configured for the OS by checking whether the **/etc/apt/sources.list** file contains the installation source address of the software package. If the file does not contain the address, configure the address by following the instructions on the Debian or Ubuntu official website.

  a. Run the following commands to install Cloud-Init:

  apt-get update

  apt-get install cloud-init

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

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

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

Cloud-Init-23.2.2 is used as an example to describe how to install Cloud-Init on CentOS, Fedora, Ubuntu, Debian, and SUSE.

Download the **cloud-init-23.2.2.tar.gz** source code package from **https://launchpad.net/cloud-init/trunk/23.2.2/+download/cloud-init-23.2.2.tar.gz**.

- **Centos 7/Fedora Server 36**

NOTICE

Ensure that Python 3 has been installed.

a. Check whether Cloud-Init has been installed. If any command output is displayed, Cloud-Init has been installed.

```
cloud-init -v
```

b. Delete the cache directory of Cloud-Init.

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

c. Install dependency packages of Cloud-Init.

```
yum install python3-pip -y
yum install python3-devel
```

d. Download the Cloud-Init package.

```
wget https://launchpad.net/cloud-init/trunk/23.2.2/+download/cloud-init-23.2.2.tar.gz
```

e. Decompress the Cloud-Init package.

```
tar -zxvf cloud-init-23.2.2.tar.gz
```

f. Go to the **cloud-init-23.2.2** directory and install dependent libraries:

```
cd cloud-init-23.2.2
pip3 install -r requirements.txt
```

g. Install Cloud-Init.

```
python3 setup.py build
python3 setup.py install --init-system systemd
```

h. (Optional) Disable Cloud-Init's network configuration capability by modifying the **/etc/cloud/cloud.cfg** file.

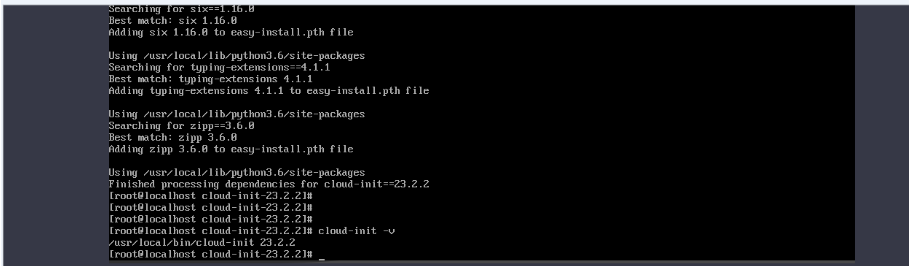
```
vi /etc/cloud/cloud.cfg
```

Add the following content to the file:

```
network:
  config: disabled
```

i. Restart Cloud-Init and check its status.

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



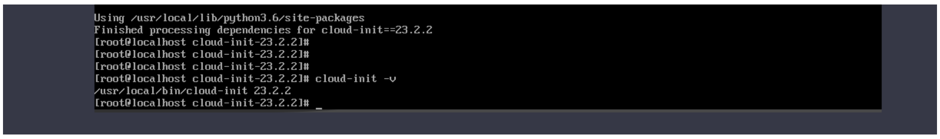
```
Searching for six==1.16.0
Best match: six 1.16.0
Adding six 1.16.0 to easy-install.pth file

Using /usr/local/lib/python3.6/site-packages
Searching for typing-extensions==4.1.1
Best match: typing-extensions 4.1.1
Adding typing-extensions 4.1.1 to easy-install.pth file

Using /usr/local/lib/python3.6/site-packages
Searching for zipp==3.6.0
Best match: zipp 3.6.0
Adding zipp 3.6.0 to easy-install.pth file

Using /usr/local/lib/python3.6/site-packages
Finished processing dependencies for cloud-init==23.2.2
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]# cloud-init -v
/usr/local/bin/cloud-init 23.2.2
[root@localhost cloud-init-23.2.2]# _
```

j. Enable Cloud-Init related services to automatically start upon system boot.

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

k. Check whether Cloud-Init is running properly.

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



```
Using /usr/local/lib/python3.6/site-packages
Finished processing dependencies for cloud-init==23.2.2
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]# cloud-init -v
/usr/local/bin/cloud-init 23.2.2
[root@localhost cloud-init-23.2.2]# _
```

- **Ubuntu 22.0.4/Debian 11**

NOTICE

Ensure that Python 3 has been installed.

a. Check and delete redundant Cloud-Init configuration files.

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

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

b. Update your package list and check whether Wget is installed. If it is not, install it.

```
sudo apt update
sudo apt install wget
```

c. Install dependency packages.

```
apt-get install cloud-guest-utils -y
apt-get install python3-pip -y
apt-get install python3-devel
```

d. Download the Cloud-Init package.

```
wget https://launchpad.net/cloud-init/trunk/23.2.2/+download/cloud-init-23.2.2.tar.gz
```

e. Decompress the Cloud-Init package.

```
tar -zxvf cloud-init-23.2.2.tar.gz
```

f. Go to the **cloud-init** directory.

```
cd cloud-init-23.2.2
```

g. Install dependent libraries.

```
pip3 install -r requirements.txt
```

h. Install Cloud-Init.

```
python3 setup.py install
```

i. (Optional) Disable Cloud-Init's network configuration capability.

You need to do so when the Cloud-Init version is 0.7.9 or later and you want to configure the network.

NOTE

1. Open the **/etc/cloud/cloud.cfg** file.

```
vi /etc/cloud/cloud.cfg
```

2. Enter **i** and configure **network**. (If there is no such a configuration item, add it.)

```
network:
  config: disabled
```

j. Restart Cloud-Init and check its status.

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

k. Enable Cloud-Init related services to automatically start upon system boot.

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

l. Check whether Cloud-Init is running properly.

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

- **SUSE Enterprise Linux Server 15**

  NOTICE

  Ensure that Python 3 has been installed.

a. View existing SUSE repositories.

```
zypper lr
```

b. Delete the SUSE repositories.

zypper rr *No. of repositories listed in* ***1***

c. Configure a SUSE repository.

zypper ar **https://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/SLE_15_SP4/Cloud:Tools.repo**

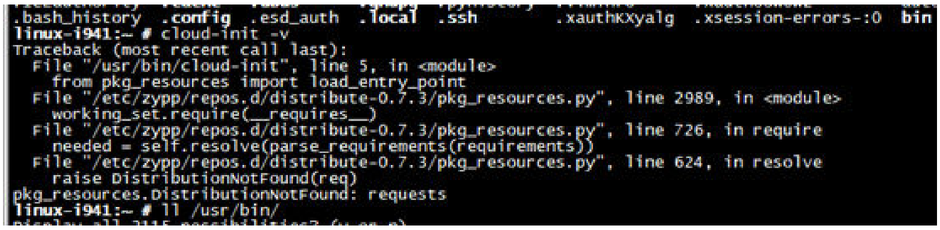
d. Refresh the SUSE repository.

```
zypper refresh
```

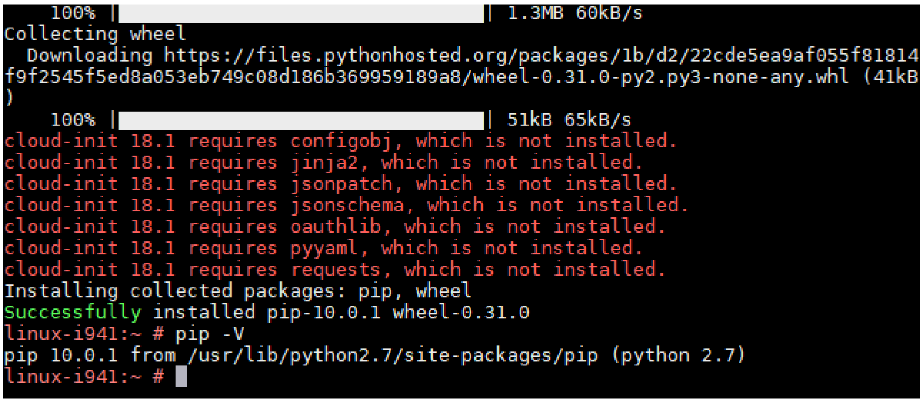
e. Install Cloud-Init.

```
zypper install cloud-init
```

f. Run **cloud-init -v**. If error messages similar to the following are displayed, install the dependency packages.



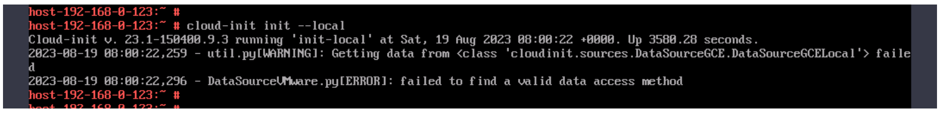
```
.bash_history  .config  .esd_auth  .local  .ssh        .xauthKXyalg  .xsession-errors-:0  bin
linux-i941:~ # cloud-init -v
Traceback (most recent call last):
  File "/usr/bin/cloud-init", line 5, in <module>
    from pkg_resources import load_entry_point
  File "/etc/zypp/repos.d/distribute-0.7.3/pkg_resources.py", line 2989, in <module>
    working_set.require(__requires__)
  File "/etc/zypp/repos.d/distribute-0.7.3/pkg_resources.py", line 726, in require
    needed = self.resolve(parse_requirements(requirements))
  File "/etc/zypp/repos.d/distribute-0.7.3/pkg_resources.py", line 624, in resolve
    raise DistributionNotFound(req)
pkg_resources.DistributionNotFound: requests
linux-i941:~ # ll /usr/bin/
```



```
    100% |████████████████████████████████| 1.3MB 60kB/s
Collecting wheel
  Downloading https://files.pythonhosted.org/packages/1b/d2/22cde5ea9af055f81814
f9f2545f5ed8a053eb749c08d186b369959189a8/wheel-0.31.0-py2.py3-none-any.whl (41kB
)
    100% |████████████████████████████████| 51kB 65kB/s
cloud-init 18.1 requires configobj, which is not installed.
cloud-init 18.1 requires jinja2, which is not installed.
cloud-init 18.1 requires jsonpatch, which is not installed.
cloud-init 18.1 requires jsonschema, which is not installed.
cloud-init 18.1 requires oauthlib, which is not installed.
cloud-init 18.1 requires pyyaml, which is not installed.
cloud-init 18.1 requires requests, which is not installed.
Installing collected packages: pip, wheel
Successfully installed pip-10.0.1 wheel-0.31.0
linux-i941:~ # pip -V
pip 10.0.1 from /usr/lib/python2.7/site-packages/pip (python 2.7)
linux-i941:~ #
```

```
pip install requests pyyaml oauthlib jsonschema jsonpatch jinja2 configobj
```

g. Check whether Cloud-Init is successfully installed. If the following error message is displayed, configure **datasource_list** in **/etc/cloud/cloud.cfg**.



```
host-192-168-0-123:~ #
host-192-168-0-123:~ # cloud-init init --local
Cloud-init v. 23.1-150400.9.3 running 'init-local' at Sat, 19 Aug 2023 08:00:22 +0000. Up 3580.28 seconds.
2023-08-19 08:00:22,259 - util.py[WARNING]: Getting data from <class 'cloudinit.sources.DataSourceGCE.DataSourceGCELocal'> faile
d
2023-08-19 08:00:22,296 - DataSourceVMware.py[ERROR]: failed to find a valid data access method
host-192-168-0-123:~ #
```

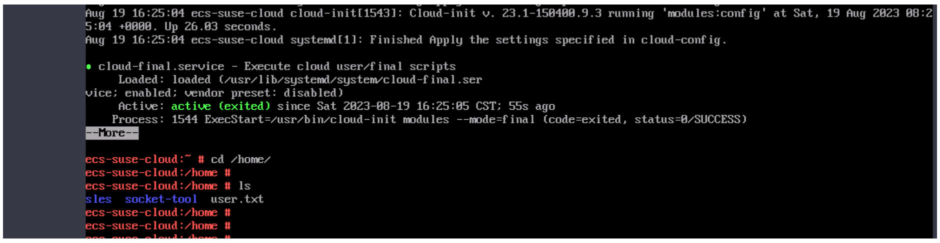
```
datasource_list: [ OpenStack ]
datasource:
  OpenStack:
    metadata_urls: ['http://169.254.169.254']
    max_wait: 120
    timeout: 5
    apply_network_config: false
```

h. Modify the configuration file, restart Cloud-Init, and check the Cloud-Init status.

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

i. Enable Cloud-Init related services to automatically start upon system boot.

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



```
Aug 19 16:25:04 ecs-suse-cloud cloud-init[1543]: Cloud-init v. 23.1-150400.9.3 running 'modules:config' at Sat, 19 Aug 2023 08:2
5:04 +0000. Up 26.03 seconds.
Aug 19 16:25:04 ecs-suse-cloud systemd[1]: Finished Apply the settings specified in cloud-config.

● cloud-final.service - Execute cloud user/final scripts
     Loaded: loaded (/usr/lib/systemd/system/cloud-final.ser
vice; enabled; vendor preset: disabled)
     Active: active (exited) since Sat 2023-08-19 16:25:05 CST; 55s ago
    Process: 1544 ExecStart=/usr/bin/cloud-init modules --mode=final (code=exited, status=0/SUCCESS)
--More--

ecs-suse-cloud:~ # cd /home/
ecs-suse-cloud:/home #
ecs-suse-cloud:/home # ls
sles  socket-tool  user.txt
ecs-suse-cloud:/home #
ecs-suse-cloud:/home #
```

j. Check whether Cloud-Init is running properly.

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

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

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

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

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

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

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

   NOTE

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

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

   NOTE

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

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

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

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

NOTE

For details about how to install a Cloud-Init source code package, see **Cloud-Init Documentation**

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

```
cloud-init 0.7.9
```

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

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

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

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

   - If the OS uses Systemd to manage automatic start of services, run the following commands:

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

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

CAUTION

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

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

   useradd syslog

   groupadd adm

   usermod -g adm syslog

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

Install Cloud-Init Using the Official GitHub Source Code

You can obtain the Cloud-Init source code from GitHub at **https://github.com/canonical/cloud-init/**

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

NOTE

Cloud-Init 0.7.6: **https://github.com/canonical/cloud-init/archive/refs/tags/0.7.6.zip**

Cloud-Init 0.7.9: **https://github.com/canonical/cloud-init/archive/refs/tags/0.7.9.zip**

All versions: **https://github.com/canonical/cloud-init/releases**

wget https://github.com/canonical/cloud-init/archive/refs/tags/0.7.6.zip

mkdir /tmp/CLOUD-INIT

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

cd /tmp/CLOUD-INIT

2. Run the following command to decompress the package:

   unzip cloud-init-0.7.6.zip

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

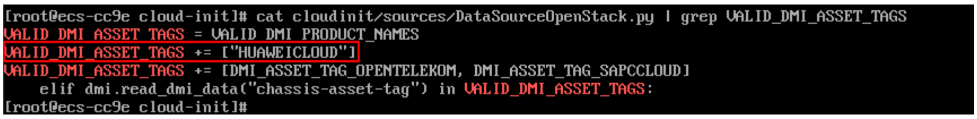
   cd cloud-init-0.7.6

4. (Optional) If the Cloud-Init version is 18.3 to 22.3, run the following commands:

   sed -i '/VALID_DMI_ASSET_TAGS =/a\VALID_DMI_ASSET_TAGS += ["HUAWEICLOUD"]' cloudinit/sources/DataSourceOpenStack.py

   cat cloudinit/sources/DataSourceOpenStack.py | grep VALID_DMI_ASSET_TAGS

   If the following information is displayed, the execution is successful.

```
[root@ecs-cc9e cloud-init]# cat cloudinit/sources/DataSourceOpenStack.py | grep VALID_DMI_ASSET_TAGS
VALID_DMI_ASSET_TAGS = VALID_DMI_PRODUCT_NAMES
VALID_DMI_ASSET_TAGS += ["HUAWEICLOUD"]
VALID_DMI_ASSET_TAGS += [DMI_ASSET_TAG_OPENTELEKOM, DMI_ASSET_TAG_SAPCCLOUD]
    elif dmi.read_dmi_data("chassis-asset-tag") in VALID_DMI_ASSET_TAGS:
[root@ecs-cc9e cloud-init]#
```

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

     python setup.py build

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

     python setup.py build

     python setup.py install --init-system systemd

   NOTE

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

   useradd syslog

   groupadd adm

   usermod -g adm syslog

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

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

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

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

– If the OS uses Systemd to manage automatic start of services, run the following commands:

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

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

7. Run the following commands to check whether Cloud-Init has been installed:

cloud-init -v

cloud-init init --local

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

```
cloud-init 0.7.6
```

Configure Cloud-Init

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

Take CentOS 6.7 as an example. If the value of **disable_root** in the **/etc/cloud/cloud.cfg** file is **0**, the permissions are enabled. (In some OSs, value **true** indicates that the permissions are disabled, and **false** indicates that the permissions are enabled). Set **ssh_pwauth** to **1**, and **lock_passwd** to **False** (indicating that user passwords are not locked).

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

disable_root: 0
ssh_pwauth: 1
```

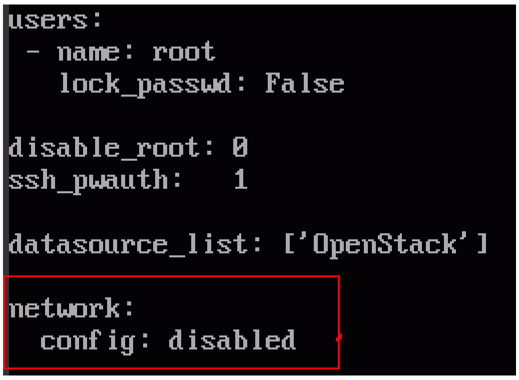
NOTE

- If you inject a password, use it for remote login through SSH or noVNC.
- If you inject a key, use it for remote login through SSH.

2. Modify the **/etc/cloud/cloud.cfg** file to disable Cloud-Init's network configuration capability.

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

Figure 2-26 Disabling Cloud-Init's network configuration capability



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

disable_root: 0
ssh_pwauth:   1

datasource_list: ['OpenStack']

network:
  config: disabled
```

NOTE

The added content must be in the YAML format.

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

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

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

NOTE

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

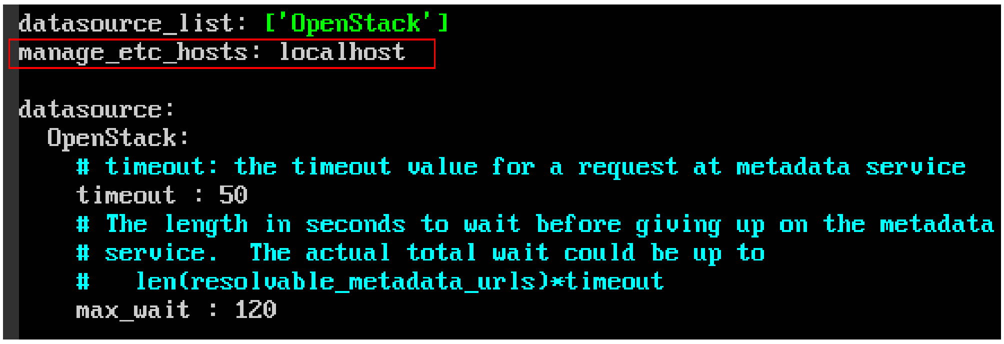
  echo "NOZEROCONF=yes" >> /etc/sysconfig/network
- **apply_network_config: false** is only requited by users who use Cloud-Init 18.3 or later.

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

   manage_etc_hosts: localhost

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

Figure 2-27 Adding **manage_etc_hosts: localhost**



```
datasource_list: ['OpenStack']
manage_etc_hosts: localhost

datasource:
  OpenStack:
    # timeout: the timeout value for a request at metadata service
    timeout : 50
    # The length in seconds to wait before giving up on the metadata
    # service.  The actual total wait could be up to
    #   len(resolvable_metadata_urls)*timeout
    max_wait : 120
```

5. Run the **vi /etc/ssh/sshd_config** command to open the **/etc/ssh/sshd_config** file using the vi editor.

   Change the value of **PasswordAuthentication** in the **sshd_config** file to **yes**.

NOTE

For SUSE and openSUSE, change the values of the following parameters in the **sshd_config** file to **yes**:

- PasswordAuthentication
- ChallengeResponseAuthentication

6. Modify **cloud_init_modules** in the **cloud.cfg** configuration file.

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

   - Enable the hostname update. Do not comment out or delete the **- update_hostname** statement.

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

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

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

      vi /usr/lib/python*.*/site-packages/cloudinit/sources/__init__.py

      The Python version varies depending on the OS.

      Press **i** to enter editing mode. Modify the file content as follows based on the keyword **toks**:

      ```
      if toks:
          toks = str(toks).split('.')
      else:
          #toks = ["ip-%s" % lhost.replace(".", "-")] # Comment out this line.
          toks = lhost.split(".novalocal")    # Add this line.

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

      if fqdn and domain != defdomain:
           return hostname
          #return "%s.%s" % (hostname, domain) # Comment out this line.
      else:
          return hostname
      ```

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

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

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

      The Python version varies depending on the OS.

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

      rm -rf __init__.pyc

      rm -rf __init__.pyo

   d. Run the following commands to clear the logs:

      rm -rf /var/lib/cloud/*

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

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

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

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

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

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

   userdel linux

   rm -fr /home/linux

10. Ensure that Cloud-Init is enabled.

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

Check the Cloud-Init Configuration

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**.

2.3.4 Installing the One-Click Password Reset Plug-In

Scenarios

You are advised to install the password reset plug-in CloudResetPwdAgent before creating a private image. In this way, you can reset the password of ECSs created from the image by a few clicks.

- ECSs created from a public image have this plug-in installed by default.
- For ECSs created from an external image file, install the plug-in by performing the operations in this section.

Precautions

- You can decide whether to install the CloudResetPwdAgent plug-in.
- The plug-in has been open-sourced in the GitHub open-source platform according to *GNU General Public License v2.0*.
- Not all OSs support the one-click password reset plug-in. **Table 2-9** lists the OSs that support this plug-in.

Table 2-9 OSs that support the one-click password reset plug-in

OS Type	OS Version
CentOS	CentOS 8.3 64bit CentOS 8.2 64bit CentOS 8.1 64bit CentOS 8.0 64bit CentOS 7.3 64bit CentOS 7.2 64bit CentOS 7.0 64bit CentOS 7.1 64bit CentOS 6.9 64bit CentOS 6.8 64bit CentOS 6.8 32bit CentOS 6.6 32bit CentOS 6.6 64bit CentOS 6.5 64bit CentOS 6.4 64bit CentOS 6.3 64bit **NOTE** For CentOS 8, disable SELinux before you install the one-click password reset plug-in. After the plug-in is installed, you can determine whether to enable SELinux as needed.
Debian	Debian 9.0 64bit Debian 8.8 64bit Debian 8.2 64bit Debian 7.5 64bit Debian 7.5 32bit
openSUSE	openSUSE 42.2 64bit openSUSE 13.2 64bit openSUSE Leap 42.2 64bit openSUSE Leap 42.1 64bit
SUSE	SUSE 12 SP2 64bit SUSE 12 SP1 64bit SUSE 11 SP4 64bit
Ubuntu	Ubuntu 16.10 32bit Ubuntu 16.04 32bit Ubuntu Server 16.04 64bit Ubuntu Server 14.04 64bit Ubuntu Server 14.04 32bit

OS Type	OS Version
EulerOS	EulerOS 2.2 64bit
Fedora	Fedora 25 64bit Fedora 24 64bit
Oracle Linux	Oracle Linux 7.3 64bit Oracle Linux 6.9 64bit Oracle Linux 6.5 64bit
Rocky Linux	Rocky Linux 9.5 64bit Rocky Linux 9.4 64bit Rocky Linux 9.3 64bit Rocky Linux 9.2 64bit Rocky Linux 9.0 64bit Rocky Linux 8.8 64bit Rocky Linux 8.5 64bit Rocky Linux 8.4 64bit

Prerequisites

- The ECS status is **Running**.
- The ECS must have a remaining space of more than 300 MB, and data can be written to its root directory.
- SELinux affects the password reset plug-in of Linux ECSs. Disable SELinux by referring to **Disabling SELinux**.
- ECSs created using a SUSE 11 SP4 image must have 4 GB or a larger memory.
- DHCP must be enabled for the VPC used by the ECS.
- Networks of the ECS are normal.
- The outbound security group rule of the ECS must meet the following requirements:
  - **Protocol**: **TCP**
  - **Port Range**: **80**
  - **Remote End**: **169.254.0.0/16**

  If you use the default outbound security group rule, preceding requirements can be met, and the ECS can be initialized. The default outbound security group rule is as follows:
  - **Protocol**: **All**
  - **Port Range**: **All**
  - **Remote End**: **0.0.0.0/16**

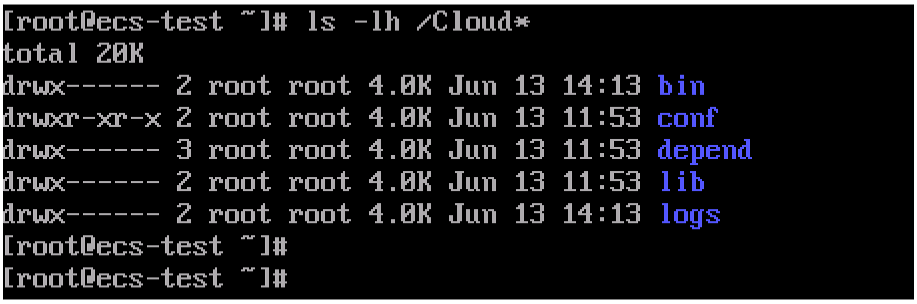
Procedure

Step 1 Check whether the one-click password reset plug-in has been installed on the ECS.

1. Log in to the ECS as user **root**.
2. Run the following command to check whether CloudResetPwdAgent has been installed:

   ls -lh /Cloud*

   Figure 2-28 Checking whether the plug-in has been installed

   ```
   [root@ecs-test ~]# ls -lh /Cloud*
   total 20K
   drwx------ 2 root root 4.0K Jun 13 14:13 bin
   drwxr-xr-x 2 root root 4.0K Jun 13 11:53 conf
   drwx------ 3 root root 4.0K Jun 13 11:53 depend
   drwx------ 2 root root 4.0K Jun 13 11:53 lib
   drwx------ 2 root root 4.0K Jun 13 14:13 logs
   [root@ecs-test ~]#
   [root@ecs-test ~]#
   ```

   Check whether the obtained information is similar to that shown in **Figure 2-28**.

   – If yes, the plug-in has been installed.

   – If no, the plug-in has not been installed. Then, install it.

Step 2 Download **CloudResetPwdAgent.zip** and verify its integrity by referring to **Obtaining the One-Click Password Reset Plug-in (Linux)**.

There is no special requirement for the directory that stores **CloudResetPwdAgent.zip**.

Step 3 Run the following command to decompress **CloudResetPwdAgent.zip**:

There is no special requirement for the directory that stores the decompressed **CloudResetPwdAgent.zip**. Use any directory.

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

For example:

If the plug-in is decompressed to **/home/linux/test**, run the following command:

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

Step 4 Install the one-click password reset plug-in.

1. Run the following command to open the **CloudResetPwdAgent.Linux** file:

   cd CloudResetPwdAgent/CloudResetPwdAgent.Linux

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

   chmod +x setup.sh

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

   sudo sh setup.sh

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

NOTE

- You can also check whether the plug-in has been installed using the methods provided in **Step 1**.
- If the installation failed, check whether the installation environment meets the requirements and install the plug-in again.

Step 5 Modify the file permissions of the password reset plug-in.

chmod 700 /CloudrResetPwdAgent/bin/cloudResetPwdAgent.script

chmod 700 /CloudrResetPwdAgent/bin/wrapper

chmod 600 /CloudrResetPwdAgent/lib/*

----End

2.3.5 Detaching Data Disks from an ECS

Scenarios

If multiple data disks are attached to the ECS used to create a private image, ECSs created from the image may be unavailable. Therefore, you need to detach all data disks from the ECS before using it to create a private image.

This section describes how to detach all data disks from an ECS.

Prerequisites

You have logged in to the ECS used to create a Linux private image.

Procedure

1. Check whether the ECS has data disks.

   Run the following command to check the number of disks attached to the ECS:

   fdisk -l

   – If the number is greater than 1, the ECS has data disks. Go to **2**.

   – If the number is equal to 1, no data disk is attached to the ECS. Go to **3**.

2. Run the following command to check the data disks attached to the ECS:

   mount

   – If the command output does not contain any EVS disk information, no EVS data disks need to be detached.
   ```
   /dev/vda1 on / type ext4 (rw,relatime,data=ordered)
   ```

   – If information similar to the following is displayed, go to **3**:
   ```
   /dev/vda1 on / type ext4 (rw,relatime,data=ordered)
   /dev/vdb1 on /mnt/test type ext4 (rw,relatime,data=ordered)
   ```

3. Delete the configuration information in the **fstab** file.

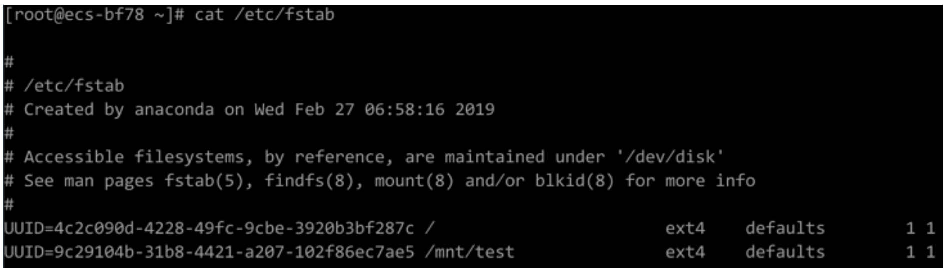
   a. Run the following command to edit the **fstab** file:

      vi /etc/fstab

   b. Delete the disk configuration from the **fstab** file.

The **/etc/fstab** file contains information about the file systems and storage devices automatically attached to the ECS when the ECS starts. The configuration about data disks automatically attached to the ECS needs to be deleted, for example, the last line shown in the following figure.

Figure 2-29 EVS disk configuration in the **fstab** file



```
[root@ecs-bf78 ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Wed Feb 27 06:58:16 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=4c2c090d-4228-49fc-9cbe-3920b3bf287c /                       ext4    defaults        1 1
UUID=9c29104b-31b8-4421-a207-102f86ec7ae5 /mnt/test               ext4    defaults        1 1
```

4. Run the following command to detach data disks from the ECS:

   Run the following command to detach the disks:

   umount */dev/vdb1*

5. Run the following command to check the data disks attached to the ECS:

   mount

   If the command output contains no information about the data disks, they have been detached from the ECS.

2.3.6 Changing Disk Identifiers in the GRUB File to UUID

Scenarios

Before using an ECS to create a private image, you need to change disk identifiers to UUID in the GRUB file of the ECS.

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

NOTE

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

Procedure

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

  a. Log in to the ECS as user **root**.

  b. Run the following command to query all types of mounted file systems and device UUIDs:

     blkid

     The following information is displayed:

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

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

cat /boot/grub/grub.cfg

The following information is displayed:

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

d. Check whether the root partition in the **/boot/grub/grub.cfg** configuration file contains **root=/dev/xvda1** or **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34**.

- If **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34** is contained, the root partition is in UUID format and requires no change.

- If **root=/dev/xvda1** is contained, the root partition is in the device name format. Go to 5.

e. Identify the UUID of the root partition device based on **root=/dev/xvda1** (device name of the root partition) and the partition information obtained by running the **blkid** command.

f. Run the following command to open the **grub.cfg** file:

vi /boot/grub/grub.cfg

g. Press **i** to enter editing mode and change the root partition to the UUID format, for example, from **root=/dev/xvda1** to **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34**.

h. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the configuration and exits the vi editor.

i. Run the following command to verify the change:

cat /boot/grub/grub.cfg

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

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

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

  a. Log in to the ECS as user **root**.

  b. Run the following command to query all types of mounted file systems and device UUIDs:

     blkid

     The following information is displayed:

     ```
     /dev/xvda1: UUID="749d6c0c-990a-4661-bed1-46769388365a" TYPE="swap"
     /dev/xvda2: UUID="f382872b-eda6-43df-9516-5a687fecdce6" TYPE="ext4"
     ```

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

     cat /boot/grub/grub.conf

     The following information is displayed:

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

  d. Check whether the root partition in the **/boot/grub/grub.conf** configuration file contains **root=/dev/xvda2** or **root=UUID=f382872b-eda6-43df-9516-5a687fecdce6**.

     - If **root=UUID=f382872b-eda6-43df-9516-5a687fecdce6** is contained, the root partition is in UUID format and requires no change.

     - If **root=/dev/xvda2** is contained, the root partition is in the device name format. Go to 5.

  e. Identify the UUID of the root partition device based on **root=/dev/xvda2** (device name of the root partition) and the partition information obtained by running the **blkid** command.

  f. Run the following command to open the **grub.conf** file:

     vi /boot/grub/grub.conf

  g. Press **i** to enter editing mode and change the root partition to the UUID format, for example, from **root=/dev/xvda2** to **root=UUID=f382872b-eda6-43df-9516-5a687fecdce6**.

h. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the configuration and exits the vi editor.

i. Run the following command to verify the change:

   cat /boot/grub/grub.conf

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

```
default=0
timeout=5
splashimage=(hd0,1)/boot/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.32-573.8.1.el6.x86_64)
root (hd0,1)
kernel /boot/vmlinuz-2.6.32-573.8.1.el6.x86_64 ro root=UUID=f382872b-
eda6-43df-9516-5a687fecdce6 rd_NO_LUKS rd_NO_LVM LANG=en_US.UTF-8 rd_NO_MD
SYSFONT=latarcyrheb-sun16 crashkernel=autoKEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM
rhgb quiet
initrd /boot/initramfs-2.6.32-573.8.1.el6.x86_64.img
```

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

a. Log in to the ECS as user **root**.

b. Run the following command to query all types of mounted file systems and device UUIDs:

   blkid

   The following information is displayed:

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

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

   cat /boot/grub2/grub.cfg

   The following information is displayed:

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

d. Check whether the root partition in the **/boot/grub2/grub.cfg** configuration file contains **root=/dev/xvda2** or **root=UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130**.

    - If **root=UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130** is contained, the root partition is in UUID format and requires no change.
    - If **root=/dev/xvda2** is contained, the root partition is in the device name format. Go to 5.

e. Identify the UUID of the root partition device based on **root=/dev/xvda2** (device name of the root partition) and the partition information obtained by running the **blkid** command.

f. Run the following command to open the **grub.cfg** file:

   vi /boot/grub2/grub.cfg

g. Press **i** to enter editing mode and change the root partition to the UUID format, for example, from **root=/dev/xvda2** to **root=UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130**.

h. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the configuration and exits the vi editor.

i. Run the following command to verify the change:

   cat /boot/grub2/grub.cfg

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

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

2.3.7 Changing Disk Identifiers in the fstab File to UUID

Scenarios

Before using an ECS to create a private image, you need to change disk identifiers to UUID in the fstab file of the ECS.

Procedure

- Take CentOS 7.0 as an example. Run **blkid** to obtain the UUIDs of all partitions. Modify the **/etc/fstab** file and use the partition UUIDs to configure automatic partition mounting.

1. Log in to the ECS as user **root**.

2. Run the following command to query all types of mounted file systems and device UUIDs:

   blkid

   The following information is displayed:

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

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

   cat /etc/fstab

   The following information is displayed:

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

4. Check whether the disk identifier in the **fstab** file is the device name.
   - If the disk is represented by a UUID, no further operation is required.
   - If the disk is represented by the device name, go to **5**.
5. Run the following command to open the **fstab** file:

   vi /etc/fstab

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

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

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

   blkid

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

   Before the change:

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

   After the change:

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

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

   cat /etc/fstab

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

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

2.3.8 Using a Script to Optimize a Xen Private Image

1. Use the Linux image to be optimized to create an ECS, and start and log in to the ECS.

2. Run the following command to download the driver installation script to the **root** directory:

   curl *URL* **> ~/resize_ecs_modify_linux.sh**

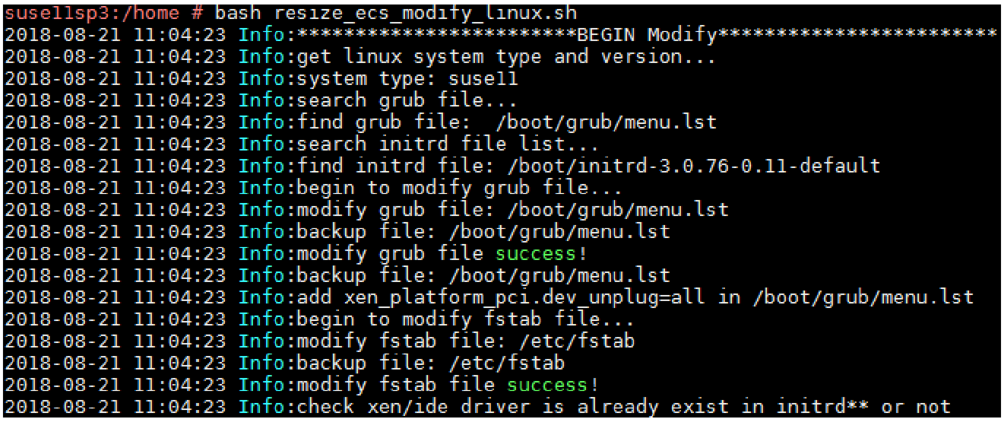
   URL indicates the script download address.

   https://latin-server-resize.obs.na-mexico-1.myhuaweicloud.com/resize_ecs_modify_linux.sh

3. Run the following command to execute the script:

   bash resize_ecs_modify_linux.sh

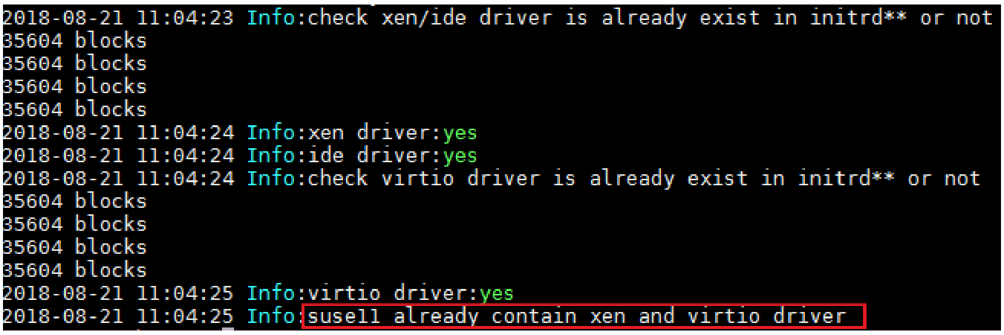
   Figure 2-30 Executing the script



```
susellsp3:/home # bash resize_ecs_modify_linux.sh
2018-08-21 11:04:23 Info:**************************BEGIN Modify**************************
2018-08-21 11:04:23 Info:get linux system type and version...
2018-08-21 11:04:23 Info:system type: susell
2018-08-21 11:04:23 Info:search grub file...
2018-08-21 11:04:23 Info:find grub file:  /boot/grub/menu.lst
2018-08-21 11:04:23 Info:search initrd file list...
2018-08-21 11:04:23 Info:find initrd file: /boot/initrd-3.0.76-0.11-default
2018-08-21 11:04:23 Info:begin to modify grub file...
2018-08-21 11:04:23 Info:modify grub file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:backup file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:modify grub file success!
2018-08-21 11:04:23 Info:backup file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:add xen_platform_pci.dev_unplug=all in /boot/grub/menu.lst
2018-08-21 11:04:23 Info:begin to modify fstab file...
2018-08-21 11:04:23 Info:modify fstab file: /etc/fstab
2018-08-21 11:04:23 Info:backup file: /etc/fstab
2018-08-21 11:04:23 Info:modify fstab file success!
2018-08-21 11:04:23 Info:check xen/ide driver is already exist in initrd** or not
```

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

   Figure 2-31 Successful script execution



```
2018-08-21 11:04:23 Info:check xen/ide driver is already exist in initrd** or not
35604 blocks
35604 blocks
35604 blocks
35604 blocks
2018-08-21 11:04:24 Info:xen driver:yes
2018-08-21 11:04:24 Info:ide driver:yes
2018-08-21 11:04:24 Info:check virtio driver is already exist in initrd** or not
35604 blocks
35604 blocks
35604 blocks
35604 blocks
2018-08-21 11:04:25 Info:virtio driver:yes
2018-08-21 11:04:25 Info:susell already contain xen and virtio driver
```

2.3.9 Installing Native Xen and KVM Drivers on a Xen ECS

Scenarios

Before using a Xen ECS to create a private image, you need to install native Xen and KVM drivers on the ECS.

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

NOTE

Alternatively, you can use a script to automate the installation. For details, see **Using a Script to Optimize a Xen Private Image**.

⚠ CAUTION

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

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

Prerequisites

- The virtualization type of the ECS is Xen.

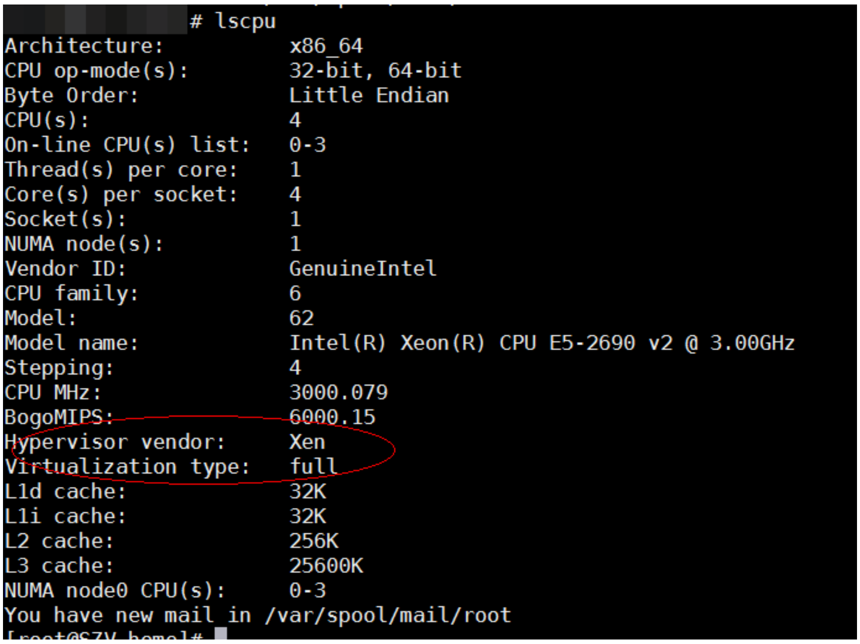
  You can run the following command to check the virtualization type of an ECS:

  lscpu

  – If the value of **Hypervisor vendor** is **Xen**, install drivers as instructed in this section.

  – If the value of **Hypervisor vendor** is **KVM**, install drivers as instructed in **Installing Native KVM Drivers on a KVM ECS**.

Figure 2-32 Checking the virtualization type of a Linux ECS



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

- The ECS kernel version must be later than 2.6.24.
- Disable your antivirus and intrusion detection software. You can enable them after the driver installation is complete.
- Operations in **Changing Disk Identifiers in the GRUB File to UUID** and **Changing Disk Identifiers in the fstab File to UUID** have been completed.

Uninstall PV Drivers

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

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

   ps -ef | grep uvp-monitor

   – If the following information is displayed, PV drivers have been installed.

   – Otherwise, PV drivers are not installed. No further actions will be required.

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

3. In the VNC login window, open the CLI.

   For how to open the CLI, see the OS manual.

4. Run the following command to uninstall PV drivers:

   /etc/.uvp-monitor/uninstall

   – PV drivers are uninstalled successfully if the following command output is displayed:

   ```
   The PV driver is uninstalled successfully. Reboot the system for the uninstallation to take effect.
   ```

   – If the command output indicates that **.uvp-monitor** is not found, go to **5**.

   ```
   -bash: /etc/.uvp-monitor/uninstall: No such file or directory
   ```

5. Perform the following operations to delete uvp-monitor that failed to take effect for KVM, preventing log overflow:

   a. Run the following command to check whether UVP user-mode programs are installed in the OS:

      rpm -qa | grep uvp

      Information similar to the following is displayed:

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

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

      rpm -e kmod-uvpmod

      rpm -e uvp-monitor

      rpm -e libxenstore_uvp

Procedure

Modify the configuration file depending on the OS.

- CentOS, EulerOS

  Take CentOS 7.0 as an example. Modify the **/etc/dracut.conf** file. Add Xen PV and VirtIO drivers to **add_drivers**. Xen PV drivers include xen-blkfront and xen-netfront. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Save and exit the **/etc/dracut.conf** file. Run the **dracut -f** command to regenerate initrd.

  For details, see **CentOS and EulerOS**.

- Ubuntu and Debian

  Modify the **/etc/initramfs-tools/modules** file. Add Xen PV and VirtIO drivers. Xen PV drivers include xen-blkfront and xen-netfront. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Save and exit the **/etc/initramfs-tools/modules** file. Run the **update-initramfs -u** command to regenerate initrd.

For details, see **Ubuntu and Debian**.

- SUSE and openSUSE
  - If the OS version is earlier than SUSE 12 SP1 or openSUSE 13, modify the **/etc/sysconfig/kernel** file and add Xen PV and VirtIO drivers to **INITRD_MODULES=""**. Xen PV drivers include xen_vnif, xen_vbd, and xen_platform_pci. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Run the **mkinitrd** command to regenerate initrd.
  - If the OS version is SUSE 12 SP1, modify the **/etc/dracut.conf** file and add Xen PV and VirtIO drivers to **add_drivers**. Xen PV drivers include xen_vnif, xen_vbd, and xen_platform_pci. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Run the **dracut -f** command to regenerate initrd.
  - If the OS version is later than SUSE 12 SP1 or openSUSE 13, modify the **/etc/dracut.conf** file and add Xen PV and VirtIO drivers to **add_drivers**. Xen PV drivers include xen-blkfront and xen-netfront. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Save and exit the **/etc/dracut.conf** file. Run the **dracut -f** command to regenerate initrd.

For details, see **SUSE and openSUSE**.

NOTE

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

rpm -qa |grep xen-kmp

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

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

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

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

CentOS and EulerOS

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

   vi /etc/dracut.conf

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

```
[root@CTU10000xxxxx ~]# vi /etc/dracut.conf
# additional kernel modules to the default
add_drivers+="xen-blkfront xen-netfront virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring
virtio"
......
```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

4. Run the following command to regenerate initrd:

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

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

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

   lsinitrd /boot/initramfs-\`uname -r\`.img | grep xen

   lsinitrd /boot/initramfs-\`uname -r\`.img | grep virtio

   If the virtual file system is initrd, run the following commands:

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

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

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

```
[root@CTU10000xxxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep xen
-rwxr--r--   1 root     root        54888 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
block/xen-blkfront.ko
-rwxr--r--   1 root     root        45664 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/
drivers/net/xen-netfront.ko

[root@CTU10000xxxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep virtio
-rwxr--r--   1 root     root        23448 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
block/virtio_blk.ko
-rwxr--r--   1 root     root        50704 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/
drivers/net/virtio_net.ko
-rwxr--r--   1 root     root        28424 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
scsi/virtio_scsi.ko
drwxr-xr-x   2 root     root            0 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio
-rwxr--r--   1 root     root        14544 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio.ko
-rwxr--r--   1 root     root        21040 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_pci.ko
-rwxr--r--   1 root     root        18016 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_ring.ko
```

   NOTE

   If you add built-in drivers to the initrd or initramfs file, the ECS will not be affected but such drivers cannot be shown by running the **lsinitrd** command. You can run the following commands to check whether there are built-in drivers in the kernel:

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

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

Ubuntu and Debian

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

   vi /etc/initramfs-tools/modules

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

```
[root@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**. The system saves the change and exits the **/etc/initramfs-tools/modules** file.
4. Run the following command to regenerate initrd:

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

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

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

```
[root@ 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 by mistake, the ECS will not be affected. The drivers cannot be found by running the **lsinitrd** command. You can run the following commands to check whether built-in drivers are in the kernel:

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

SUSE and openSUSE

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

If the OS version is SUSE 12 SP1, modify the **/etc/dracut.conf** file to install the drivers. For details, see **scenario 2**.

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

- Earlier than SUSE 12 SP1 or openSUSE 13:

  NOTE

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

  rpm -qa |grep xen-kmp

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

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

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

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

     vi /etc/sysconfig/kernel

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

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

c. Run the **mkinitrd** command to regenerate initrd.

NOTE

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

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

```
default 0
timeout 10
gfxmenu (hd0,0)/boot/message
title sles11sp4_001_[_VMX_]
root (hd0,0)
kernel /boot/linux.vmx vga=0x314 splash=silent console=ttyS0,115200n8 console=tty0
net.ifnames=0 NON_PERSISTENT_DEVICE_NAMES=1 showopts
initrd /boot/initrd.vmx
title Failsafe_sles11sp4_001_[_VMX_]
root (hd0,0)
kernel /boot/linux.vmx vga=0x314 splash=silent ide=nodma apm=off noresume edd=off
powersaved=off nohz=off highres=off processor.max+cstate=1 nomodeset x11failsafe
console=ttyS0,115200n8 console=tty0 net.ifnames=0 NON_PERSISTENT_DEVICE_NAMES=1
showopts
initrd /boot/initrd.vmx
```

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

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

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

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

```
SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rwxr--r-- 1 root root 42400 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
xen-blkfront.ko
-rwxr--r-- 1 root root 44200 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
xen-netfront.ko

SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/
virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
virtio_net.ko
```

e. Restart the ECS.

f. Modify the **/boot/grub/menu.lst** file to add **xen_platform_pci.dev_unplug=all** and change the root settings.

Before the modification:

```
###Don't change this comment -YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11SP4 - 3.0.76-0.11 (default)
root (hd0,0)
kernel /boot/vmlinuz-3.0.76-0.11-default root=UUID=4eb40294-4c6f-4384-bbb6-
b8795bbb1130 splash=silentcrashkernel=256M-:128M showopts vga=0x314
initrd /boot/initrd-3.0.76-0.11-default
```

After the modification:

```
###Don't change this comment -YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11SP4 - 3.0.76-0.11 (default)
root (hd0,0)
kernel /boot/vmlinuz-3.0.76-0.11-default root=UUID=4eb40294-4c6f-4384-bbb6-
b8795bbb1130 splash=silentcrashkernel=256M-:128M showopts vga=0x314
xen_platform_pci.dev_unplug=all
initrd /boot/initrd-3.0.76-0.11-default
```

NOTE

- Ensure that the root partition is in UUID format.
- **xen_platform_pci.dev_unplug=all** is used to shield QEMU devices.
- For SUSE 11 SP1 64bit to SUSE 11 SP4 64bit, add **xen_platform_pci.dev_unplug=all** to the **menu.lst** file. For SUSE 12 or later, QEMU device shield is enabled by default, and you do not need to configure it.

g. Run the following commands to check whether Xen drivers exist in initrd:

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

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

```
SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rwxr--r-- 1 root root 42400 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
xen-blkfront.ko
-rwxr--r-- 1 root root 44200 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
xen-netfront.ko

SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/
virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
virtio_net.ko
```

NOTE

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

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

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

- SUSE 12 SP1:

a. Run the following command to open the **/etc/dracut.conf** file:

vi /etc/dracut.conf

b. Press **i** to enter editing mode and add Xen PV and VirtIO drivers to **add-drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxxx ~]# vi /etc/dracut.conf
# additional kernel modules to the default
add_drivers+="ata_piix ata_generic xen_vnif xen_vbd xen_platform_pci virtio_blk virtio_scsi
virtio_net virtio_pci virtio_ring virtio"
```

c. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

d. Run the following command to regenerate initrd:

dracut -f /boot/initramfs-*File name*

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

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

lsinitrd /boot/initramfs-\`uname -r\`.img | grep xen

lsinitrd /boot/initramfs-\`uname -r\`.img | grep virtio

If the virtual file system is initrd, run the following commands:

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

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

- Later than SUSE 12 SP1 or openSUSE 13:

  Take SUSE Linux Enterprise Server 12 SP2 (x86_64) as an example.

a. Run the following command to open the **/etc/dracut.conf** file:

vi /etc/dracut.conf

b. Press **i** to enter editing mode and add Xen PV and VirtIO drivers to **add_drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxxx ~]# vi /etc/dracut.conf
# additional kernel modules to the default
add_drivers+="ata_piix ata_generic xen-blkfront xen-netfront virtio_blk virtio_scsi
virtio_net virtio_pci virtio_ring virtio"
```

c. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

d. Run the following command to regenerate initrd:

dracut -f /boot/initramfs-*File name*

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

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

lsinitrd /boot/initramfs-\`uname -r\`.img | grep xen

lsinitrd /boot/initramfs-\`uname -r\`.img | grep virtio

If the virtual file system is initrd, run the following commands:

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

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

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

```
sluo-ecs-30dc:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rw-r--r-- 1 root root 69575 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/block/xen-blkfront.ko
-rw-r--r-- 1 root root 53415 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/net/xen-netfront.ko
drwxr-xr-x 2 root root 0 Sep 28 10:21 lib/modules/4.4.21-69-default/updates/pvdriver/xen-hcall
-rwxr-xr-x 1 root root 8320 Sep 28 10:21 lib/modules/4.4.21-69-default/updates/pvdriver/xen-hcall/xen-hcall.ko

sluo-ecs-30dc:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rw-r--r-- 1 root root 29335 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/block/virtio_blk.ko
-rw-r--r-- 1 root root 57007 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/net/virtio_net.ko
-rw-r--r-- 1 root root 32415 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/scsi/virtio_scsi.ko
drwxr-xr-x 2 root root 0 Sep 28 10:21 lib/modules/4.4.21-69-default/kernel/drivers/virtio
-rw-r--r-- 1 root root 19623 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio.ko
-rw-r--r-- 1 root root 38943 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio_pci.ko
-rw-r--r-- 1 root root 24431 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio_ring.ko
```

NOTE

> If you add built-in drivers to the initrd or initramfs file by mistake, the ECS will not be affected. The drivers cannot be found by running the **lsinitrd** command. You can run the following commands to check whether built-in drivers are in the kernel:
>
> **cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y**
>
> **cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y**

Follow-up Procedure

Delete log files, historical records, and other data.

1. Delete unnecessary key files.

   echo > */$path/$to/$root***/.ssh/authorized_keys**

   Example: **echo > /root/.ssh/authorized_keys**

   echo > */$path/$to/$none-root***/.ssh/authorized_keys**

   Example: **echo > /home/linux/.ssh/authorized_keys**

2. Delete log files from the **/var/log** directory.

   rm -rf /var/log/*

   NOTE

   > Before deleting log files, back up log directories and log files required by application startup. For example, if the default Nginx log directory **/var/log/nginx** is deleted, Nginx may fail to be started.

3. Delete historical records.

   echo > /root/.bash_history

   history -c

2.3.10 Installing Native KVM Drivers on a KVM ECS

Scenarios

Before using a KVM ECS to create a private image, you need to install native KVM drivers on the ECS. If the drivers have been installed, skip this section.

⚠ CAUTION

If you do not install KVM drivers, NICs of the ECS may not be detected and the ECS cannot communicate with other resources.

Prerequisites

- The virtualization type of the ECS is KVM.

  You can run the following command to check the virtualization type of an ECS:

  lscpu

  – If the value of **Hypervisor vendor** is **XEN**, install drivers as instructed in **Installing Native Xen and KVM Drivers on a Xen ECS**.

  – If the value of **Hypervisor vendor** is **KVM**, install drivers as instructed in this section.

    NOTE

    If the command output does not contain **Hypervisor vendor**, install drivers as instructed in this section.

- No native KVM drivers are installed on the ECS.

  a. Check whether VirtIO drivers are installed. The command varies depending on the OS.

     ■ CentOS/EulerOS

       If the root filesystem is mounted by initramfs, run the following command:

       lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

       If the root filesystem is mounted by initrd, run the following command:

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

     ■ Ubuntu/Debian

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

     ■ SUSE/openSUSE

       ○ SUSE 12 SP1/openSUSE 13 or earlier:

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

       ○ SUSE 12 SP1 or later than SUSE 12 SP1/openSUSE 13:

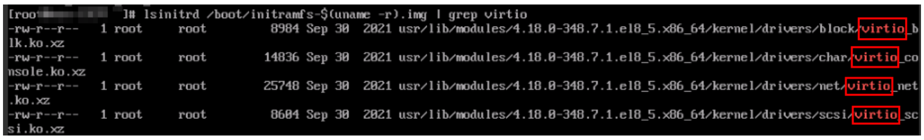
         If the root filesystem is mounted by initramfs, run the following command:

lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

If the root filesystem is mounted by initrd, run the following command:

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

If VirtIO drivers have been installed, skip this section.



```
[roo[redacted]]# lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
-rw-r--r--   1 root     root         8984 Sep 30  2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/block/virtio_b
lk.ko.xz
-rw-r--r--   1 root     root        14836 Sep 30  2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/char/virtio_co
nsole.ko.xz
-rw-r--r--   1 root     root        25748 Sep 30  2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/net/virtio_net
.ko.xz
-rw-r--r--   1 root     root         8604 Sep 30  2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/scsi/virtio_sc
si.ko.xz
```

If VirtIO drivers have not been installed, install them as instructed in this section.

- The ECS kernel must be later than 2.6.24.
- Disable your antivirus and intrusion detection software. You can enable the software after KVM drivers are installed.
- You have performed operations in **Changing Disk Identifiers in the GRUB File to UUID** and **Changing Disk Identifiers in the fstab File to UUID**.

Procedure

Modify the configuration file based on the OS version.

Table 2-10 Modifying configuration files for different OSs

OS	Configuration	Reference
CentOS/EulerOS	Take CentOS 7.0 as an example. 1. In the **/etc/dracut.conf** file, add VirtIO drivers to **add_drivers**, including virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. 2. Save and exit the **/etc/dracut.conf** file and run the **dracut -f** command to generate **initrd** again.	**CentOS and EulerOS**
Ubuntu/Debian	1. In the **/etc/initramfs-tools/modules** file, add VirtIO drivers, including virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. 2. Save and exit the **/etc/initramfs-tools/modules** file and run the **update-initramfs -u** command to generate **initrd** again.	**Ubuntu and Debian**

OS	Configuration	Reference
SUSE and openSUSE	If the OS version is earlier than SUSE 12 SP1 or openSUSE 13: 1. In the **/etc/sysconfig/kernel** file, add VirtIO drivers to **INITRD_MODULES=""**. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. 2. Run the **mkinitrd** command to generate **initrd** again.	**SUSE and openSUSE (Earlier than SUSE 12 SP1 or openSUSE 13)**
	If the OS version is SUSE 12 SP1: 1. In the **/etc/dracut.conf** file, add VirtIO drivers to **add_drivers**. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. 2. Run the **dracut -f** command to generate **initrd** again.	**SUSE and openSUSE (SUSE 12 SP1)**
	If the OS version is later than SUSE 12 SP1 or openSUSE 13: 1. In the **/etc/dracut.conf** file, add VirtIO drivers to **add_drivers**, including virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. 2. Save and exit the **/etc/dracut.conf** file and run the **dracut -f** command to generate **initrd** again.	**SUSE and openSUSE (Later than SUSE 12 SP1 or openSUSE 13)**

CentOS and EulerOS

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

   vi /etc/dracut.conf

2. Press **i** to enter the editing mode and add VirtIO drivers to **add_drivers** (the format varies depending on the OS).

   ```
   [root@CTU10000xxxxx ~]# vi /etc/dracut.conf
   # additional kernel modules to the default
   add_drivers+="virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring virtio"
   ....
   ```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

4. Run the following command to regenerate initrd:

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

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

5. If the virtual file system is initramfs, run the following command to check whether native KVM drivers have been installed:

   lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

   If the virtual file system is initrd, run the following command to check whether native KVM drivers have been installed:

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

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

```
[root@CTU10000xxxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep virtio
-rwxr--r--   1 root     root        23448 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
block/virtio_blk.ko
-rwxr--r--   1 root     root        50704 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/
drivers/net/virtio_net.ko
-rwxr--r--   1 root     root        28424 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
scsi/virtio_scsi.ko
drwxr-xr-x   2 root     root            0 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio
-rwxr--r--   1 root     root        14544 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio.ko
-rwxr--r--   1 root     root        21040 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_pci.ko
-rwxr--r--   1 root     root        18016 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_ring.ko
```

   NOTE

   If you add built-in drivers to the initrd or initramfs file, the ECS will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the **lsinitrd** command. You can run the following command to check whether the drivers are built-in ones in the kernel:

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

Ubuntu and Debian

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

   vi /etc/initramfs-tools/modules

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

```
[root@CTU10000xxxxx ~]#vi /etc/initramfs-tools/modules
...
# Examples:
#
# raid1
# sd_mOd
virtio_blk
virtio_scsi
virtio_net
virtio_pci
virtio_ring
virtio
```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/initramfs-tools/modules** file.

4. Run the following command to regenerate initrd:

   update-initramfs -u

5. Run the following command to check whether native KVM drivers have been installed:

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

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

   ```
   [root@ 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
   ```

SUSE and openSUSE (Earlier than SUSE 12 SP1 or openSUSE 13)

Modify the **/etc/sysconfig/kernel** file.

1. Run the following command to modify the **/etc/sysconfig/kernel** file:

   vi /etc/sysconfig/kernel

2. Add VirtIO drivers to **INITRD_MODULES=""** (the format of drivers depends on the OS).

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

3. Run the **mkinitrd** command to generate **initrd** again.

   NOTE

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

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

   ```
   default 0
   timeout 10
   gfxmenu (hd0,0)/boot/message
   title sles11sp4_001_[_VMX_]
   root (hd0,0)
   kernel /boot/linux.vmx vga=0x314 splash=silent console=ttyS0,115200n8 console=tty0 net.ifnames=0
   NON_PERSISTENT_DEVICE_NAMES=1 showopts
   initrd /boot/initrd.vmx
   title Failsafe_sles11sp4_001_[_VMX_]
   root (hd0,0)
   kernel /boot/linux.vmx vga=0x314 splash=silent ide=nodma apm=off noresume edd=off
   powersaved=off nohz=off highres=off processor.max+cstate=1 nomodeset x11failsafe
   console=ttyS0,115200n8 console=tty0 net.ifnames=0 NON_PERSISTENT_DEVICE_NAMES=1 showopts
   initrd /boot/initrd.vmx
   ```

   /boot/initrd.vmx in the **initrd** line is the **initrd** file actually used. Run the **dracut -f /boot/initrd.vmx** command. If the **initrd** file does not contain the **/**

boot directory, such as **/initramfs-***xxx*, run the **dracut -f /boot/initramfs-***xxx* command.

4. Run the following command to check whether KVM VirtIO drivers have been installed:

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

```
SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/virtio_net.ko
```

5. Restart the ECS.

6. Run the following command to check whether KVM drivers exist in initrd:

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

```
SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/virtio_net.ko
```

NOTE

If you add built-in drivers to the initrd or initramfs file, the ECS will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the **lsinitrd** command. You can run the following command to check whether the drivers are built-in ones in the kernel:

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

SUSE and openSUSE (SUSE 12 SP1)

Modify the **/etc/dracut.conf** file.

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

   vi /etc/dracut.conf

2. Press **i** to enter the editing mode and add VirtIO drivers to **add-drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxxx ~]# vi /etc/dracut.conf
# additional kernel modules to the default
add_drivers+="ata_piix ata_generic virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring virtio"
```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

4. Run the following command to regenerate initrd:

dracut -f /boot/initramfs-*File name*

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

5. If the virtual file system is initramfs, run the following command to check whether native KVM drivers have been installed:

   lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

   If the virtual file system is initrd, run the following command to check whether native KVM drivers have been installed:

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

SUSE and openSUSE (Later than SUSE 12 SP1 or openSUSE 13)

Modify the **/etc/dracut.conf** file.

Take SUSE Linux Enterprise Server 12 SP2 (x86_64) as an example.

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

   vi /etc/dracut.conf

2. Press **i** to enter the editing mode and add VirtIO drivers to **add_drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxxx ~]# vi /etc/dracut.conf
# additional kernel modules to the default
add_drivers+="ata_piix ata_generic virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring virtio"
```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

4. Run the following command to regenerate initrd:

   dracut -f /boot/initramfs-*File name*

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

5. If the virtual file system is initramfs, run the following command to check whether native KVM drivers have been installed:

   lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

   If the virtual file system is initrd, run the following command to check whether native KVM drivers have been installed:

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

   Assume that the virtual file system is initrd. The following command output will be displayed:

```
sluo-ecs-30dc:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rw-r--r-- 1 root root 29335 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/block/
virtio_blk.ko
-rw-r--r-- 1 root root 57007 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/net/
virtio_net.ko
-rw-r--r-- 1 root root 32415 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/scsi/
virtio_scsi.ko
drwxr-xr-x 2 root root 0 Sep 28 10:21 lib/modules/4.4.21-69-default/kernel/drivers/virtio
```

```
-rw-r--r-- 1 root root 19623 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio.ko
-rw-r--r-- 1 root root 38943 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/
virtio_pci.ko
-rw-r--r-- 1 root root 24431 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/
virtio_ring.ko
```

NOTE

If you add built-in drivers to the initrd or initramfs file, the ECS will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the **lsinitrd** command. You can run the following command to check whether the drivers are built-in ones in the kernel:

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

Follow-up Procedure

Delete log files, historical records, and other data.

1. Delete unnecessary key files.

   echo > */$path/$to/$root*/**.ssh/authorized_keys**

   Example: **echo > /root/.ssh/authorized_keys**

   echo > */$path/$to/$none-root*/**.ssh/authorized_keys**

   Example: **echo > /home/linux/.ssh/authorized_keys**

2. Delete log files from the **/var/log** directory.

   rm -rf /var/log/*

   NOTE

   Before deleting log files, back up log directories and log files required by application startup. For example, if the default Nginx log directory **/var/log/nginx** is deleted, Nginx may fail to be started.

3. Delete historical records.

   echo > /root/.bash_history

   history -c

3 Creating a Private Image from a Cloud Server or a Backup

3.1 Overview

A private image contains an OS or service data, preinstalled public applications, and a user's personal applications. Private images are only available to the users who created them.

IMS provides multiple methods for creating private images.

Table 3-1 Creating a private image

Method	Description	Helpful Link
Creating a private image from a cloud server or a backup	If you already have an ECS on Huawei Cloud and configured it based on your service requirements (for example, by installing software or setting up an application environment), you can use this ECS to create a private image. A private image can be a system disk image, data disk image, or full-ECS image. ● System disk image: contains an OS and application software from the system disk. ● Data disk image: contains service data from data disks. ● Full-ECS image: contains data of an entire ECS, that is, the OS and application software from the system disk and service data from data disks.	● **Creating a System Disk Image from an ECS** ● **Creating a Full-ECS Image from an ECS** ● **Creating a Full-ECS Image from a CSBS Backup** ● **Creating a Full-ECS Image from a CBR Backup**

Method	Description	Helpful Link
Creating a private image from an image file	You can import an image file from your local PC or other cloud platforms to Huawei Cloud IMS and register it as a private image. Then, you can use the image to create new ECSs or data disks, or change the OS for existing ECSs. This way, your services can be migrated to the cloud or in the cloud.	**Overview**

3.2 Creating a System Disk Image from an ECS

Scenarios

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

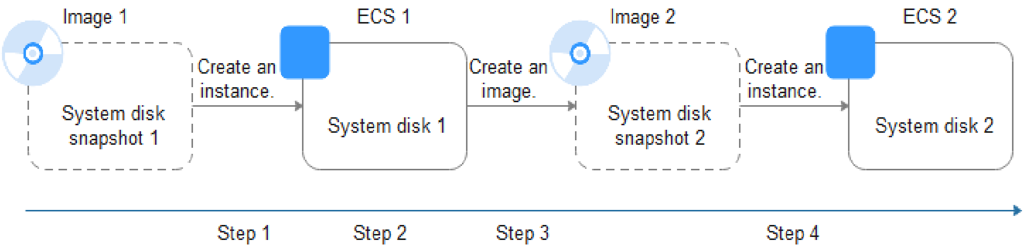
Creating a system disk image does not affect services on the cloud server or cause data loss.

Video Tutorial

Background

The following figure shows the process of creating a system disk image from a cloud server and using the image to create new cloud servers.

Figure 3-1 Creating a system disk image and using it to create a cloud server



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

a. Create a system disk image from a cloud server.

NOTE

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

- ISO images
- Private images created from a SUSE, Red Hat, Ubuntu, Oracle Linux, or Windows public image
- Private images created from a KooGallery image

b. Export the image to an OBS bucket. For details, see **Exporting an Image**.

c. Download the image file from the OBS bucket.

- You can create an image from a running cloud server.

  The image creation does not affect services on the cloud server.

  In this process, do not stop, start, or restart the cloud server, or the image creation may fail.
- The time required for creating an image depends on the system disk size, network quality, and the number of concurrent tasks.
- A system disk image will be created in the same region as the cloud server that was used to create it. For example, if a cloud server is located in the CN-Hong Kong region, the system disk image created from that cloud server will also be located in the CN-Hong Kong region. If you want to use the image in another region, you must first replicate it to that region. For details, see **Replicating Images Across Regions**.
- If a cloud server has expired or been released, you can use the system disk image created from the cloud server to restore it.

Constraints

The system disk capacity of the cloud server used to create a system disk image must be no greater than 1 TB.

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

Prerequisites

Before creating a private image from a cloud server:

- Delete any sensitive data the ECS may contain.
- Ensure that the ECS is in the **Running** or **Stopped** state.
- Complete all operations in **Windows Private Images** or **Linux Private Images** to configure the cloud server.
- If the cloud server is a BMS, understand the related constraints and prerequisites. For details, see **Creating a Private Image from a BMS**.

Procedure

Step 1 Access the IMS console.

1. Log in to the management console.

2. Under **Compute**, click **Image Management Service**.

   The IMS console is displayed.

Step 2 Create a system disk image.

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

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

Table 3-2 Image type and source

Parameter	Description
Type	Select **Create Image**.
Region	Select a region close to where your services will be provided. If you select an incorrect region here, you can replicate the created image to your desired region later. For details, see **Replicating an Image Across Regions**.
Image Type	Select **System disk image**.
Source	Select a cloud server with required configurations.

Table 3-3 Image information

Parameter	Description
Encryption	This parameter specifies whether the image will be encrypted. The value is provided by the system and cannot be changed. – Only an unencrypted private image can be created from an unencrypted ECS. – Only an encrypted private image can be created from an encrypted ECS.
Name	Set a name for the image.
Enterprise Project	Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. To enable this function, contact your customer manager. An enterprise project provides central management of cloud resources on a project.

Parameter	Description
Tag	(Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. **NOTE** If your organization has configured tag policies for images, you need to add tags to your images based on the policies. If you add a tag that does not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies. – Each tag consists of a key and a value. The key contains a maximum of 36 characters, and the value contains a maximum of 43 characters. The key cannot be left blank or an empty string. The value cannot be left blank but can be an empty string. – An image can have a maximum of 10 tags.
Description	(Optional) Describe the image.

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

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

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

NOTE

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

----End

Follow-up Procedure

After a system disk image is created, you can:

- Use the image to create new cloud servers. For details, see **Creating an ECS from an Image**.
- Use the image to change the OSs of existing cloud servers. For details, see **Changing the OS**.

3.3 Creating a Data Disk Image from a Cloud Server

Scenarios

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

You are advised to use data disk images in the following scenarios:

- Migrate service data on an ECS to another account.

  Create a data disk image from the data disk and **share** the image with the target account. Then you can use the data disk image under the account to create data disks, completing the service data migration.

- Migrate service data on an ECS to another region.

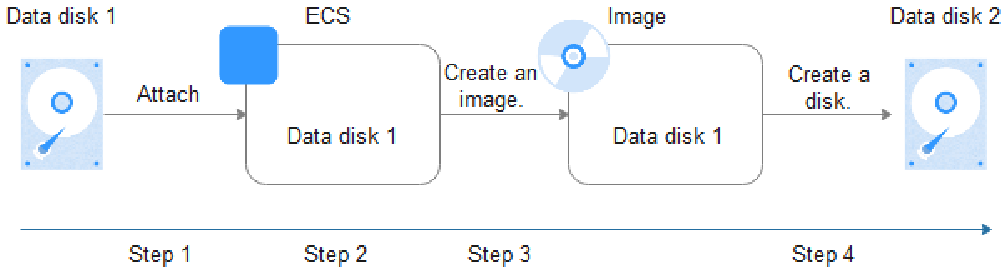
  Create a data disk image from the data disk in the current region and replicate the image to the target region (for details, see **Replicating Images Across Regions**). Then you can use the data disk image in the target region to create data disks, completing the service data migration.

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

Background

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

Figure 3-2 Creating a data disk image and using it to create data disks



Prerequisites

- A data disk has been attached to the ECS. For details, see *Elastic Cloud Server User Guide*.
- The ECS status is **Running** or **Stopped**.

Constraints

The data disk capacity of the cloud server must be no greater than 1 TB.

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

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

Step 2 Create a data disk image.

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

Figure 3-3 Creating a data disk image

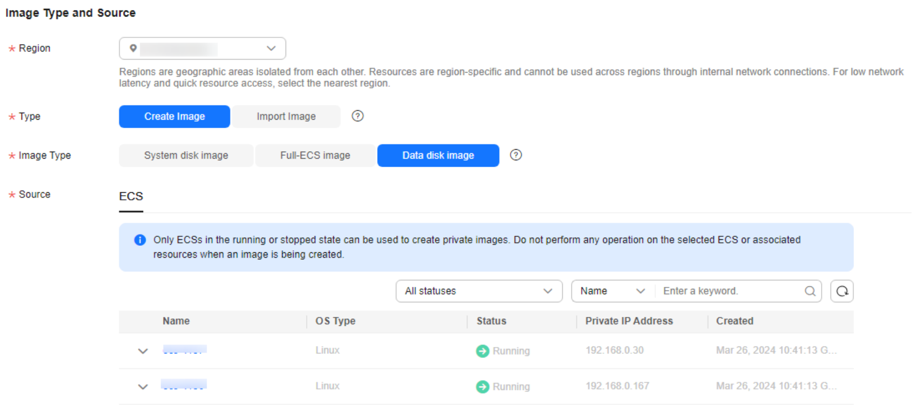


Image Type and Source

* Region [redacted]

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* Type: Create Image | Import Image

* Image Type: System disk image | Full-ECS image | Data disk image

* Source: ECS

Only ECSs in the running or stopped state can be used to create private images. Do not perform any operation on the selected ECS or associated resources when an image is being created.

All statuses | Name | Enter a keyword.

Name	OS Type	Status	Private IP Address	Created
[redacted]	Linux	Running	192.168.0.30	Mar 26, 2024 10:41:13 G...
[redacted]	Linux	Running	192.168.0.167	Mar 26, 2024 10:41:13 G...

4. In the **Image Information** area, set **Name**, **Tag**, and **Description**, and select an enterprise project.

   If the data disk is not encrypted, the private image created from it is also not encrypted. The encryption attribute cannot be changed during image creation. After the image is created, you can change its encryption attribute based on **Replicating Images Within a Region**.

   NOTE

   If your organization has configured tag policies for images, you need to add tags to your images based on the policies. If you do not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies.

   – Each tag consists of a key and a value. The key contains a maximum of 36 characters, and the value contains a maximum of 43 characters. The key cannot be left blank or an empty string. The value cannot be left blank but can be an empty string.

   – An image can have a maximum of 10 tags.

5. Click **Next**.
6. Confirm the settings. Read the image disclaimer and select **I have read and agree to the Image Disclaimer**, and click **Submit**.

   The private image list is displayed. Wait until the data disk image is created successfully.

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

----End

Follow-up Procedure

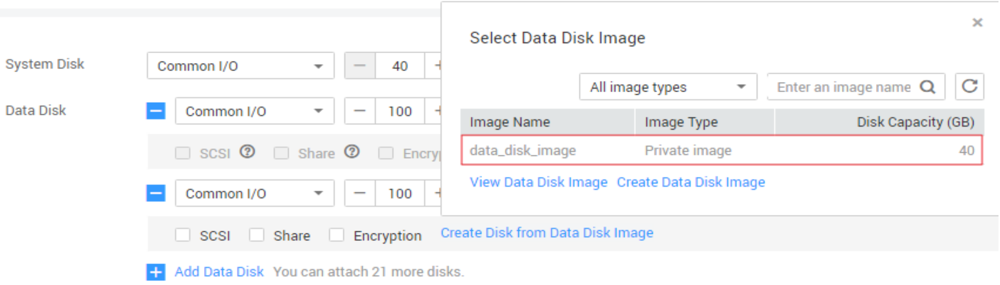
If you want to use the created data disk image to create an EVS disk and attach it to an ECS, you can perform either of the following operations:

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

NOTE

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

Figure 3-4 Adding data disks



System Disk Common I/O 40

Data Disk Common I/O 100

□ SCSI □ Share □ Encry

Common I/O 100

□ SCSI □ Share □ Encryption Create Disk from Data Disk Image

Add Data Disk You can attach 21 more disks.

Select Data Disk Image

All image types Enter an image name

Image Name	Image Type	Disk Capacity (GB)
data_disk_image	Private image	40

View Data Disk Image Create Data Disk Image

3.4 Creating a Full-ECS Image from an ECS

Scenarios

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

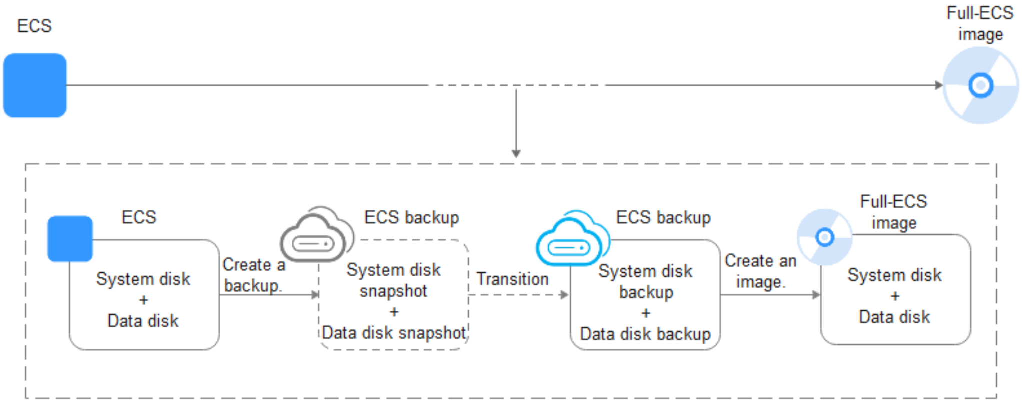
NOTE

This section does not apply to a BMS.

Background

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

Figure 3-5 Creating a full-ECS image from an ECS



- The time required for creating a full-ECS image depends on the disk size, network quality, and the number of concurrent tasks.
- The ECS used to create a full-ECS image must be in **Running** or **Stopped** state. To create a full-ECS image containing a database, use a stopped ECS.
- If an ECS is in **Stopped** state, do not start it when you are using it to create a full-ECS image.
- When a full-ECS image is being created from an ECS, do not perform any operations on the ECS, or the image creation may fail.
- In **Figure 3-5**, if there are snapshots of the system disk and data disks but the ECS backup creation is not complete, the full-ECS image you create will only be available in the AZ where the source ECS is and can only be used to provision ECSs in this AZ. You cannot provision ECSs in other AZs in the region until the original ECS is fully backed up and the full-ECS image is in the **Normal** state.
- If you use a full-ECS image to change an ECS OS, only the system disk data can be written into the ECS. Therefore, if you want to restore or migrate the data disk data of an ECS by using a full-ECS image, you can only use the image to create a new ECS rather than use it to change the ECS OS.

Constraints

- When creating a full-ECS image from an ECS, ensure that the ECS has been properly configured, or the image creation may fail.

  For details, see **How Do I Configure an ECS, BMS, or Image File Before I Use It to Create an Image?**
- A Windows ECS used to create a full-ECS image cannot have a spanned volume, or data may be lost when ECSs are created from that image.
- A Linux ECS used to create a full-ECS image cannot have a disk group or logical disk that contains multiple physical disks, or data may be lost when ECSs are created from that image.
- An ECS used to create a full-ECS image cannot contain a Dedicated Distributed Storage Service (DSS) disk.
- A full-ECS image cannot be published in KooGallery.
- A full-ECS image cannot be exported.

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

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

  A full-ECS image created using an ECS backup can be replicated from the region where they reside to another region, but the replicated full-ECS image cannot be replicated across regions again.
- When creating a full-ECS image from a Windows ECS, you need to change the SAN policy of the ECS to OnlineAll. Otherwise, EVS disks attached to the ECSs created from the image may be offline.

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

Table 3-4 SAN policies in Windows

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

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

   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 **c**.

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

   san policy=onlineall

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

Step 2 Create a full-ECS image.

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

Figure 3-6 Creating a full-ECS image using an ECS

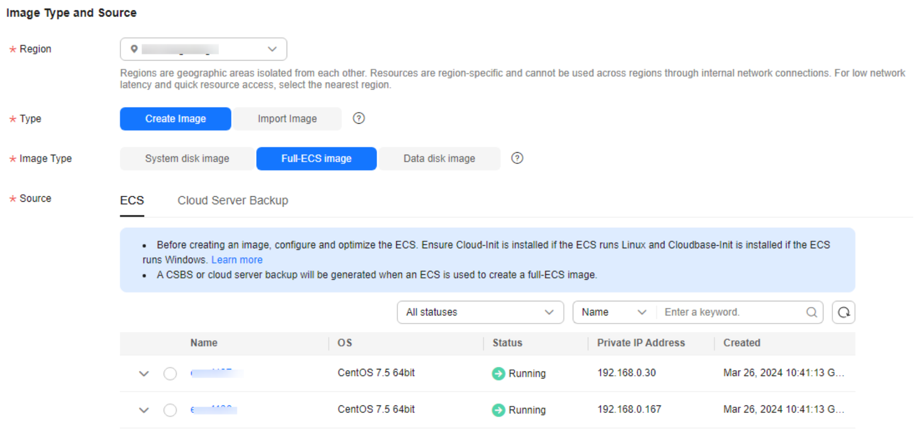


Image Type and Source

* Region [redacted]

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* Type: Create Image | Import Image

* Image Type: System disk image | Full-ECS image | Data disk image

* Source: ECS | Cloud Server Backup

- Before creating an image, configure and optimize the ECS. Ensure Cloud-Init is installed if the ECS runs Linux and Cloudbase-Init is installed if the ECS runs Windows. Learn more
- A CSBS or cloud server backup will be generated when an ECS is used to create a full-ECS image.

All statuses | Name | Enter a keyword.

	Name	OS	Status	Private IP Address	Created
○	[redacted]	CentOS 7.5 64bit	Running	192.168.0.30	Mar 26, 2024 10:41:13 G...
○	[redacted]	CentOS 7.5 64bit	Running	192.168.0.167	Mar 26, 2024 10:41:13 G...

4. Specify **Server Backup Vault** to store backups.

   The created full-ECS image and backup are stored in the server backup vault.

   If no server backup vault is available, click **Create Server Backup Vault** to create one. Ensure that you select **Backup** for **Protection Type**. For more information about CBR backups and vaults, see **What Is CBR?**

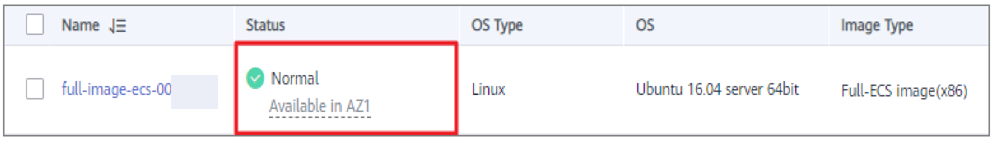
5. In the **Image Information** area, configure basic image details, such as the image name and description.
6. Click **Next**.
7. Confirm the settings. Read the image disclaimer and select **I have read and agree to the Image Disclaimer**, and click **Submit**.

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

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

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

Figure 3-7 Full-ECS image status



□ Name	Status	OS Type	OS	Image Type
□ full-image-ecs-00[redacted]	Normal Available in AZ1	Linux	Ubuntu 16.04 server 64bit	Full-ECS image(x86)

----End

Follow-up Procedure

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

  NOTE

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

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

3.5 Creating a Full-ECS Image from a CSBS Backup

Scenarios

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

NOTE

CSBS is being gradually replaced by CBR. If **CSBS Backup** is unavailable for **Source**, select another image source.

Background

- If you use a CSBS backup to create a full-ECS image, you will only be charged for the CSBS backup. For detailed service pricing, see **Cloud Server Backup Service** in **Product Pricing Details**.

- When deleting a full-ECS image, you can choose whether to delete the associated CSBS backup. If you choose not to delete the CSBS backup, you will continue to be charged for it.
- If you use a full-ECS image to change an ECS OS, only the system disk data can be written into the ECS. Therefore, if you want to restore or migrate the data disk data of an ECS by using a full-ECS image, you can only use the image to create a new ECS rather than use it to change the ECS OS.

Constraints

- When creating a full-ECS image from a CSBS backup, ensure that the source ECS of the CSBS backup has been properly configured, or the image creation may fail.

  For details, see **How Do I Configure an ECS, BMS, or Image File Before I Use It to Create an Image?**
- If an ECS is in **Stopped** state, do not start it when you are using it to create a full-ECS image.
- A CSBS backup used to create a full-ECS image cannot have shared disks.
- Only an available CSBS backup can be used to create a full-ECS image. A CSBS backup can be used to create only one full-ECS image.
- A full-ECS image cannot be published in KooGallery.
- A full-ECS image cannot be exported.
- A full-ECS image cannot be replicated within a region.
- Cross-region replication of full-ECS images is only available for certain regions.

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

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

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

Step 2 Create a full-ECS image.

1. Click **Create Image** in the upper right corner.
2. In the **Image Type and Source** area, select **Create Image** for **Type** and then select **Full-ECS image** for **Image Type**.
3. Select **CSBS Backup** for **Source** and then select a backup from the list.
4. In the **Image Information** area, configure basic image details, such as the image name and description.
5. Click **Next**.

6. Confirm the settings. Read the image disclaimer and select **I have read and agree to the Image Disclaimer**, and click **Submit**.

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

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

----End

Follow-up Procedure

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

  NOTE

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

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

3.6 Creating a Full-ECS Image from a CBR Backup

Scenarios

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

Background

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

data disk data of an ECS by using a full-ECS image, you can only use the image to create a new ECS rather than use it to change the ECS OS.

Constraints

- When creating a full-ECS image from a CBR backup, ensure that the source ECS of the CBR backup has been properly configured, or the image creation may fail.

  For details, see **How Do I Configure an ECS, BMS, or Image File Before I Use It to Create an Image?**
- A CBR backup can be used to create only one full-ECS image.
- If an ECS is in **Stopped** state, do not start it when you are using it to create a full-ECS image.
- A full-ECS image created from a CBR backup can be shared with other tenants. However, if it is a shared CBR backup, the full-ECS image created from it cannot be shared.
- A full-ECS image cannot be published in KooGallery.
- A full-ECS image cannot be exported.
- A full-ECS image cannot be replicated within a region.
- Cross-region replication of full-ECS images is only available for certain regions.

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

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

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

Step 2 Create a full-ECS image.

1. Click **Create Image** in the upper right corner.
2. In the **Image Type and Source** area, select **Create Image** for **Type** and then select **Full-ECS image** for **Image Type**.
3. Select **Cloud Server Backup** for **Source** and then select a CBR backup from the list.
4. In the **Image Information** area, configure basic image details, such as the image name and description.
5. Click **Next**.
6. Confirm the settings. Read the image disclaimer and select **I have read and agree to the Image Disclaimer**, and click **Submit**.

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

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

----End

Follow-up Procedure

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

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

  NOTE

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

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

3.7 Creating a System Disk Image from a BMS

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

- **Creating a Private Image from a BMS**
- **Creating a Private Image from an External Image File**

4 Creating a Private Image from an Image File

4.1 Overview

A private image contains an OS or service data, preinstalled public applications, and a user's personal applications. Private images are only available to the users who created them.

You can import an image file from your local PC or other cloud platforms to Huawei Cloud IMS and register it as a private image. Then, you can use the image to create new cloud servers or data disks, or change the OS for existing cloud servers. This way, your services can be migrated to the cloud or in the cloud.

The methods for creating a private image from an image file vary depending on the image file format and size.

Table 4-1 Overview

Image File Format	Image File Size	Helpful Link
VMDK, VHD, QCOW2, VHDX, QED, VDI, QCOW, or ZVHD	No larger than 128 GB	• **Creating a System Disk Image from an Image File** • **Creating a Data Disk Image from an Image File**
RAW or ZVHD2	No larger than 1 TB	• **Fast Import of an Image File** • **Creating a Data Disk Image from an Image File**
ISO	No larger than 128 GB	• **Creating a Windows System Disk Image from an ISO File** • **Creating a Linux System Disk Image from an ISO File**

You can also create a private image from a cloud server or a backup. For details, see **Overview**.

4.2 Creating a System Disk Image from an Image File

You can import a system disk image file from your local PC or other cloud and register the image file as a private image. Then, you can use this image to create ECSs or reinstall the OSs for existing ECSs.

Constraints

- The image file format can be VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, or ZVHD.
- The image file size cannot exceed 128 GB.

  If an image file is between 128 GB and 1 TB, convert it into RAW or ZVHD2 and import it using fast import.

  - For details about how to convert the image file format, see **Converting the Image Format Using qemu-img-hw**.
  - For details about fast import, see **Fast Import of an Image File**.
- For details about the supported OS versions, see **External Image File Formats and Supported OSs**. These OSs support automatic configuration. For details, see **What Will the System Do to an Image File When I Use the File to Register a Private Image?** For other OSs, check and install drivers by yourself. For Windows, see **Installing PV Drivers** and **Installing VirtIO Drivers**.

  For Linux, see **Installing Native Xen and KVM Drivers on a Xen ECS**. When you register an image file as a private image, select **Other Windows** or **Other Linux**. The OS can start up normally only after all the required drivers are installed.
- The OS cannot be bound to specific hardware.
- The OS must support full virtualization.
- Currently, images with data disks cannot be created. The image file must contain only a system disk, and the system disk size must be [40 GB, 1024 GB].
- The initial password in the image file must contain uppercase letters, lowercase letters, digits, and special characters (!@$%^-_=+[{}]:,./?).
- The boot partition and system partition must be on the same disk.
- The image file must contain a valid tenant administrator account and password.
- If you use an image file to create a Windows system disk image and then use the image to create a cloud server, you cannot log in to the cloud server using a key pair or obtain the password from the key pair.
- Supported boot modes:

  Some x86 OS images support the UEFI boot mode. (For details, see **OSs Supporting UEFI Boot Mode**.)

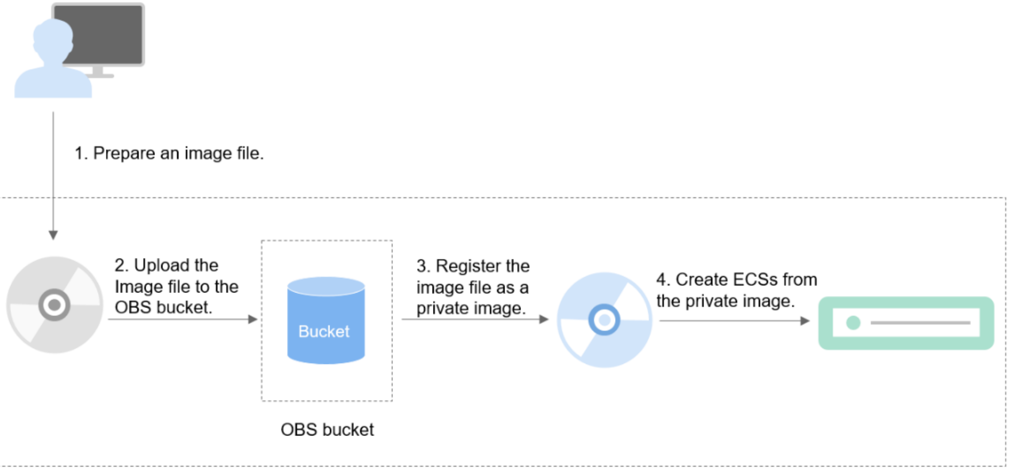
  Arm OS images support only the UEFI boot mode.
- The image file cannot be encrypted, or cloud servers created from the registered image may not work properly.

- A VMDK image file must be generated from a VM created in VMware Tools. Otherwise, the system may fail to start due to image parsing problems.

Process

Figure 4-1 shows the process of creating a private image.

Figure 4-1 Creating a system disk image


1. Prepare an image file.
2. Upload the Image file to the OBS bucket.
Bucket
OBS bucket
3. Register the image file as a private image.
4. Create ECSs from the private image.

The steps are as follows:

1. Prepare an image file that meets the cloud platform requirements. For details, see **Prepare an Image File**.
2. Upload the image file to your OBS bucket. For details, see **Upload an Image File**.
3. On the management console, select the uploaded image file and register it as a private image. For details, see **Register an Image File as a Private Image**.
4. After the private image is registered, you can use it to create ECSs. For details, see **Create an ECS from an Image**.

Video Tutorial

Prepare an Image File

Before preparing an image file, you need to understand the constraints in this section and known issues (see **Known Issues**).

The initial configuration mentioned in **Preparations for Creating a Private Image** must be completed on the source VM before an image file is exported from it.

If you did not configure it, use the image file to create an ECS, configure the ECS, and use the ECS to create a private image. For details, see **What Do I Do If a Windows Image File Is Not Pre-Configured When I Use It to Register a Private Image?**

Upload an Image File

You are advised to use OBS Browser+ to upload external image files to OBS buckets. For details, see **OBS Browser+ Best Practices**.

For how to download OBS Browser+, see **https://support.huaweicloud.com/intl/en-us/browsertg-obs/obs_03_1003.html**.

NOTE

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

Register an Image File as a Private Image

Step 1 Access the IMS console.

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

   The IMS console is displayed.

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

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

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

Table 4-2 Image type and source

Parameter	Description
Type	Select **Import Image**.
Region	Select a region close to where your services will be provided. If you select an incorrect region here, you can replicate the created image to your desired region later. For details, see **Replicating an Image Across Regions**.
Image Type	Select **System disk image**.
Source	Select the bucket storing the image file from the list and then select the image file.

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

Table 4-3 Image information

Parameter	Description
Enable automatic configuration	If you select this option, the system will automatically check and optimize the image file. For details, see **What Will the System Do to an Image File When I Use the File to Register a Private Image?**
Function	Specifies whether the image is used to create ECSs or BMSs. The value can be **ECS system disk image** or **BMS system disk image**. This section uses **ECS system disk image** as an example.
Architecture	The value can be **x86** or **ARM**. – If the system identifies that the architecture in the image file is different from what you set here, the identified architecture prevails. – If the system fails to identify an architecture, the architecture you set will be used.
Boot Mode	This parameter is optional. The value can be **BIOS** or **UEFI**. For details about the differences between them, see **How Is BIOS Different from UEFI?** For details about which OSs support UEFI boot, see **OSs supporting UEFI Boot Mode**. The boot mode must be the same as that in the image file. You need to confirm which boot mode is used in the image file. After you select the right boot mode, the boot mode will be configured for the image at the background. Select the right boot mode, or ECSs created using the image will not be able to boot up.

Parameter	Description
OS	To ensure that the image can be created and used properly, select an OS consistent with that in the image file. If you do not select an OS, the system attempts to automatically identify the OS in the image file. **NOTE** – If the system identifies that the OS in the image file is different from the one you select here, the identified OS prevails. – If the system fails to identify an OS, the OS you select will be used. – If the OS you selected or identified by the system is inconsistent with the actual one, ECSs created from the image file may not work properly.
License Type	Bring Your Own License (BYOL) is supported. If you have obtained an OS license, you do not need to apply for a license any more. This parameter is only available for Windows.
System Disk (GB)	The system disk capacity (value range: 40 GB to 1024 GB). Ensure that this value is not less than the system disk capacity in the image file. **NOTE** If the uploaded VHD image is generated using qemu-img or similar tools, check the system disk capacity based on **What Do I Do If the System Disk Capacity in a VHD Image File Exceeds the One I Have Specified on the Management Console When I Use This File to Register a Private Image?**
Data Disk (GB)	You can also add data disks to the image. You need to obtain an image file containing data disks in advance. This function is used to migrate VMs and data disks from other platforms to the current platform. To add data disks, click ⊕, configure the data disk capacity, and click **Select Image File**. In the displayed dialog box, select the target bucket and then the target image file containing the data disk. A maximum of three data disks can be added.
Name	Set a name for the image.
Encryption	(Optional) If you want to encrypt the image, select **KMS encryption** and select the key to be used from the key list. After you select **KMS encryption**, the system will create a default key **ims/default** for you. You can also select a key from the key list. For how to encrypt an image, see **Introduction**.

Parameter	Description
Enterprise Project	Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. An enterprise project provides central management of cloud resources on a project by project basis.
Tag	(Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. **NOTE** If your organization has configured tag policies for images, you need to add tags to your images based on the policies. If you do not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies. – Each tag consists of a key and a value. The key contains a maximum of 36 characters, and the value contains a maximum of 43 characters. The key cannot be left blank or an empty string. The value cannot be left blank but can be an empty string. – An image can have a maximum of 10 tags.
Description	(Optional) Describe the image.

3. Click **Next** and confirm the image specifications. Read and agree to the disclaimer and click **Submit**.

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

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

NOTE

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

----End

Create an ECS from an Image

Create an ECS by referring to **Creating an ECS from an Image**.

Note the following when setting the parameters:

- **Region**: Select the region where the private image is located.
- **Specifications**: Select a flavor based on the OS type in the image and the OS versions described in **OSs Supported for Different Types of ECSs**.
- **Image**: Select **Private image** and then the created image from the drop-down list.

- (Optional) **Data Disk**: Add data disks. These data disks are created from a data disk image generated together with a system disk image. In this way, you can migrate the data of data disks together with system disk data from the VM on the original platform to the current cloud platform.

Follow-up Procedure

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

4.3 Creating a Data Disk Image from an Image File

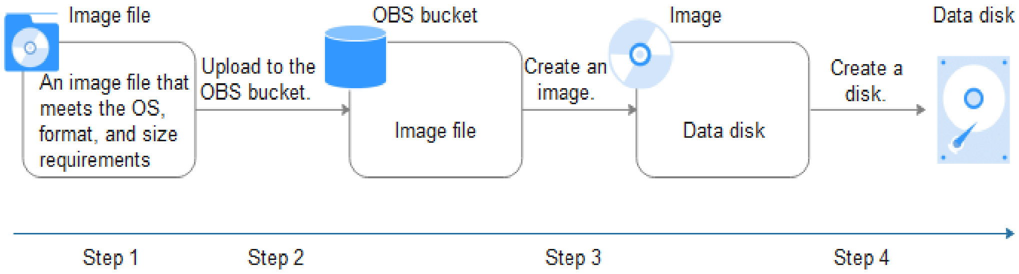
Scenarios

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

Background

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

Figure 4-2 Creating a data disk image from an external image file



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

   For details about image file format conversion, see **Converting the Image Format Using qemu-img** or **Converting the Image Format Using qemu-img-hw**.
2. When uploading the external image file, you must select an OBS bucket with standard storage. For details, see **Upload an Image File**.
3. Create a data disk image. For details, see **Procedure**.
4. Use the data disk image to create data disks. For details, see **Follow-up Procedure**.

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

Step 2 Create a data disk image.

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

   Figure 4-3 Creating a data disk image from an external image file

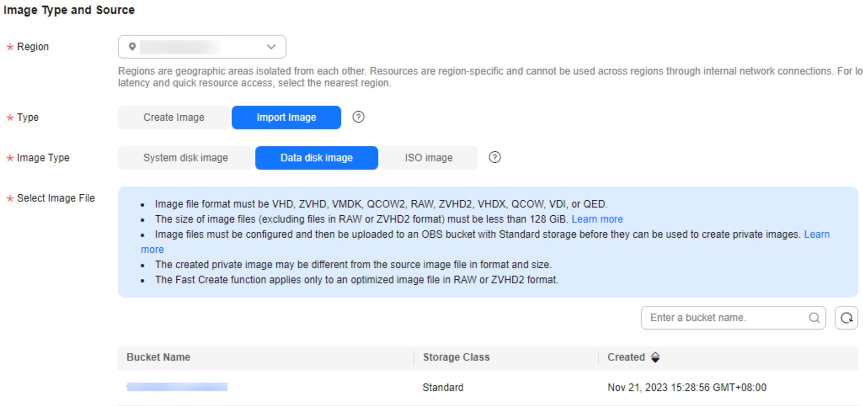
   

   Image Type and Source

   * Region [redacted]

   Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

   * Type: Create Image | **Import Image**

   * Image Type: System disk image | **Data disk image** | ISO image

   * Select Image File

   - Image file format must be VHD, ZVHD, VMDK, QCOW2, RAW, ZVHD2, VHDX, QCOW, VDI, or QED.
   - The size of image files (excluding files in RAW or ZVHD2 format) must be less than 128 GiB. Learn more
   - Image files must be configured and then be uploaded to an OBS bucket with Standard storage before they can be used to create private images. Learn more
   - The created private image may be different from the source image file in format and size.
   - The Fast Create function applies only to an optimized image file in RAW or ZVHD2 format.

   Enter a bucket name.

Bucket Name	Storage Class	Created
[redacted]	Standard	Nov 21, 2023 15:28:56 GMT+08:00

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

   NOTE

   – Currently, fast import is only available for ZVHD2 and RAW image files.

   – For how to convert image file formats and generate bitmap files, see **Fast Import of an Image File**.

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

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

– (Optional) **Tag**: Set a tag key and a tag value for the image to easily identify and manage it.

NOTE

If your organization has configured tag policies for images, you need to add tags to your images based on the policies. If you add a tag that does not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies.

- Each tag consists of a key and a value. The key contains a maximum of 36 characters, and the value contains a maximum of 43 characters. The key cannot be left blank or an empty string. The value cannot be left blank but can be an empty string.
- An image can have a maximum of 10 tags.

– (Optional) **Description**: Describe the image.

6. Click **Next**.
7. Confirm the settings. Read the image disclaimer and select **I have read and agree to the Image Disclaimer**, and click **Submit**.

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

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

----End

Follow-up Procedure

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

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

NOTE

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

Figure 4-4 Adding data disks

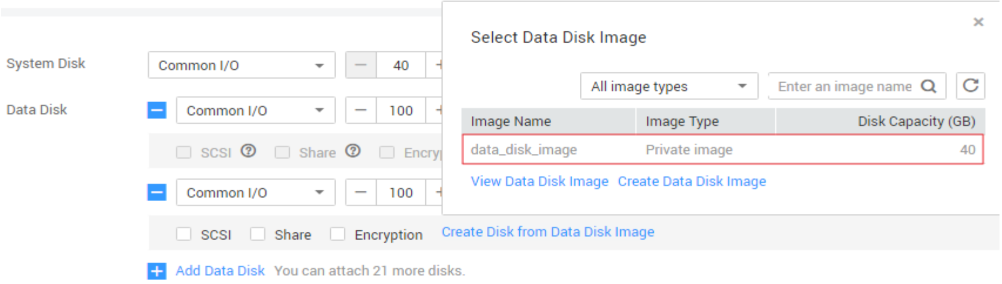


Image Name	Image Type	Disk Capacity (GB)
data_disk_image	Private image	40

4.4 Creating a Windows System Disk Image from an ISO File

4.4.1 Overview

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

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

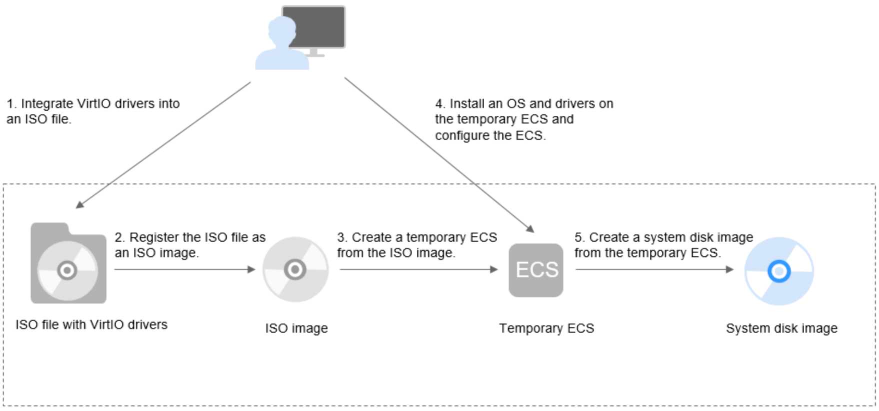
NOTE

This section is applicable only to the management console. If you are an API user, see **Creating an Image from an ISO File**.

Creation Process

Figure 4-5 shows the process of creating a Windows system disk image from an ISO file.

Figure 4-5 Creating a Windows system disk image


1. Integrate VirtIO drivers into an ISO file.
4. Install an OS and drivers on the temporary ECS and configure the ECS.
2. Register the ISO file as an ISO image.
3. Create a temporary ECS from the ISO image.
ECS
5. Create a system disk image from the temporary ECS.
ISO file with VirtIO drivers
ISO image
Temporary ECS
System disk image

The procedure is as follows:

1. Integrate VirtIO drivers into the ISO file.

   Windows uses Integrated Drive Electronics (IDE) disks and VirtIO NICs. Before registering an image on the cloud platform, integrate VirtIO drivers into the Windows ISO file. For details, see **Integrating VirtIO Drivers into an ISO File**.

2. Register the ISO file as an ISO image.

On the management console, register the ISO file with VirtIO drivers as an image. The image is an ISO image and cannot be used to provision ECSs. For details, see **Registering a Windows ISO File as a Private Image**.

3. Create a temporary ECS from the ISO image.

   Use the registered ISO image to create a temporary ECS. The ECS has no OS or driver installed. For details, see **Creating a Windows ECS from an ISO Image**.

4. Install an OS and necessary drivers for the temporary ECS and configure related settings.

   You need to install an OS, PV drivers, and VirtIO drivers, and configure NICs. For details, see **Installing a Windows OS and VirtIO Drivers** and **Step 1** in **Configuring the ECS and Creating a Windows System Disk Image**.

5. Create a system disk image from the temporary ECS.

   On the management console, create a system disk image from the temporary ECS on which the installation and configuration have been completed. After the image is created, delete the temporary ECS to avoid generating any additional charges. For details, see **Creating a System Disk Image from an ECS**.

Constraints

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

4.4.2 Integrating VirtIO Drivers into an ISO File

Scenarios

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

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

NOTE

- AnyBurn is lightweight CD/DVD/Blu-ray burning software with a free version.
- UltraISO is an ISO CD/DVD image file handling tool. A free trial version is limited to ISO files of 300 MB or less. You are advised to buy a standard version.
- VirtIO is a standard interface for VMs to access host devices. It is used to improve the I/O performance between VMs and hosts. For details about VirtIO, see **VirtIO**. For details about open source code of virtio-win/kvm-guest-drivers-windows, see **https://github.com/virtio-win/kvm-guest-drivers-windows**.

Prerequisites

You have obtained an ISO file.

NOTE

The ISO file name can contain only letters, digits, hyphens (-), and underscores (_).

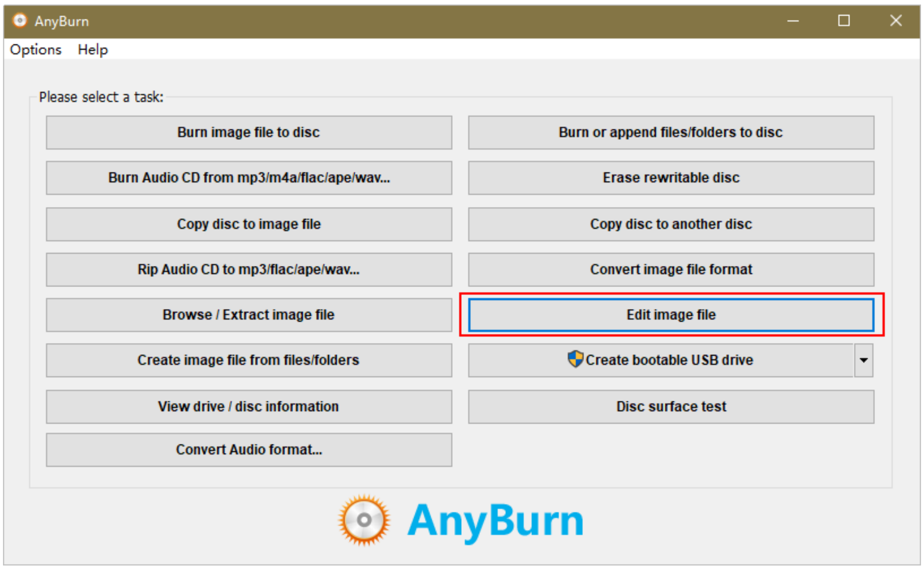
AnyBurn

1. Download **AnyBurn** and install it on your local PC.
2. Download VirtIO drivers.

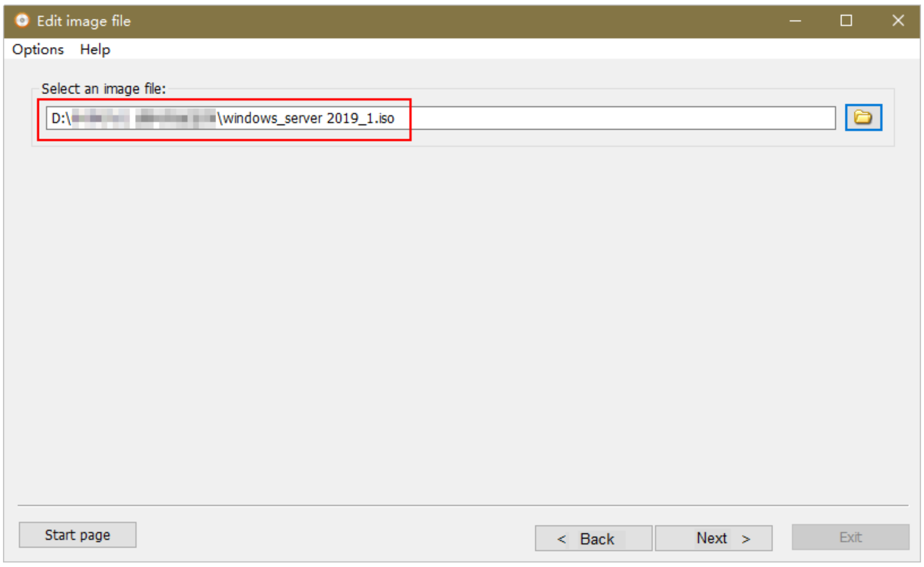
   https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtio-win.iso

   Other versions:

   https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/
3. Use AnyBurn to open the ISO file.
   a. Open AnyBurn and select **Edit Image File**.


AnyBurn
Options Help
Please select a task:
Burn image file to disc
Burn or append files/folders to disc
Burn Audio CD from mp3/m4a/flac/ape/wav...
Erase rewritable disc
Copy disc to image file
Copy disc to another disc
Rip Audio CD to mp3/flac/ape/wav...
Convert image file format
Browse / Extract image file
Edit image file
Create image file from files/folders
Create bootable USB drive
View drive / disc information
Disc surface test
Convert Audio format...
AnyBurn

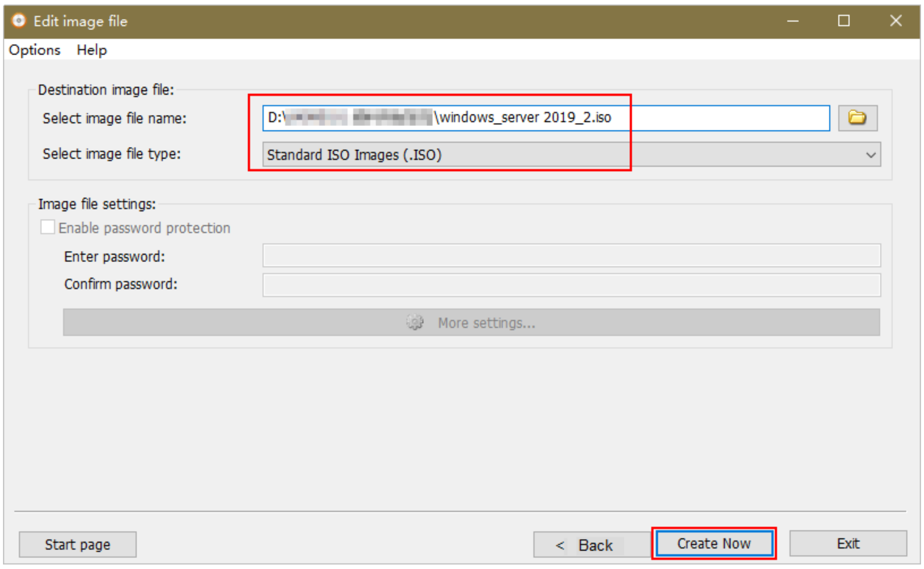
   b. Select the ISO file and click **Next**.



Select an image file: D:\[redacted]\windows_server 2019_1.iso

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

      After the new ISO file is generated, view VirtIO drivers in it.



Destination image file:

Select image file name: D:\[redacted]\windows_server 2019_2.iso

Select image file type: Standard ISO Images (.ISO)

Image file settings:

□ Enable password protection

Enter password:

Confirm password:

UltraISO

1. Download UltraISO and install it on your local PC.

   Download address: **https://www.ultraiso.com/**
2. Download VirtIO drivers.

   https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtio-win.iso

   Other versions:

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

3. Use UltraISO to open the ISO file.

⚠ CAUTION

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

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

4.4.3 Registering a Windows ISO File as a Private Image

Scenarios

Register an external ISO file on the cloud platform as a private image (ISO image). Before registering an image, ensure that the ISO file with VirtIO drivers integrated has been uploaded to an OBS bucket.

An ISO image cannot be replicated or exported.

Prerequisites

- The file to be registered must be in ISO format.
- The ISO file has been uploaded to an OBS bucket. For details, see **Upload an Image File**.

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

Step 2 Register an ISO file as an ISO image.

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

Figure 4-6 Creating a private image from an ISO file

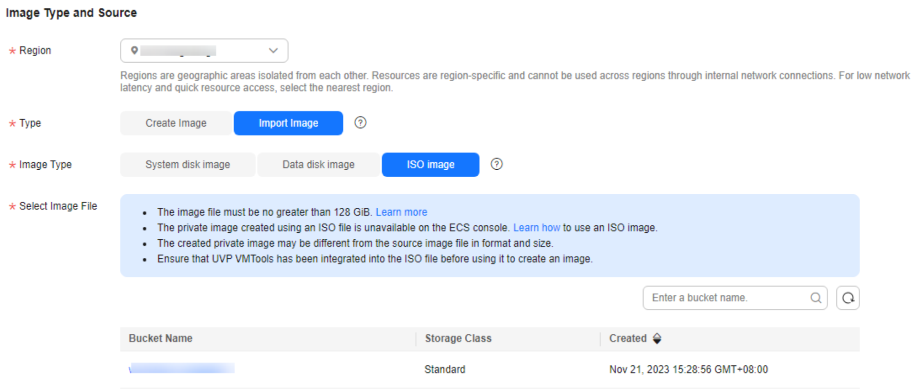


Image Type and Source

* Region [redacted]

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* Type: Create Image | **Import Image**

* Image Type: System disk image | Data disk image | **ISO image**

* Select Image File

- The image file must be no greater than 128 GiB. Learn more
- The private image created using an ISO file is unavailable on the ECS console. Learn how to use an ISO image.
- The created private image may be different from the source image file in format and size.
- Ensure that UVP VMTools has been integrated into the ISO file before using it to create an image.

Enter a bucket name.

Bucket Name	Storage Class	Created
[redacted]	Standard	Nov 21, 2023 15:28:56 GMT+08:00

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

Figure 4-7 Configuring image information

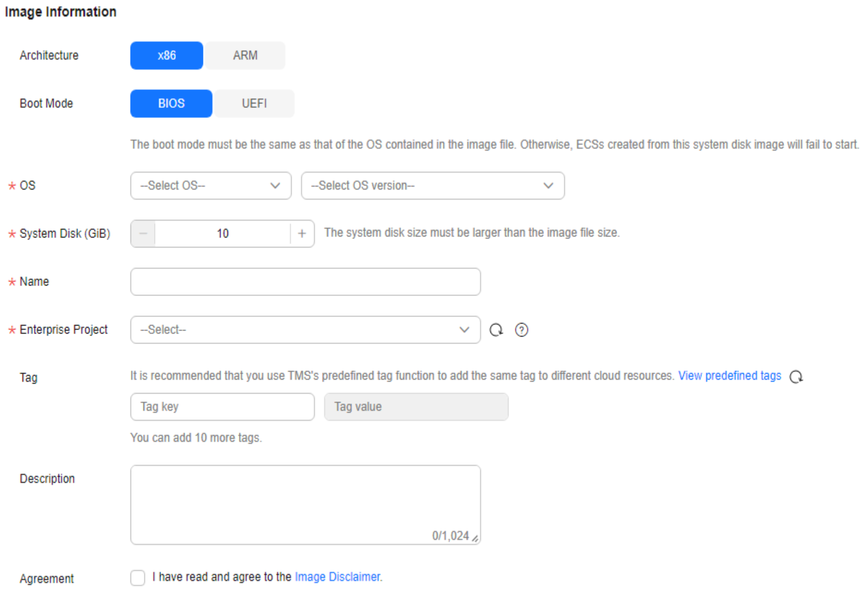


Image Information

Architecture: **x86** | ARM

Boot Mode: **BIOS** | UEFI

The boot mode must be the same as that of the OS contained in the image file. Otherwise, ECSs created from this system disk image will fail to start.

* OS: --Select OS-- | --Select OS version--

* System Disk (GiB): 10 — The system disk size must be larger than the image file size.

* Name

* Enterprise Project: --Select--

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Tag key | Tag value

You can add 10 more tags.

Description: 0/1,024

Agreement: □ I have read and agree to the Image Disclaimer.

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

  NOTE

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

- **Boot Mode**: Select **BIOS** or **UEFI**. Ensure that the selected boot mode is the same as that in the image file, or the ECSs created from this image will not be able to boot up. The Arm architecture does not support the BIOS boot mode.
- **OS**: Select the OS specified in the ISO file to ensure that the image can be created and used properly.
- **License Type**: If you have already had an OS license, you can bring your own license (BYOL) and you do not need to apply for a new license anymore This parameter is only available for Windows.

- **System Disk**: Set the system disk capacity (value range: 40 GB to 1024 GB), which must be no less than the capacity of the system disk in the image file.
- **Name**: Enter a name for the image to be created.
- **Enterprise Project**: Select the enterprise project your image belongs to.
- **Tag**: (Optional) Add a tag to the image to be created.

  NOTE

  If your organization has configured tag policies for images, you need to add tags to your images based on the policies. If you add a tag that does not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies.

  - Each tag consists of a key and a value. The key contains a maximum of 36 characters, and the value contains a maximum of 43 characters. The key cannot be left blank or an empty string. The value cannot be left blank but can be an empty string.
  - An image can have a maximum of 10 tags.
- (Optional) **Description**: Describe the image as needed.

5. Click **Next**.
6. Confirm the settings. Read and agree to the disclaimer and click **Submit**.

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

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

----End

4.4.4 Creating a Windows ECS from an ISO Image

Scenarios

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

Constraints

Dedicated Cloud (DeC) users cannot create ECSs from ISO images.

If the DeC service is enabled for a user in a specified region, the user will be a DeC user. For more information, see **What Is DeC?**

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

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

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

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

NOTE

If you are a **DeC** user, the **Create ECS** button in the **Operation** column will be unavailable for you because a DeC user cannot use an ISO image to create an ECS.

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

----End

Follow-up Procedure

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

4.4.5 Installing a Windows OS and VirtIO Drivers

Scenarios

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

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

NOTE

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

Prerequisites

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

Procedure

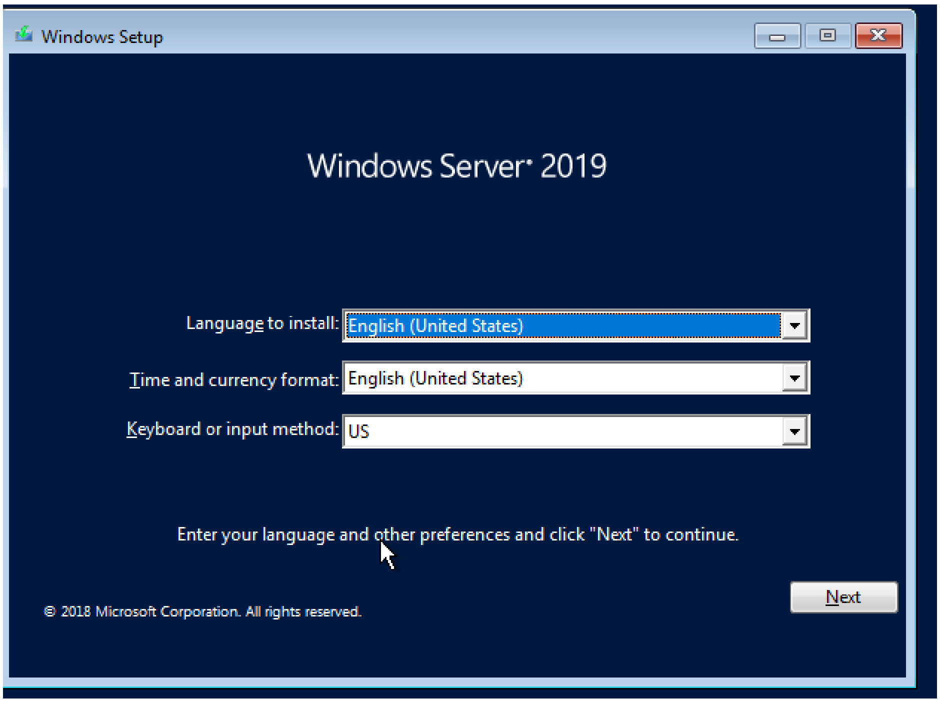
⚠ CAUTION

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

Step 1 Install the Windows OS.

1. Configure Windows setup.

Figure 4-8 Windows setup



Language to install: English (United States)

Time and currency format: English (United States)

Keyboard or input method: US

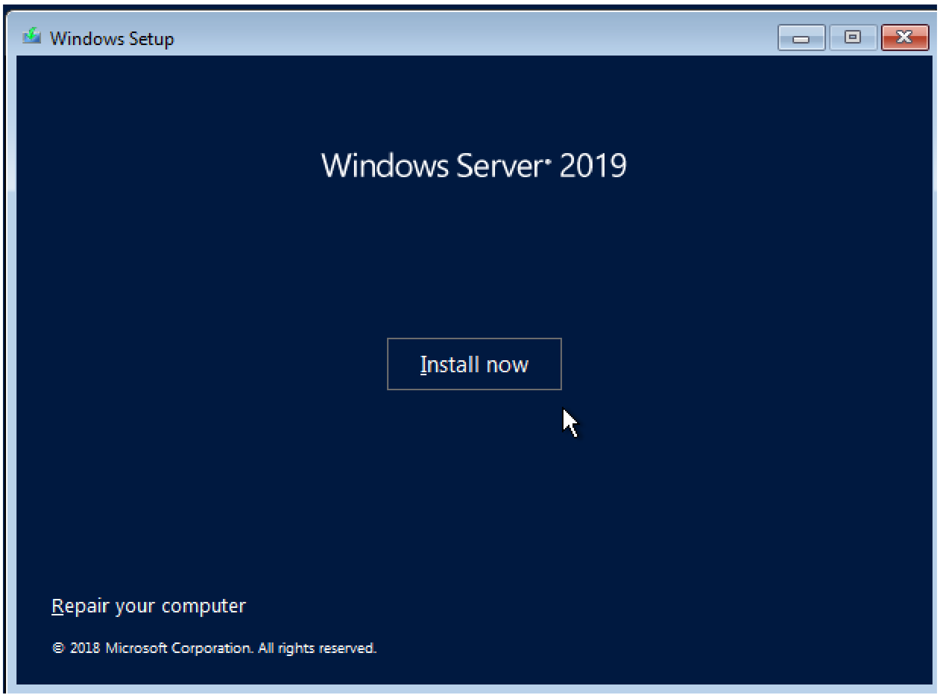
Enter your language and other preferences and click "Next" to continue.

© 2018 Microsoft Corporation. All rights reserved.

2. Click **Next**.

   The installation confirmation window is displayed.

Figure 4-9 Installation confirmation



© 2018 Microsoft Corporation. All rights reserved.

3. Click **Install now**.

   The **Select the operating system you want to install** dialog box is displayed.

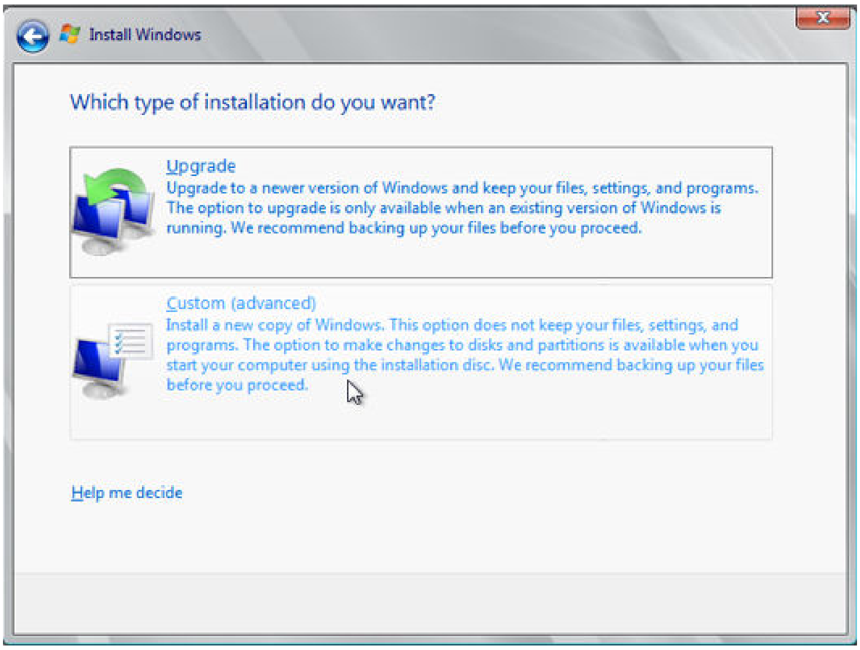
4. Select the version of the OS to be installed and click **Next**.

   The **Please read the license terms** dialog box is displayed.

5. Select **I accept the license terms**, and click **Next**.

   The **Which type of installation do you want?** dialog box is displayed.

   Figure 4-10 Installation type

   Which type of installation do you want?

   Upgrade
   Upgrade to a newer version of Windows and keep your files, settings, and programs. The option to upgrade is only available when an existing version of Windows is running. We recommend backing up your files before you proceed.

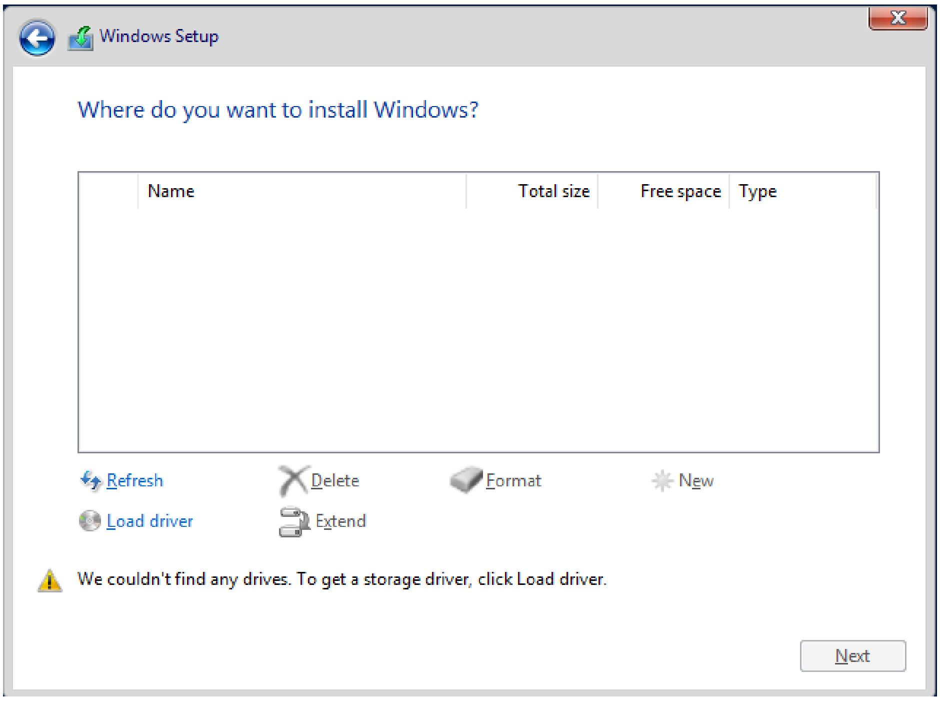
   Custom (advanced)
   Install a new copy of Windows. This option does not keep your files, settings, and programs. The option to make changes to disks and partitions is available when you start your computer using the installation disc. We recommend backing up your files before you proceed.

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

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

   – If the system displays a message indicating that no driver is found, go to **Step 1.7**.

   Figure 4-11 Installation path

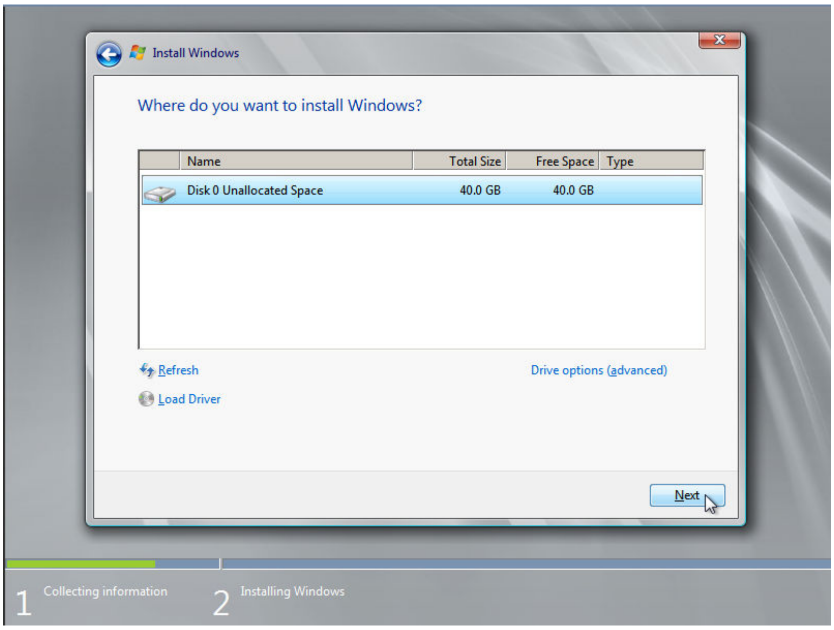
   Where do you want to install Windows?

Name	Total size	Free space	Type

   We couldn't find any drives. To get a storage driver, click Load driver.

- If a disk is displayed, go to **Step 1.9**.

Figure 4-12 Installation path



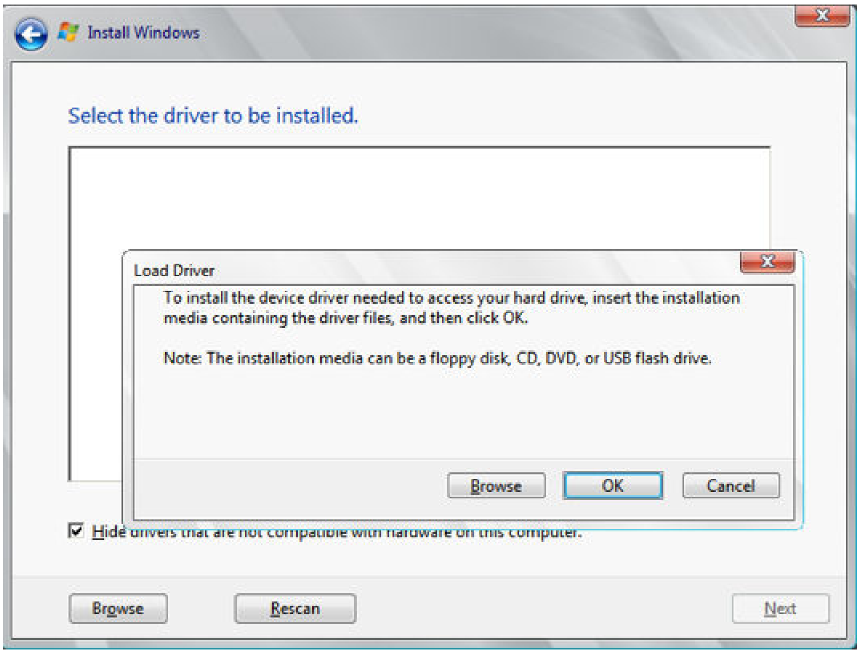
Install Windows

Where do you want to install Windows?

Name	Total Size	Free Space	Type
Disk 0 Unallocated Space	40.0 GB	40.0 GB	

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

Figure 4-13 Loading drivers



Install Windows

Select the driver to be installed.

Load Driver

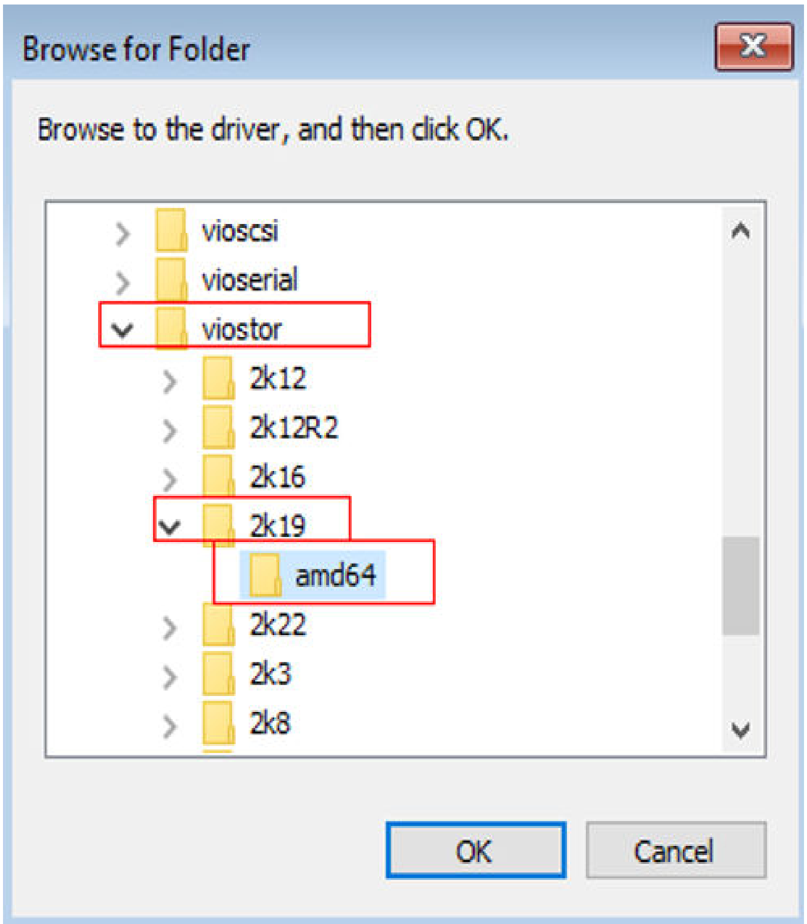
To install the device driver needed to access your hard drive, insert the installation media containing the driver files, and then click OK.

Note: The installation media can be a floppy disk, CD, DVD, or USB flash drive.

☑ Hide drivers that are not compatible with hardware on this computer.

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

Figure 4-14 Browsing for a folder

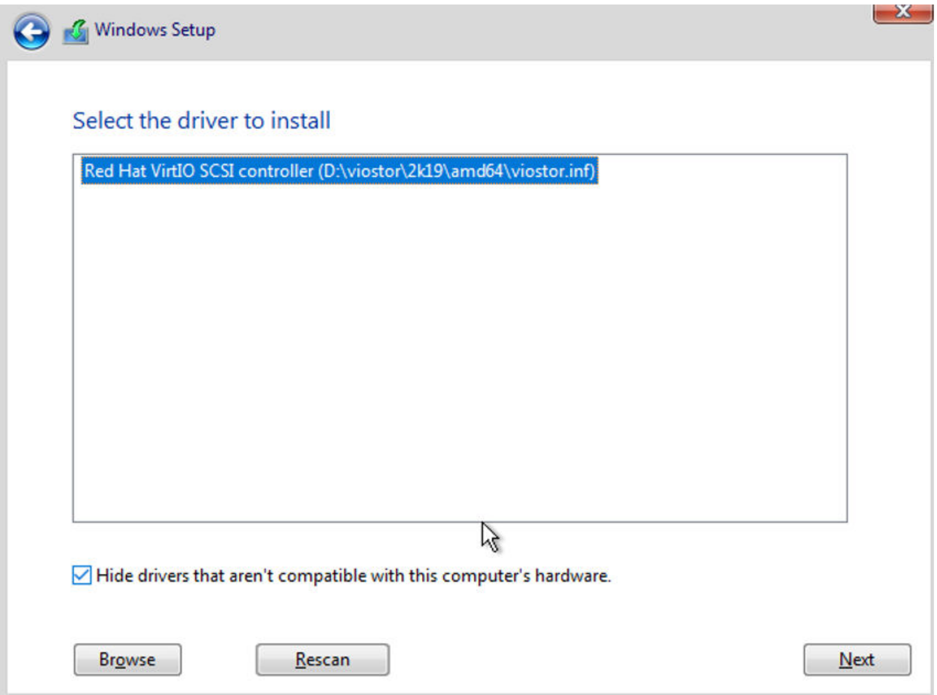


Browse for Folder

Browse to the driver, and then click OK.

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

Figure 4-15 Selecting the driver to install



Windows Setup

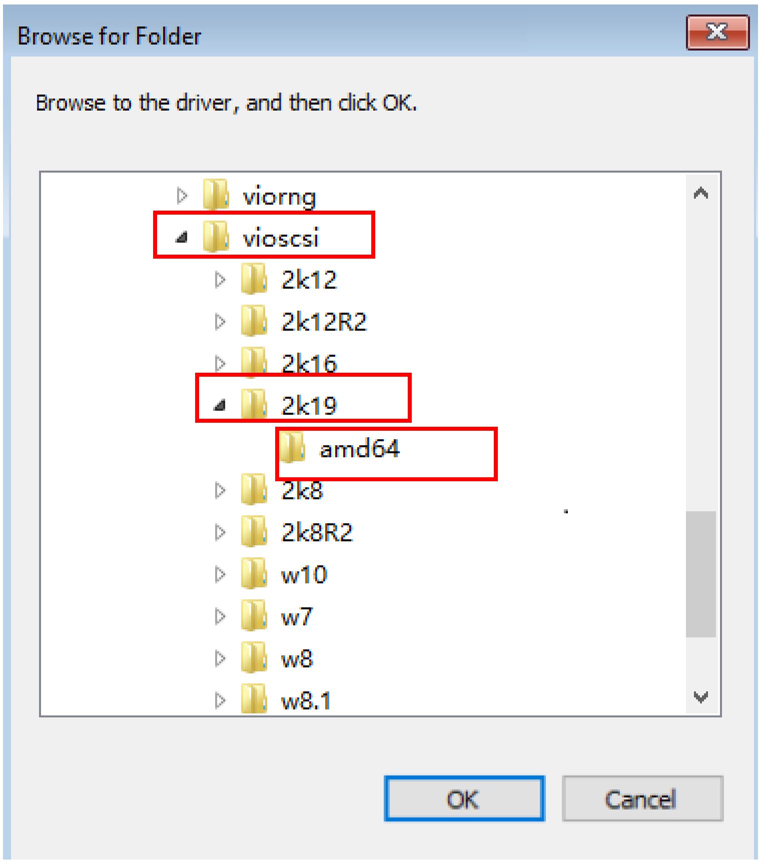
Select the driver to install

Red Hat VirtIO SCSI controller (D:\viostor\2k19\amd64\viostor.inf)

☑ Hide drivers that aren't compatible with this computer's hardware.

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

Figure 4-16 Browsing for a folder

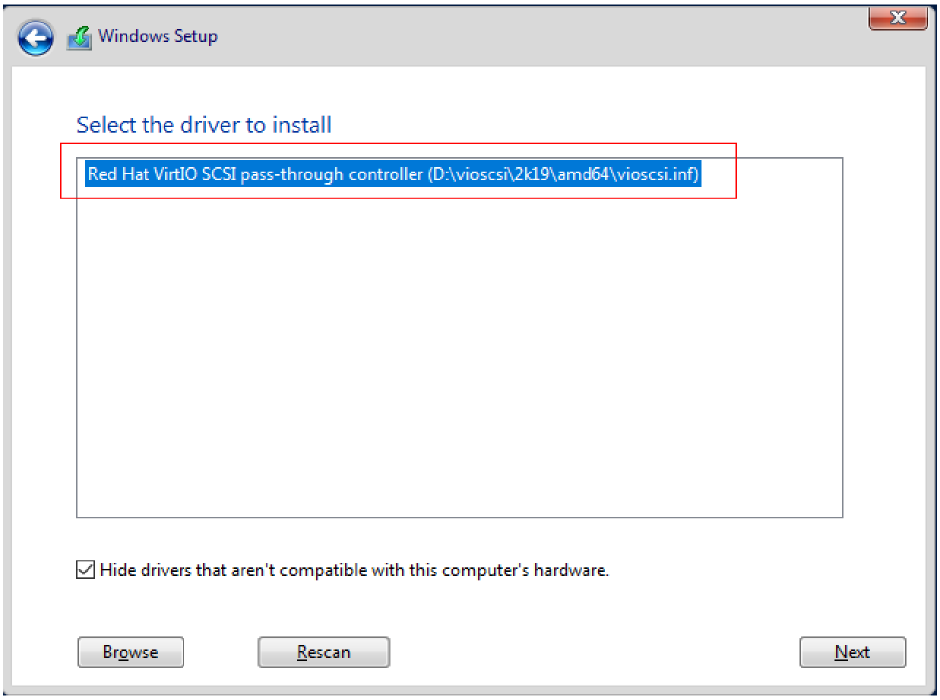


Browse for Folder

Browse to the driver, and then click OK.

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

Figure 4-17 Selecting the driver to install



Windows Setup

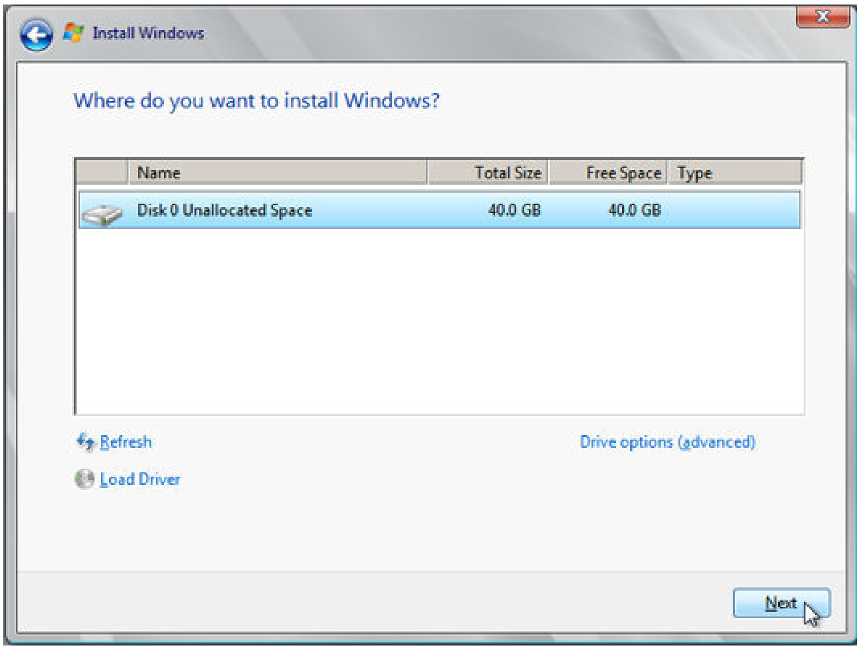
Select the driver to install

Red Hat VirtIO SCSI pass-through controller (D:\vioscsi\2k19\amd64\vioscsi.inf)

☑ Hide drivers that aren't compatible with this computer's hardware.

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

Figure 4-18 Installation path



Install Windows

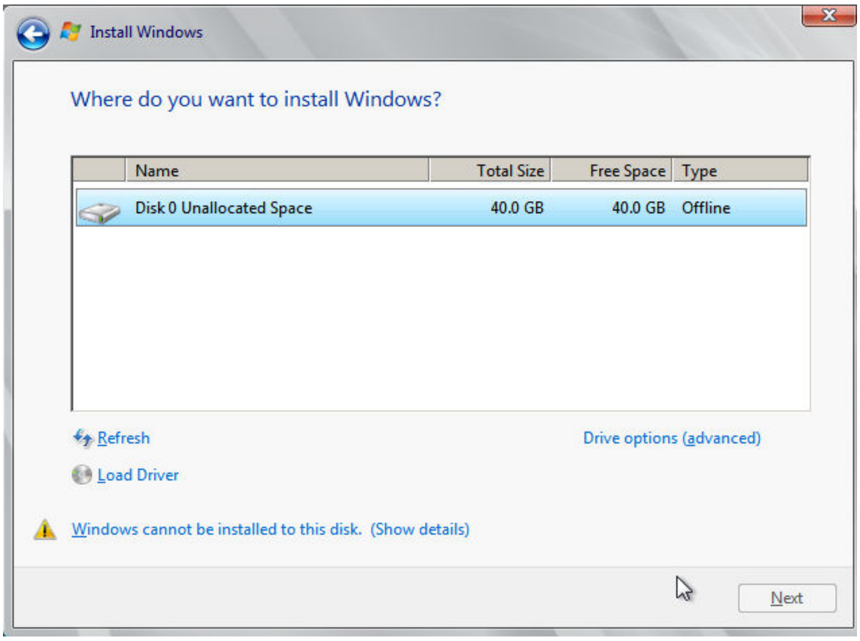
Where do you want to install Windows?

	Name	Total Size	Free Space	Type
	Disk 0 Unallocated Space	40.0 GB	40.0 GB	

NOTE

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

Figure 4-19 Offline disk



Where do you want to install Windows?

Name	Total Size	Free Space	Type
Disk 0 Unallocated Space	40.0 GB	40.0 GB	Offline

Windows cannot be installed to this disk. (Show details)

10. The **Installing Windows** dialog box is displayed, and the OS installation starts.

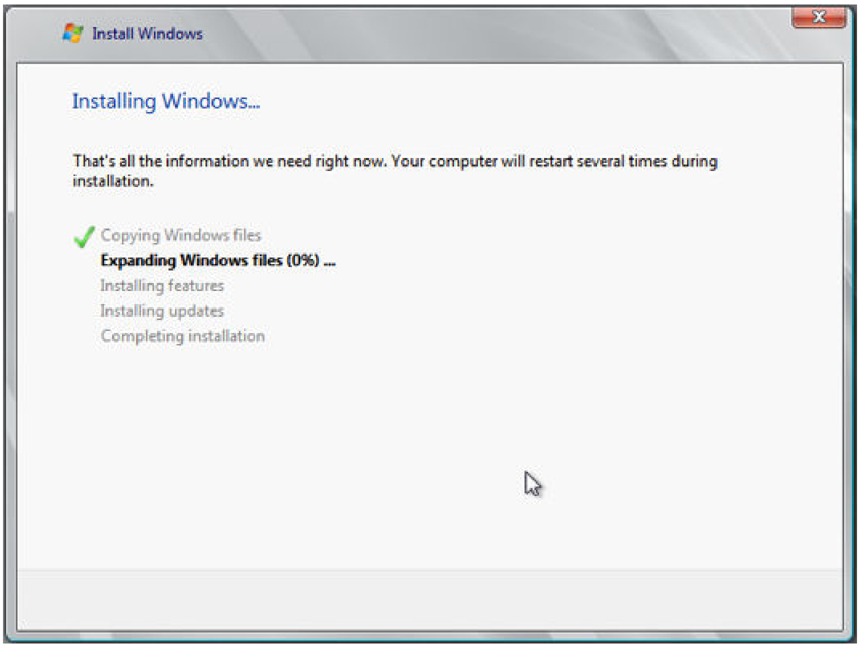
    The installation takes about 50 minutes. The ECS restarts during the installation. After the ECS successfully restarts, log in to it again and configure the OS as prompted.

    NOTE

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

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

Figure 4-20 Installation progress



Installing Windows...

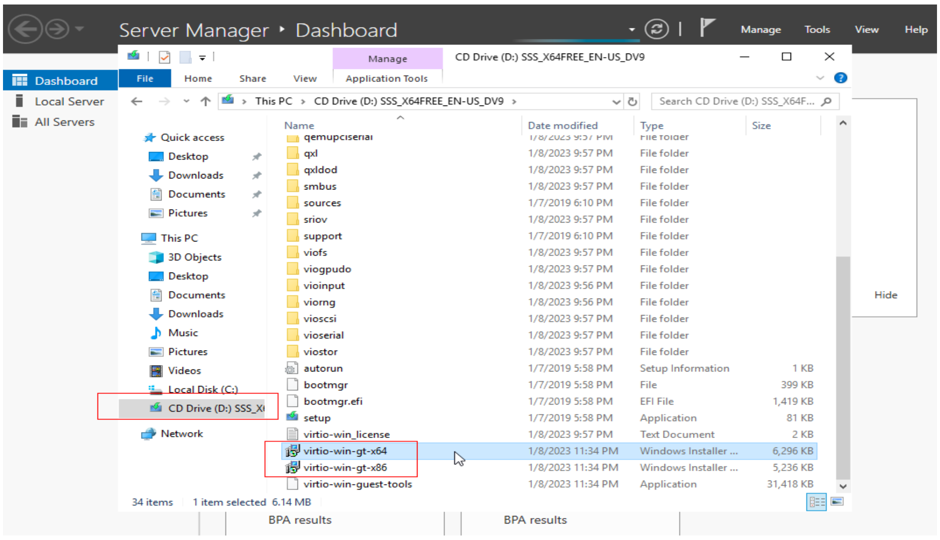
That's all the information we need right now. Your computer will restart several times during installation.

✓ Copying Windows files
Expanding Windows files (0%) ...
Installing features
Installing updates
Completing installation

Step 2 Install drivers.

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

Figure 4-21 Starting the CD drive

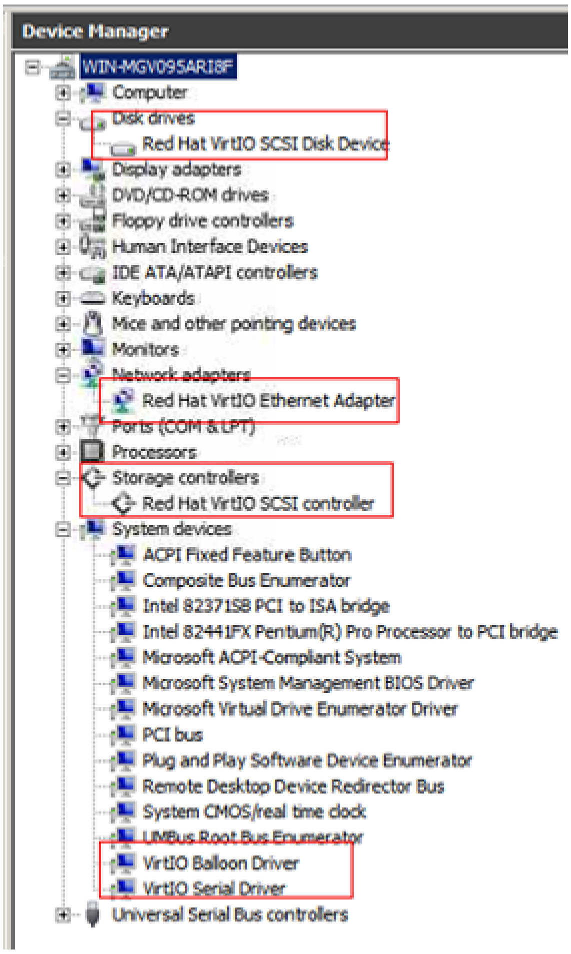


Name	Date modified	Type	Size
qemupciserial	1/8/2023 9:57 PM	File folder	
qxl	1/8/2023 9:57 PM	File folder	
qxldod	1/8/2023 9:57 PM	File folder	
smbus	1/8/2023 9:57 PM	File folder	
sources	1/7/2019 6:10 PM	File folder	
sriov	1/8/2023 9:57 PM	File folder	
support	1/7/2019 6:10 PM	File folder	
viofs	1/8/2023 9:57 PM	File folder	
viogpudo	1/8/2023 9:57 PM	File folder	
vioinput	1/8/2023 9:56 PM	File folder	
viorng	1/8/2023 9:56 PM	File folder	
vioscsi	1/8/2023 9:57 PM	File folder	
vioserial	1/8/2023 9:57 PM	File folder	
viostor	1/8/2023 9:57 PM	File folder	
autorun	1/7/2019 5:58 PM	Setup Information	1 KB
bootmgr	1/7/2019 5:58 PM	File	399 KB
bootmgr.efi	1/7/2019 5:58 PM	EFI File	1,419 KB
setup	1/7/2019 5:58 PM	Application	81 KB
virtio-win_license	1/8/2023 9:57 PM	Text Document	2 KB
virtio-win-gt-x64	1/8/2023 11:34 PM	Windows Installer ...	6,296 KB
virtio-win-gt-x86	1/8/2023 11:34 PM	Windows Installer ...	5,236 KB
virtio-win-guest-tools	1/8/2023 11:34 PM	Application	31,418 KB

34 items 1 item selected 6.14 MB

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

Figure 4-22 Device Manager



Device Manager

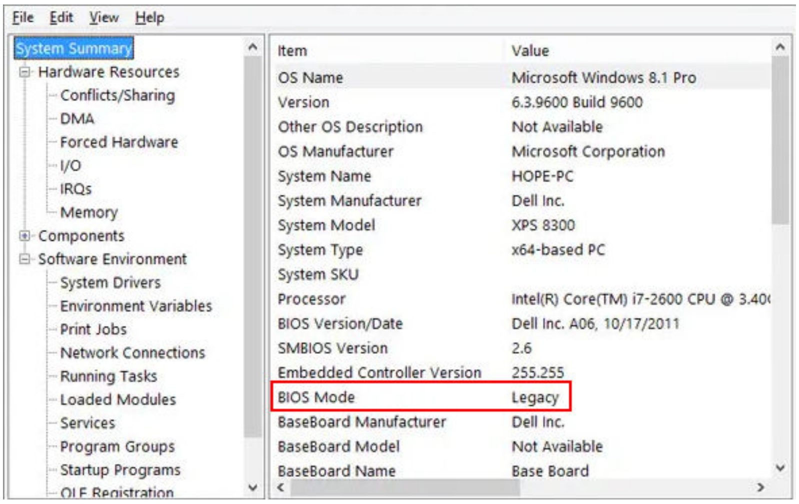
- WIN-MGV095ARI8F
  - Computer
  - Disk drives
    - Red Hat VirtIO SCSI Disk Device
  - Display adapters
  - DVD/CD-ROM drives
  - Floppy drive controllers
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
    - Red Hat VirtIO Ethernet Adapter
  - Ports (COM & LPT)
  - Processors
  - Storage controllers
    - Red Hat VirtIO SCSI controller
  - System devices
    - ACPI Fixed Feature Button
    - Composite Bus Enumerator
    - Intel 82371SB PCI to ISA bridge
    - Intel 82441FX Pentium(R) Pro Processor to PCI bridge
    - Microsoft ACPI-Compliant System
    - Microsoft System Management BIOS Driver
    - Microsoft Virtual Drive Enumerator Driver
    - PCI bus
    - Plug and Play Software Device Enumerator
    - Remote Desktop Device Redirector Bus
    - System CMOS/real time clock
    - UMBus Root Bus Enumerator
    - VirtIO Balloon Driver
    - VirtIO Serial Driver
  - Universal Serial Bus controllers

----End

Follow-up Procedure

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

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



Item	Value
OS Name	Microsoft Windows 8.1 Pro
Version	6.3.9600 Build 9600
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	HOPE-PC
System Manufacturer	Dell Inc.
System Model	XPS 8300
System Type	x64-based PC
System SKU	
Processor	Intel(R) Core(TM) i7-2600 CPU @ 3.40
BIOS Version/Date	Dell Inc. A06, 10/17/2011
SMBIOS Version	2.6
Embedded Controller Version	255.255
BIOS Mode	Legacy
BaseBoard Manufacturer	Dell Inc.
BaseBoard Model	Not Available
BaseBoard Name	Base Board

- If the value of **BIOS Mode** is **Legacy**, the system boot mode is BIOS. Go to the step for **configuring image information**, select **BIOS** for **Boot Mode**.
- If the value of **BIOS Mode** is **UEFI**, address the resolution change failure by referring to **What Do I Do If I Cannot Change the Resolution of a Windows OS Booted in UEFI Mode?**

4.4.6 Configuring the ECS and Creating a Windows System Disk Image

Scenarios

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

NOTE

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

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

Procedure

Step 1 Configure the ECS.

1. Check whether DHCP is configured. If the ECS is configured with a static IP address, change its IP address assignment mode to DHCP as instructed in **Configuring DHCP**.
2. Enable remote desktop connection for the ECS as needed. For details about how to enable this function, see **Enabling Remote Desktop Connection**.
3. To install PV drivers, see **Installing PV Drivers**.

   After the installation is complete, you need to delete system logs. For details, see **Clearing System Logs**.
4. Install and configure Cloudbase-Init. User data injection on the management console is available for the new ECSs created from the image only after this

tool is installed. For example, you can use data injection to set the login password for a new ECS. For details, see **Installing and Configuring Cloudbase-Init**.

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

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

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

For details, see **Creating a System Disk Image from an ECS**.

----End

Follow-up Procedure

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

4.5 Creating a Linux System Disk Image from an ISO File

4.5.1 Overview

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

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

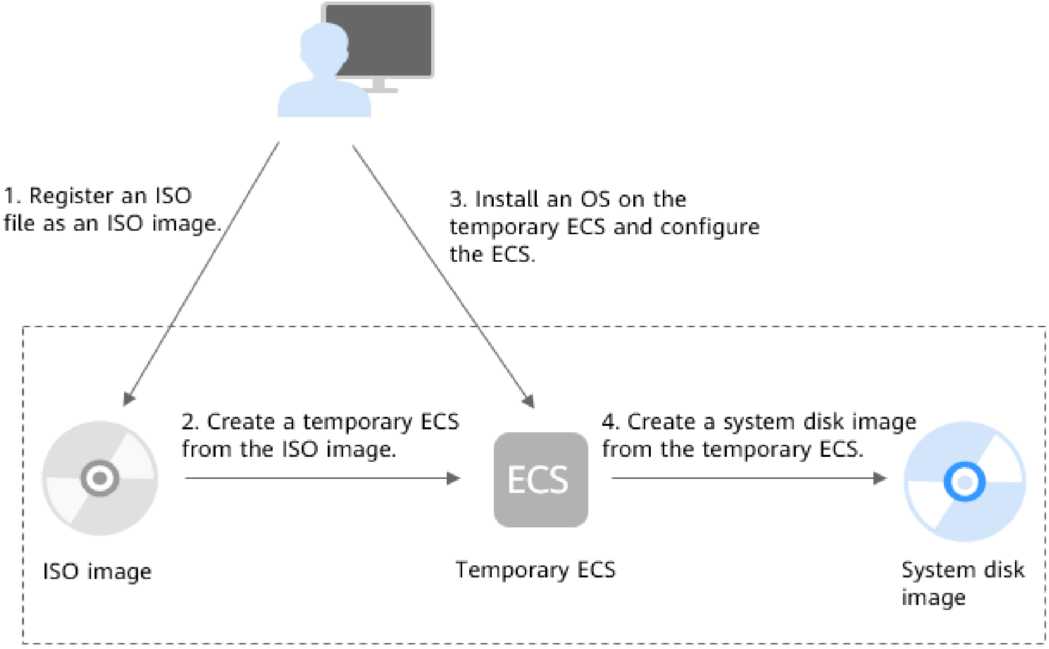
NOTE

This section is applicable only to the management console. If you are an API user, see **Creating an Image from an ISO File**.

Creation Process

Figure 4-23 shows the process of creating a Linux system disk image from an ISO file.

Figure 4-23 Creating a Linux system disk image


1. Register an ISO file as an ISO image.
3. Install an OS on the temporary ECS and configure the ECS.
2. Create a temporary ECS from the ISO image.
ECS
4. Create a system disk image from the temporary ECS.
ISO image
Temporary ECS
System disk image

The procedure is as follows:

1. Register an ISO file as an ISO image.

   On the management console, register the prepared ISO file as an image. The image is an ISO image and cannot be used to provision ECSs. For details, see **Registering a Linux ISO File as a Private Image**.

2. Create a temporary ECS from the ISO image.

   Use the registered ISO image to create a temporary ECS. The ECS has no OS or driver installed. For details, see **Creating a Linux ECS from an ISO Image**.

3. Install an OS and necessary drivers for the temporary ECS and configure related settings.

   The operations include installing an OS, installing native Xen and KVM drivers, configuring NICs, and deleting files from the network rule directory. For details, see **Installing a Linux OS** and **Step 1** in **Configuring the ECS and Creating a Linux System Disk Image**.

4. Create a system disk image from the temporary ECS.

   On the management console, create a system disk image from the temporary ECS on which the installation and configuration have been completed. After the image is created, delete the temporary ECS to avoid generating any additional charges. For details, see **Creating a System Disk Image from an ECS**.

Constraints

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

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

4.5.2 Registering a Linux ISO File as a Private Image

Scenarios

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

An ISO image cannot be replicated or exported.

Prerequisites

- The file to be registered must be in ISO format.
- The ISO image file has been uploaded to the OBS bucket. For details, see **Upload an Image File**.

  NOTE

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

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

Step 2 Register an ISO file as an ISO image.

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

Figure 4-24 Creating a private image from an ISO file

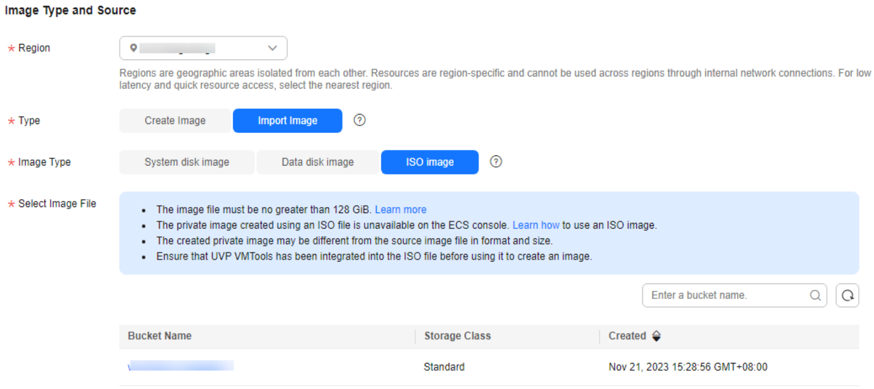


Image Type and Source

* Region [redacted]

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* Type: Create Image | Import Image

* Image Type: System disk image | Data disk image | ISO image

* Select Image File

- The image file must be no greater than 128 GiB. Learn more
- The private image created using an ISO file is unavailable on the ECS console. Learn how to use an ISO image.
- The created private image may be different from the source image file in format and size.
- Ensure that UVP VMTools has been integrated into the ISO file before using it to create an image.

Enter a bucket name.

Bucket Name	Storage Class	Created
[redacted]	Standard	Nov 21, 2023 15:28:56 GMT+08:00

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

Figure 4-25 Configuring image information

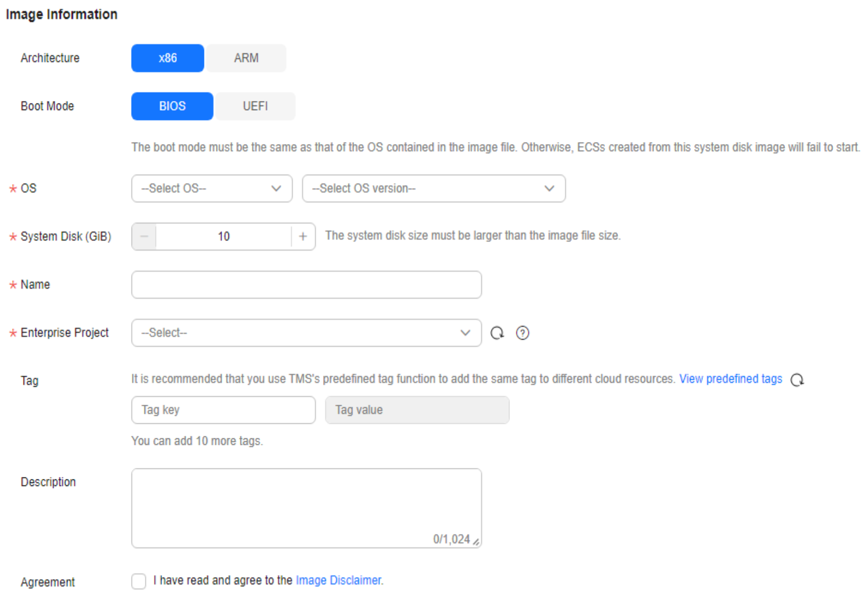


Image Information

Architecture: x86 | ARM

Boot Mode: BIOS | UEFI

The boot mode must be the same as that of the OS contained in the image file. Otherwise, ECSs created from this system disk image will fail to start.

* OS: --Select OS-- | --Select OS version--

* System Disk (GiB): − 10 + The system disk size must be larger than the image file size.

* Name:

* Enterprise Project: --Select--

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Tag key | Tag value

You can add 10 more tags.

Description: 0/1,024

Agreement: □ I have read and agree to the Image Disclaimer.

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

  NOTE

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

- **Boot Mode**: Select **BIOS** or **UEFI**. Ensure that the selected boot mode is the same as that in the image file, or the ECSs created from this image will not be able to boot up. The Arm architecture does not support the BIOS boot mode.
- **OS**: Select the OS specified in the ISO file to ensure that the image can be created and used properly.
- **License Type**: If you have already had an OS license, you can bring your own license (BYOL) and you do not need to apply for a new license anymore This parameter is only available for Windows.
- **System Disk**: Set the system disk capacity (value range: 40 GB to 1024 GB), which must be no less than the capacity of the system disk in the image file.
- **Name**: Enter a name for the image to be created.
- **Enterprise Project**: Select the enterprise project your image belongs to.
- **Tag**: (Optional) Add a tag to the image to be created.

NOTE

If your organization has configured tag policies for images, you need to add tags to your images based on the policies. If you add a tag that does not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies.

- Each tag consists of a key and a value. The key contains a maximum of 36 characters, and the value contains a maximum of 43 characters. The key cannot be left blank or an empty string. The value cannot be left blank but can be an empty string.
- An image can have a maximum of 10 tags.

– (Optional) **Description**: Describe the image as needed.

5. Click **Next**.
6. Confirm the settings. Read and agree to the disclaimer and click **Submit**.

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

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

----End

4.5.3 Creating a Linux ECS from an ISO Image

Scenarios

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

Constraints

Dedicated Cloud (DeC) users cannot create ECSs from ISO images.

If the DeC service is enabled for a user in a specified region, the user will be a DeC user. For more information, see **What Is DeC?**

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

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

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

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

NOTE

If you are a **DeC** user, the **Create ECS** button in the **Operation** column will be unavailable for you because a DeC user cannot use an ISO image to create an ECS.

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

----End

Follow-up Procedure

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

4.5.4 Installing a Linux OS

Scenarios

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

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

NOTE

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

Prerequisites

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

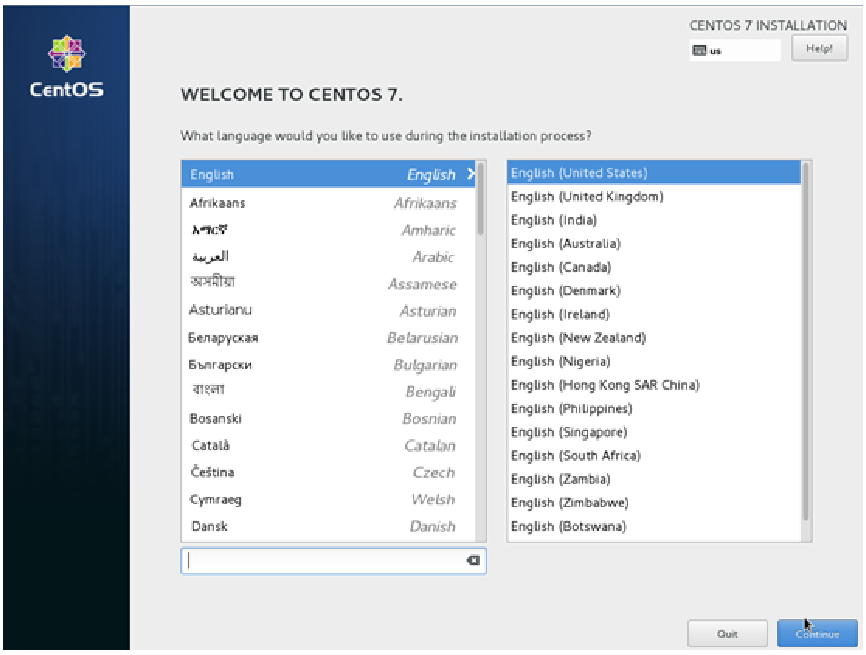
Procedure

CAUTION

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

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

Figure 4-26 Installation page



CENTOS 7 INSTALLATION

us

Help!

WELCOME TO CENTOS 7.

What language would you like to use during the installation process?

English	English
Afrikaans	Afrikaans
አማርኛ	Amharic
العربية	Arabic
অসমীয়া	Assamese
Asturianu	Asturian
Беларуская	Belarusian
Български	Bulgarian
বাংলা	Bengali
Bosanski	Bosnian
Català	Catalan
Čeština	Czech
Cymraeg	Welsh
Dansk	Danish

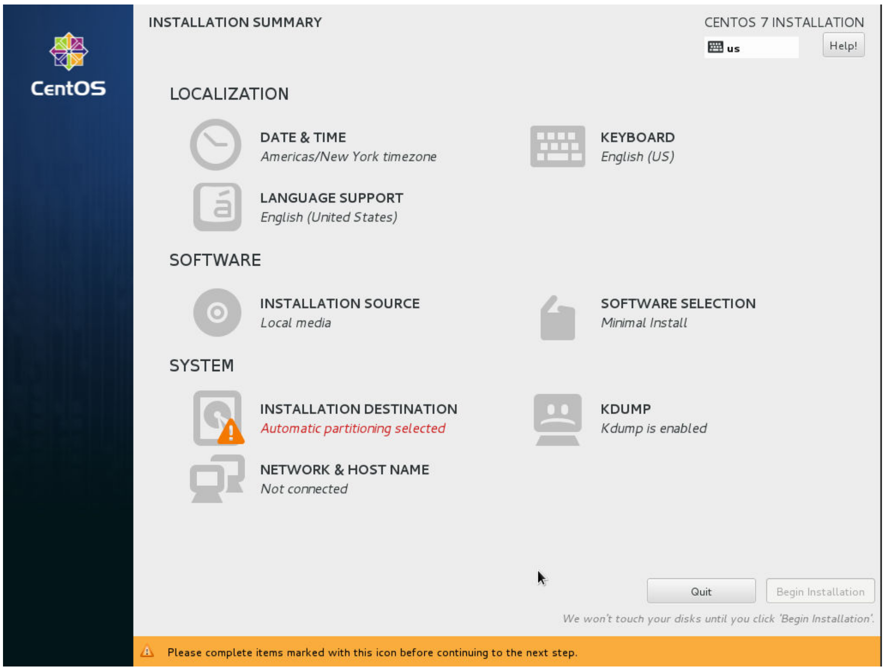
English (United States)
English (United Kingdom)
English (India)
English (Australia)
English (Canada)
English (Denmark)
English (Ireland)
English (New Zealand)
English (Nigeria)
English (Hong Kong SAR China)
English (Philippines)
English (Singapore)
English (South Africa)
English (Zambia)
English (Zimbabwe)
English (Botswana)

Quit

Continue

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

Figure 4-27 INSTALLATION SUMMARY page



INSTALLATION SUMMARY

CENTOS 7 INSTALLATION

us

Help!

LOCALIZATION

DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Minimal Install

SYSTEM

INSTALLATION DESTINATION
Automatic partitioning selected

KDUMP
Kdump is enabled

NETWORK & HOST NAME
Not connected

Quit

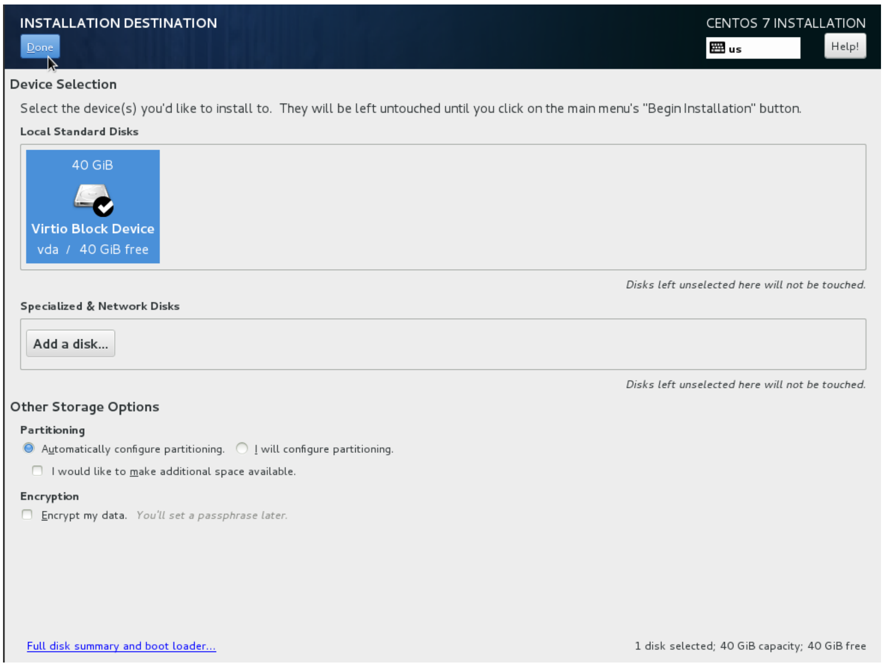
Begin Installation

We won't touch your disks until you click 'Begin Installation'.

Please complete items marked with this icon before continuing to the next step.

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

Figure 4-28 Installation location



Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

40 GiB
Virtio Block Device
vda / 40 GiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Disks left unselected here will not be touched.

Other Storage Options

Partitioning

● Automatically configure partitioning. ○ I will configure partitioning.

□ I would like to make additional space available.

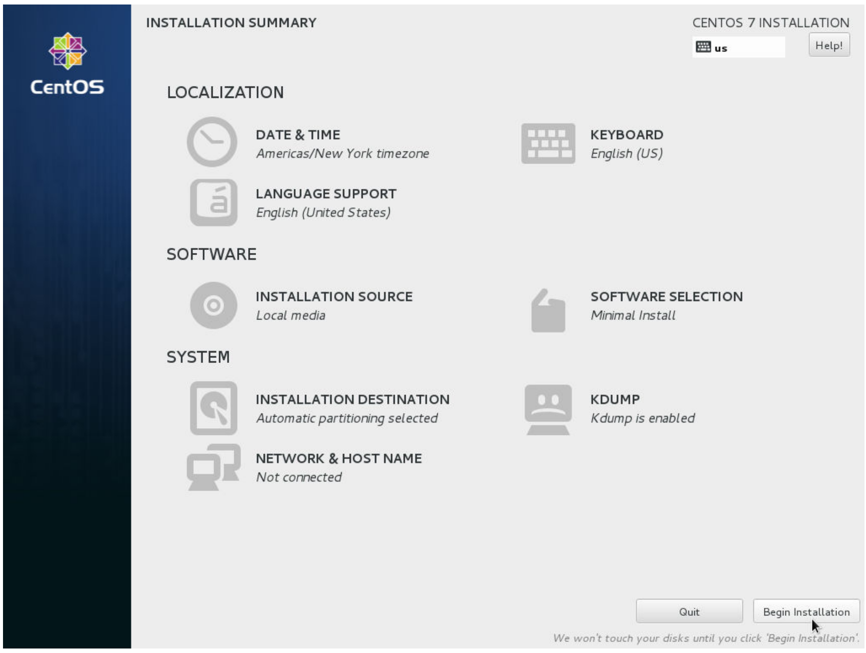
Encryption

□ Encrypt my data. *You'll set a passphrase later.*

1 disk selected; 40 GiB capacity; 40 GiB free

4. Click **Begin Installation**.

Figure 4-29 Starting installation



DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Minimal Install

INSTALLATION DESTINATION
Automatic partitioning selected

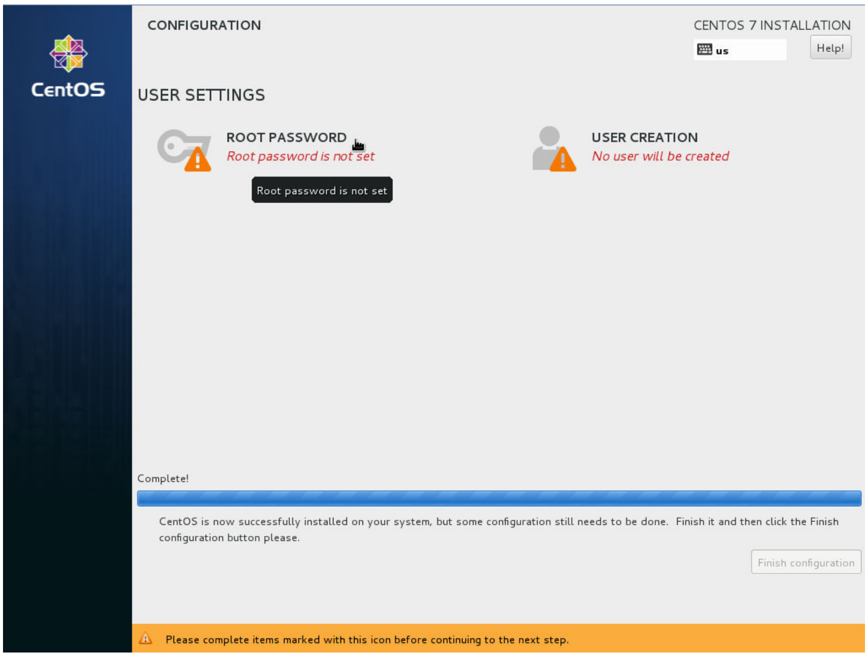
KDUMP
Kdump is enabled

NETWORK & HOST NAME
Not connected

We won't touch your disks until you click 'Begin Installation'.

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

Figure 4-30 Successful installation



Root password is not set

Root password is not set

No user will be created

Complete!

CentOS is now successfully installed on your system, but some configuration still needs to be done. Finish it and then click the Finish configuration button please.

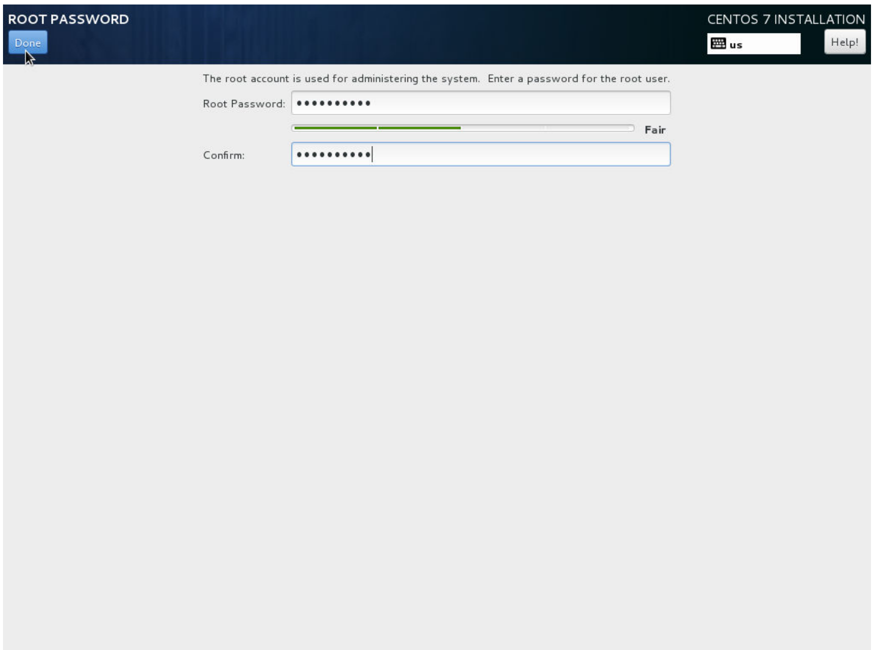
Please complete items marked with this icon before continuing to the next step.

6. In the **USER SETTINGS** area, click **ROOT PASSWORD**.

   The **ROOT PASSWORD** page is displayed.

7. Set a password for user **root** as prompted and click **Done**.

Figure 4-31 Setting a password for user root



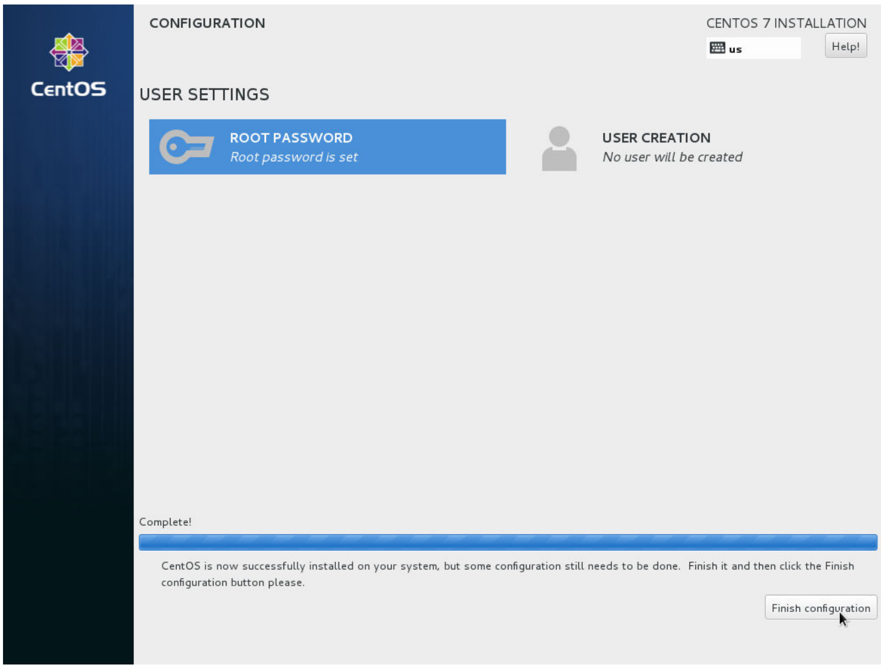
The root account is used for administering the system. Enter a password for the root user.

Root Password: ••••••••••

Confirm: ••••••••••

8. Click **Finish configuration**.

Figure 4-32 Completing configuration



CONFIGURATION

CENTOS 7 INSTALLATION

USER SETTINGS

ROOT PASSWORD
Root password is set

USER CREATION
No user will be created

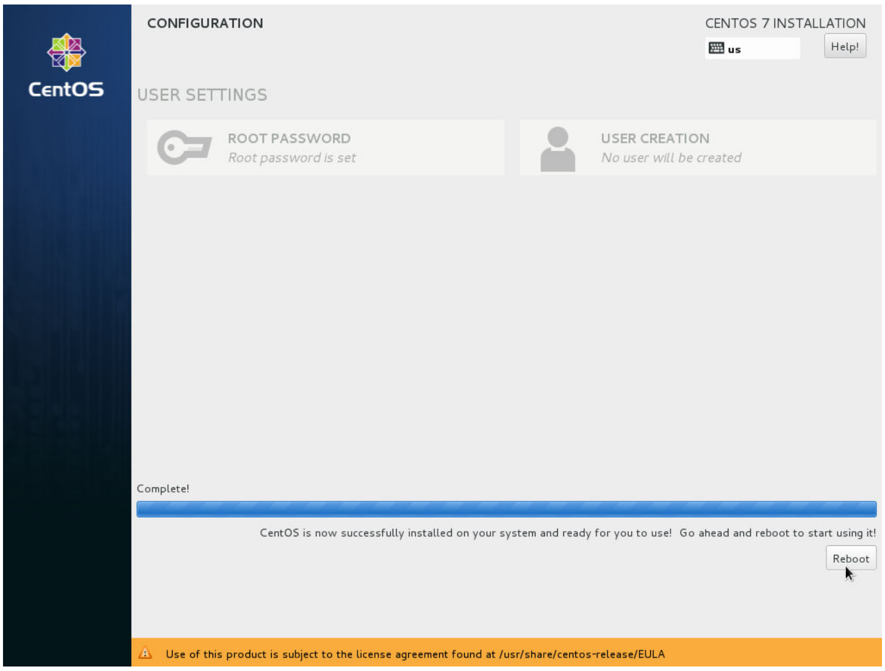
Complete!

CentOS is now successfully installed on your system, but some configuration still needs to be done. Finish it and then click the Finish configuration button please.

9. Click **Reboot**.

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

Figure 4-33 Restarting the ECS



CONFIGURATION

CENTOS 7 INSTALLATION

USER SETTINGS

ROOT PASSWORD
Root password is set

USER CREATION
No user will be created

Complete!

CentOS is now successfully installed on your system and ready for you to use! Go ahead and reboot to start using it!

Use of this product is subject to the license agreement found at /usr/share/centos-release/EULA

4.5.5 Configuring the ECS and Creating a Linux System Disk Image

Scenarios

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

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

Procedure

Step 1 Configure the ECS.

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

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

   NOTE

   Disable your antivirus and intrusion detection software. You can enable them after the driver installation is complete.

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

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

Step 2 Create a Linux system disk image.

For details, see **Creating a System Disk Image from an ECS**.

----End

Follow-up Procedure

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

4.6 Fast Import of an Image File

4.6.1 Overview

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

Constraints

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

Methods

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

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

    ii. Convert the image file format to ZVHD2.
    iii. Upload the image file to an OBS bucket.
    iv. Register the image file on the cloud platform.

  - If the file format is converted to RAW:

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

NOTE

- Fast import is used to quickly import large files. It depends on lazy loading which defers loading of file data until the data is needed. This reduces the initial loading time. However, RAW files do not support lazy loading. When you upload a RAW file, you need to upload its bitmap together.
- For details about the initial configuration required for an image file, see **Table 2-2**. Perform the configuration based on the OS in the image file.

Import Process

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

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

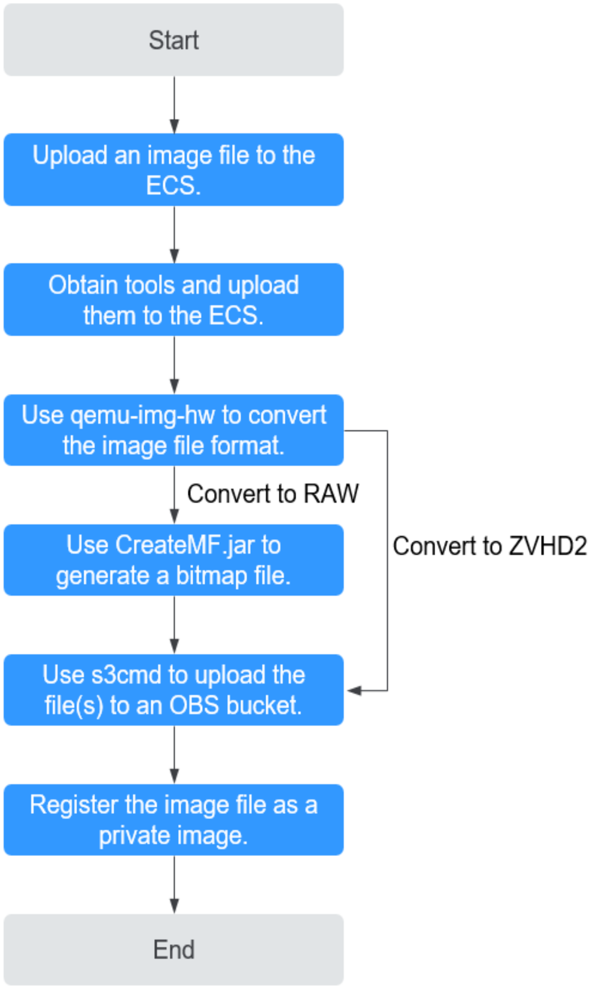
NOTE

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

- Linux

  You are advised to use a EulerOS ECS to convert the file format.

Figure 4-34 Import process (Linux)


Start
Upload an image file to the ECS.
Obtain tools and upload them to the ECS.
Use qemu-img-hw to convert the image file format.
Convert to RAW
Convert to ZVHD2
Use CreateMF.jar to generate a bitmap file.
Use s3cmd to upload the file(s) to an OBS bucket.
Register the image file as a private image.
End

For details, see **Fast Import of an Image File in Linux**.

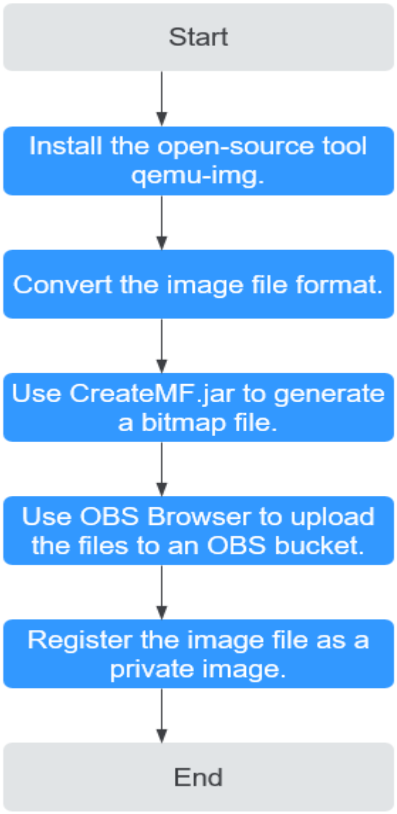
- Windows

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

  NOTE

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

Figure 4-35 Import process (Windows)


Start
Install the open-source tool qemu-img.
Convert the image file format.
Use CreateMF.jar to generate a bitmap file.
Use OBS Browser to upload the files to an OBS bucket.
Register the image file as a private image.
End

For details, see **Fast Import of an Image File in Windows**.

4.6.2 Fast Import of an Image File in Linux

Scenarios

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

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

Prerequisites

- The image file has been initially configured as instructed in **Table 2-2** based on the OS in the image file.
- You have created an ECS running EulerOS on the management console and bound an EIP to the ECS.
- An OBS bucket has been created on the management console.

Procedure

Step 1 Upload an image file.

- If the image file is uploaded from a Linux PC, run the **scp** command.

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

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

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

- If the image file is uploaded from a Windows PC, use a file transfer tool, such as WinSCP, to upload the image file.

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

Table 4-4 Tool packages

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

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

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

   cd /usr/qemu-img-hw

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

   chmod +x qemu-img-hw

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

   Command format:

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

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

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

   – If the image file is converted to the ZVHD2 format, go to **Step 5**.

   – If the image file is converted to the RAW format, go to **Step 4**.

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

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

   Run the following commands to check whether JDK is installed:

   source /etc/profile

   java -version

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

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

   cd /usr/createMF

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

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

   Example:

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

   ⚠ CAUTION

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

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

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

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

   a. Run the following command to install setuptools:

      yum install python-setuptools

   b. Run the following command to install wget:

      yum install wget

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

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

      mv master.zip s3cmd-master.zip

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

      unzip s3cmd-master.zip

      cd s3cmd-master

      python setup.py install

2. Configure **s3cmd**.

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

```
s3cmd --configure
Access Key: Enter an AK.
Secret Key: Enter an SK.
Default Region: Enter the region where the bucket is located.
S3 Endpoint: Refer to the OBS endpoint.
DNS-style bucket+hostname:port template for accessing a bucket: Enter a server address with a
bucket name, for example, mybucket.obs.myclouds.com.
Encryption password: Press Enter.
Path to GPG program: Press Enter.
Use HTTPS protocol: Specifies whether to use HTTPS. The value can be Yes or No.
HTTP Proxy server name: Specifies the proxy address used to connect the cloud from an external
network. (If you do not need it, press Enter.)
HTTP Proxy server port: Specifies the proxy port used to connect to the cloud from an external
network (If you do not need it, press Enter.)
Test access with supplied credentials? y
(If "Success. Your access key and secret key worked fine :-)" is displayed, the connection is successful.)
Save settings? y (Specifies whether to save the configurations. If you enter y, the configuration will be
saved.)
```

NOTE

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

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

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

CAUTION

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

Step 6 Register a private image.

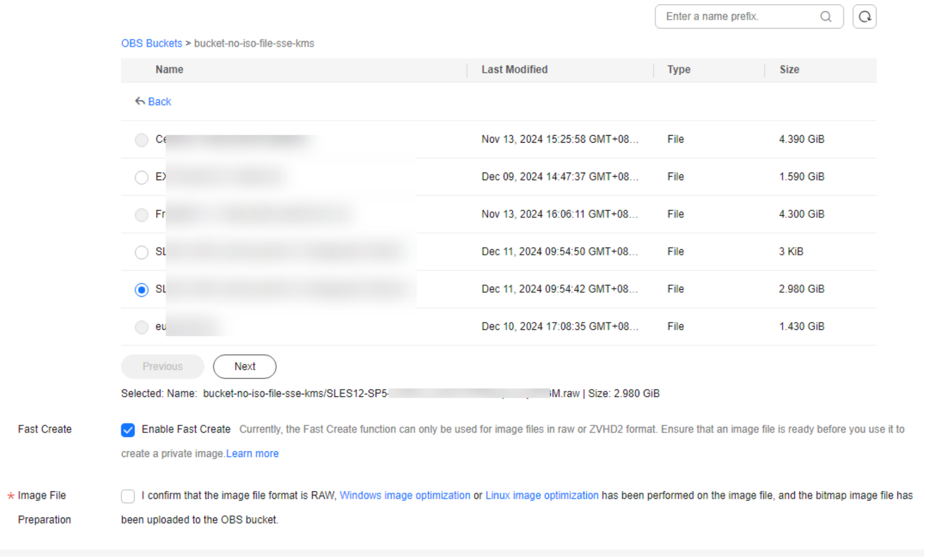
You can register a private image using the converted ZVHD2 or RAW file on the console or using an API.

Method 1: Register a private image on the console.

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

      The IMS console is displayed.
2. In the upper right corner, click **Create Image**.
3. In the **Image Type and Source** area, select **Import Image** for **Type** and then select **System disk image** or **Data disk image** for **Image Type**.
4. Select the bucket storing the ZVHD2 or RAW image file and then select the image file.
5. Select **Enable Fast Create**, and select the sentence following **Image File Preparation**.

Figure 4-36 Fast import of an image file



OBS Buckets > bucket-no-iso-file-sse-kms

	Name	Last Modified	Type	Size
	↶ Back			
○	Ce[redacted]	Nov 13, 2024 15:25:58 GMT+08...	File	4.390 GiB
○	EX[redacted]	Dec 09, 2024 14:47:37 GMT+08...	File	1.590 GiB
○	Fr[redacted]	Nov 13, 2024 16:06:11 GMT+08...	File	4.300 GiB
○	SL[redacted]	Dec 11, 2024 09:54:50 GMT+08...	File	3 KiB
●	SL[redacted]	Dec 11, 2024 09:54:42 GMT+08...	File	2.980 GiB
○	eu[redacted]	Dec 10, 2024 17:08:35 GMT+08...	File	1.430 GiB

Selected: Name: bucket-no-iso-file-sse-kms/SLES12-SP5-[redacted]M.raw | Size: 2.980 GiB

Fast Create ☑ Enable Fast Create Currently, the Fast Create function can only be used for image files in raw or ZVHD2 format. Ensure that an image file is ready before you use it to create a private image.Learn more

* Image File Preparation □ I confirm that the image file format is RAW, Windows image optimization or Linux image optimization has been performed on the image file, and the bitmap image file has been uploaded to the OBS bucket.

6. Set parameters as prompted.

   For details about the parameters, see **Register an Image File as a Private Image**.

   ⚠ CAUTION

   – The OS must be the same as that in the image file.

   – The system disk capacity must be greater than that specified in the image file.

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

     qemu-img-hw info *test.zvhd2*

Method 2: Register a private image using an API.

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

For details about how to call this API, see **Importing an Image File Quickly**.

----End

Appendix 1: Common qemu-img-hw Commands

- Converting image file formats: **qemu-img-hw convert -p -O** *Target_image_format Source_image__file Target_image_file*

  The parameters are described as follows:

  -p: indicates the conversion progress.

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

  For example, run the following command to convert a QCOW2 image file to a ZVHD2 file:

  qemu-img-hw convert -p -O zvhd2 test.qcow2 test.zvhd2

- Querying image file information: **qemu-img-hw info** *Source image file*

  An example command is **qemu-img-hw info test.zvhd2**.

- Viewing help information: **qemu-img-hw -help**

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

- Symptom:

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

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

  Solution:

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

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

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

tar -xvf glibc-2.15.tar.gz

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

mv glibc-ports-2.15 glibc-2.15/ports

mkdir glibc-build-2.15

cd glibc-build-2.15

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

NOTE

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

make

make install

- Symptom:

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

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

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

- Symptom:

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

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

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

  Run the following commands to install OpenSSL 1.0:

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

  tar -xvf openssl-1.0.2k.tar.gz

  cd openssl-1.0.2k

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

  make

  make install

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

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

4.6.3 Fast Import of an Image File in Windows

Scenarios

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

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

Prerequisites

- The image file has been initially configured as instructed in **Table 2-2** based on the OS in the image file.
- An OBS bucket has been created on the management console, and OBS Browser+ has been ready.

Procedure

Step 1 Install the open-source image conversion tool **qemu-img**. For details, see **Converting the Image Format Using qemu-img**.

Step 2 Run the **cmd** command to go to the **qemu-img** installation directory and run the **qemu-img** command to convert the image file to the RAW format.

For example, run the following command to convert an **image.qcow2** file to an **image.raw** file:

```
qemu-img convert -p -O raw image.qcow2 image.raw
```

Step 3 Use **CreateMF.jar** to generate a bitmap file.

1. Obtain the **CreateMF.jar** package and decompress it.

Table 4-5 CreateMF.jar package

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

2. Ensure that JDK has been installed in the current environment.

   You can verify the installation by running **cmd.exe** and then **java -version**. If Java version information is displayed, JDK has been installed.

3. Go to the directory where **CreateMF.jar** is stored.

   For example, if you have downloaded **CreateMF.jar** to **D:/test**, run the following commands to access the directory:

   ```
   D:
   cd test
   ```

4. Run the following command to generate a bitmap file for the RAW image file:

   ```
   java -jar CreateMF.jar D:/image01.raw D:/image01.mf
   ```

⚠ CAUTION

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

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

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

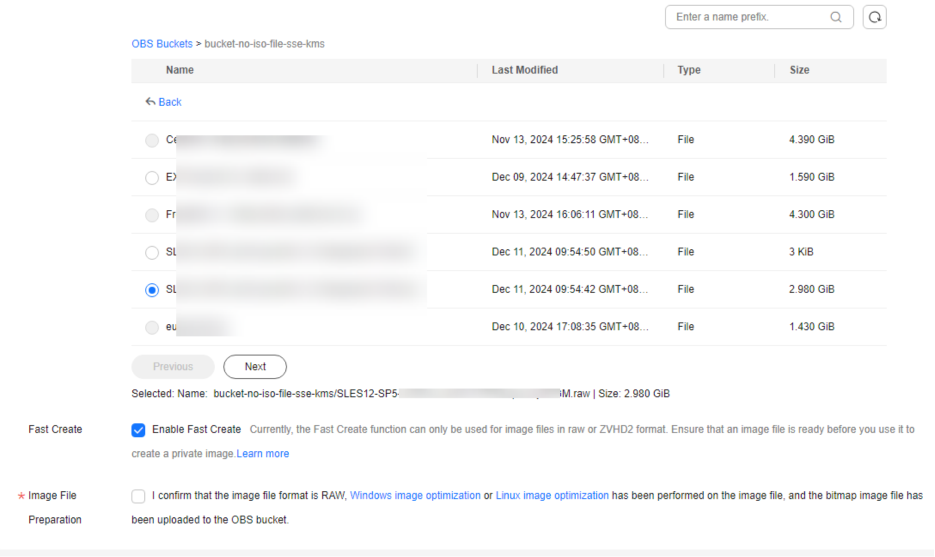
Step 5 Register a private image.

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

Method 1: Register a private image on the console.

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

Figure 4-37 Fast import of an image file



OBS Buckets > bucket-no-iso-file-sse-kms

	Name	Last Modified	Type	Size
	Back			
○	Ce[redacted]	Nov 13, 2024 15:25:58 GMT+08...	File	4.390 GiB
○	EX[redacted]	Dec 09, 2024 14:47:37 GMT+08...	File	1.590 GiB
○	Fr[redacted]	Nov 13, 2024 16:06:11 GMT+08...	File	4.300 GiB
○	SL[redacted]	Dec 11, 2024 09:54:50 GMT+08...	File	3 KiB
●	SL[redacted]	Dec 11, 2024 09:54:42 GMT+08...	File	2.980 GiB
○	eu[redacted]	Dec 10, 2024 17:08:35 GMT+08...	File	1.430 GiB

Selected: Name: bucket-no-iso-file-sse-kms/SLES12-SP5-[redacted]M.raw | Size: 2.980 GiB

Fast Create ☑ Enable Fast Create Currently, the Fast Create function can only be used for image files in raw or ZVHD2 format. Ensure that an image file is ready before you use it to create a private image.Learn more

* Image File Preparation □ I confirm that the image file format is RAW, Windows image optimization or Linux image optimization has been performed on the image file, and the bitmap image file has been uploaded to the OBS bucket.

6. Set parameters as prompted.
   For details about the parameters, see **Register an Image File as a Private Image**.

⚠ CAUTION

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

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

  qemu-img-hw info *test.zvhd2*

Method 2: Register a private image using an API.

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

For details about how to call this API, see **Importing an Image File Quickly**.

----End

5 Managing Private Images

5.1 Creating an ECS from an Image

Scenarios

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

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

Procedure

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

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

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

   NOTE

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

5.2 Modifying an Image

Scenarios

You can modify the following attributes of a private image:

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

  NIC multi-queue enables multiple CPUs to process NIC interrupts for load balancing. For details, see **How Do I Enable NIC Multi-Queue for an Image?**
- Boot mode
- SR-IOV driver
- Virtio-net passthrough

Constraints

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

Procedure

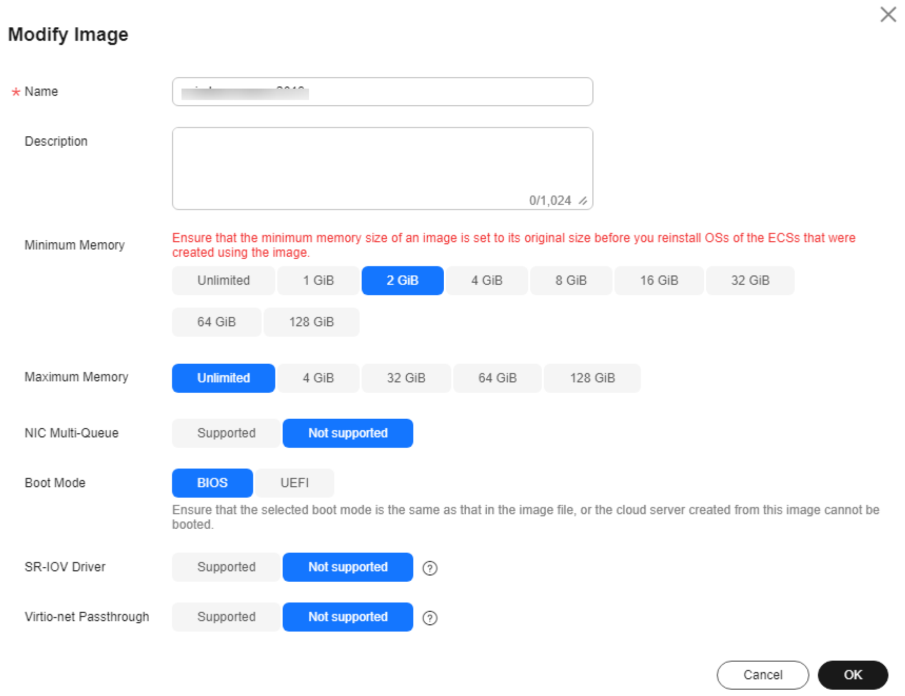
Use any of the following methods to modify an image:

Method 1:

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

      The IMS console is displayed.
2. Click the **Private Images** tab to display the image list.
3. Locate the row that contains the image and click **Modify** in the **Operation** column.
4. In the **Modify Image** dialog box, modify the image.

Figure 5-1 Modifying an image



Modify Image

* Name [redacted]

Description 0/1,024

Minimum Memory
Ensure that the minimum memory size of an image is set to its original size before you reinstall OSs of the ECSs that were created using the image.
Unlimited 1 GiB [✓ 2 GiB] 4 GiB 8 GiB 16 GiB 32 GiB 64 GiB 128 GiB

Maximum Memory [✓ Unlimited] 4 GiB 32 GiB 64 GiB 128 GiB

NIC Multi-Queue Supported [✓ Not supported]

Boot Mode [✓ BIOS] UEFI
Ensure that the selected boot mode is the same as that in the image file, or the cloud server created from this image cannot be booted.

SR-IOV Driver Supported [✓ Not supported]

Virtio-net Passthrough Supported [✓ Not supported]

Method 2:

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

Method 3:

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

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

5.3 Exporting an Image

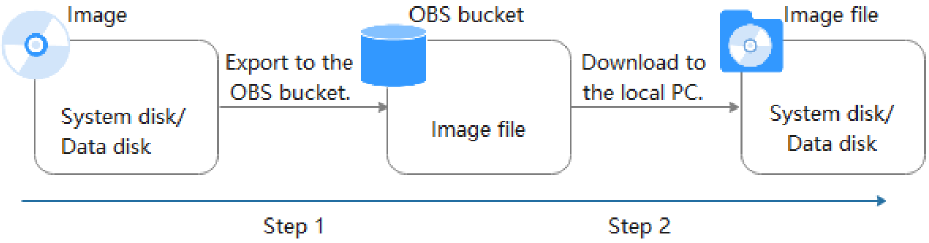
Scenarios

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

Background

- You can export images of cloud servers from the cloud platform and then use the exported images to create cloud servers for use in on-premises clusters or private clouds. The following figure shows the process of exporting an image.

  Figure 5-2 Exporting an image



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

  NOTE

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

Constraints

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

> NOTE
>
> In some regions, an image larger than 128 GB can be exported without enabling **Fast Export**. You can see on the console if such a large image can be exported in that way.

Prerequisites

- You have Administrator permissions for OBS.
- An OBS bucket is available for storing the private image in the region where the private image is located.

  If no OBS bucket is available, create one by referring to **Creating a Bucket**. Select **Standard** for **Storage Class**.

> NOTE
>
> You will be charged for storing exported images in the OBS bucket. For details, see **OBS Pricing Details**.

Procedure

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

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

     > NOTE
     >
     > For details about the differences between standard and fast export, see **What Are the Differences Between Standard and Fast Import/Export?**
   - **Format**: Select one from **qcow2**, **vmdk**, **vhd**, and **zvhd** as you need.
   - **Name**: Enter a name that is easy to identify.
   - **Storage Path**: Click 🗀 to expand the bucket list and select an OBS bucket for storing the exported image.

     > NOTE
     >
     > An image can only be exported to a Standard bucket that is in the same region as the image. So, only such buckets are listed.
4. Click **OK**.

   You can view the image export progress above the private image list.

Follow-up Procedure

After the image is exported, you can download it from the OBS bucket through the management console or OBS Browser+. For details, see **Downloading an Object**.

5.4 Exporting Image List

Scenarios

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

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

Exporting Private Image Information

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

      The IMS console is displayed.
2. On the **Private Images** tab, click **Export** above the image list and select what images to export.

   The system will automatically export the list of selected private images in the current region under your account to a local directory.

Exporting Public Image Information

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

      The IMS console is displayed.
2. On the **Public Images** tab, click **Export** above the image list, and select **Export all data to an XLSX file**.

   The system will automatically export the list of all public images in the current region to a local directory.

5.5 Checking the Disk Capacity of an Image

Scenarios

You can check the disk capacity of a private image.

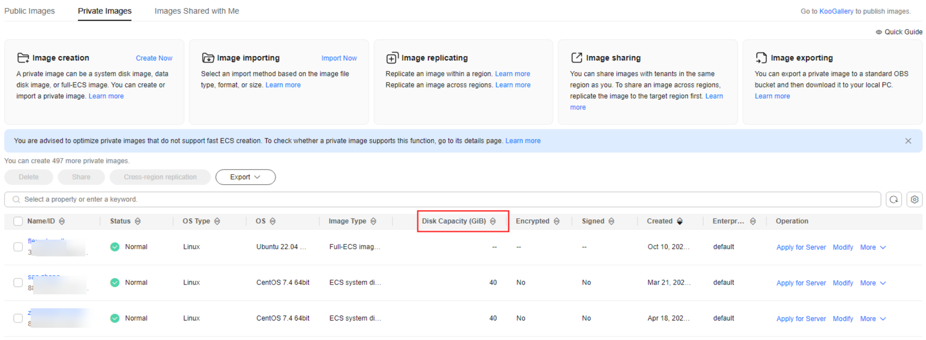
- To check the disk capacity of a system disk image, data disk image, or ISO image, see **Check the Disk Capacity of a System Disk Image, Data Disk Image, or ISO Image**.
- To check the disk capacity of a full-ECS image, see **Check the Disk Capacity of a Full-ECS Image**.

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

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

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

Figure 5-3 Checking the disk capacity of a system disk image, data disk image, or ISO image



A private image can be a system disk image, data disk image, or full-ECS image. You can create or import a private image. Learn more

Select an import method based on the image file type, format, or size. Learn more

Replicate an image within a region. Learn more
Replicate an image across regions. Learn more

You can share images with tenants in the same region as you. To share an image across regions, replicate the image to the target region first. Learn more

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

You are advised to optimize private images that do not support fast ECS creation. To check whether a private image supports this function, go to its details page. Learn more

You can create 497 more private images.

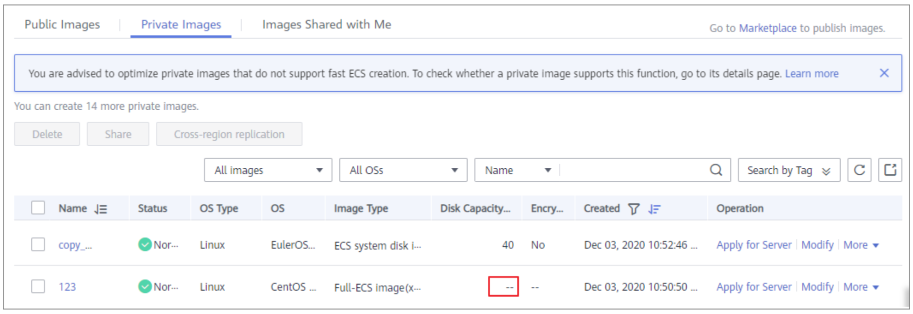
Name/ID	Status	OS Type	OS	Image Type	Disk Capacity (GiB)	Encrypted	Signed	Created	Enterpr...	Operation
[redacted]	Normal	Linux	Ubuntu 22.04 ...	Full-ECS imag...	--	--	--	Oct 10, 202...	default	Apply for Server Modify More
[redacted]	Normal	Linux	CentOS 7.4 64bit	ECS system di...	40	No	No	Mar 21, 202...	default	Apply for Server Modify More
[redacted]	Normal	Linux	CentOS 7.4 64bit	ECS system di...	40	No	No	Apr 18, 202...	default	Apply for Server Modify More

Check the Disk Capacity of a Full-ECS Image

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

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

Figure 5-4 Checking the disk capacity of a full-ECS image



You are advised to optimize private images that do not support fast ECS creation. To check whether a private image supports this function, go to its details page. Learn more

You can create 14 more private images.

Name	Status	OS Type	OS	Image Type	Disk Capacity...	Encry...	Created	Operation
copy_...	Nor...	Linux	EulerOS...	ECS system disk i...	40	No	Dec 03, 2020 10:52:46 ...	Apply for Server | Modify | More
123	Nor...	Linux	CentOS ...	Full-ECS image(x...	--	--	Dec 03, 2020 10:50:50 ...	Apply for Server | Modify | More

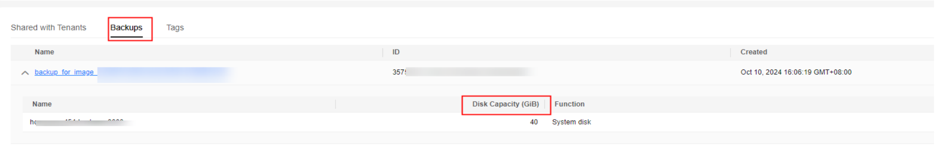
3. Click the full-ECS image name.
4. Click the **Backups** tab and view the capacities of the system disk and data disks in the backup.

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

   For example:

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

     Figure 5-5 Checking backup details

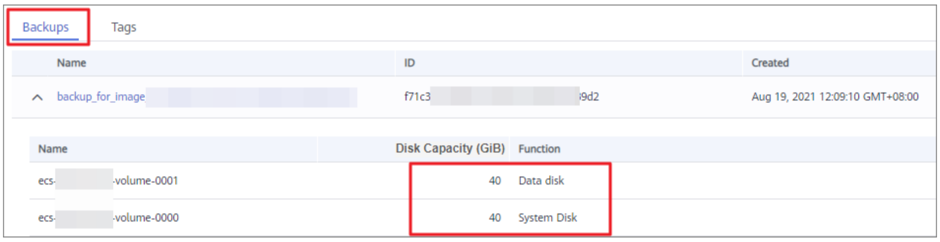
     

Name	ID	Created
backup_for_image_[redacted]	357[redacted]	Oct 10, 2024 16:06:19 GMT+08:00

Name	Disk Capacity (GiB)	Function
hc[redacted]	40	System disk

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

     Figure 5-6 Checking backup details

Name	ID	Created
backup_for_image[redacted]	f71c3[redacted]9d2	Aug 19, 2021 12:09:10 GMT+08:00

Name	Disk Capacity (GiB)	Function
ecs-[redacted]-volume-0001	40	Data disk
ecs-[redacted]-volume-0000	40	System Disk

5.6 Deleting Images

Scenarios

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

- Deleted private images cannot be retrieved. Perform this operation only when absolutely necessary.
- After a private image is deleted, it cannot be used to create ECSs or EVS disks.

- After a private image is deleted, ECSs created from the image can still be used and are still billed. However, the OS cannot be reinstalled for the ECSs and ECSs with the same configuration cannot be created.
- Deleting the source image of a replicated image has no effect on the replicated image. Similarly, deleting a replicated image has no effect on its source.
- If a full-ECS image is still being created when you delete it, some intermediate backups may fail to be deleted. To avoid generating any unnecessary expenditures, you can delete them on the CSBS or CBR console.

Constraints

- Private images that have been published in KooGallery cannot be deleted.
- If an image is shared with an account or organization, you need first to remove the account or organization from the image recipients before you delete the image.

Procedure

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

      The IMS console is displayed.
2. Click the **Private Images** tab to display the image list.
3. Locate the row that contains the image, choose **More** > **Delete** in the **Operation** column.

   NOTE

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

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

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

   NOTE

   If CSBS or CBR backups are not deleted, they will continue to be billed. You can delete them later on the CSBS or CBR console.
5. Enter **DELETE** to confirm the deletion. Click **OK**.

5.7 Sharing Images

5.7.1 Overview

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

⚠ CAUTION

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

Constraints

- You cannot share private images that have been published in KooGallery.
- You can share images only within the region where they reside. To share an image across regions, you need to replicate the image to the target region first.
- A system disk image or data disk image can be shared with up to 128 tenants, projects, or organizations, and a full-ECS image can be shared with up to 10 tenants, projects, or organizations.

  NOTE

  Currently, image sharing with an account or organization is available only in certain regions.
- A full-ECS image is shareable only when it is created from a CBR backup or from an ECS that has never had a CSBS backup.

Procedure

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

1. You obtain the project ID, account ID, or organization URN from the tenant.

   NOTE

   For details about how to obtain a project ID or an account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**. For details about how to obtain an organization URN, see **Viewing Details About an Organization**.
2. You share an image with the tenant.
3. The tenant accepts the shared image.

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

   NOTE

   If the image is shared with an account or organization, the tenant can skip this step.

Video Tutorial

FAQ

If you have any questions, see **Image Sharing FAQ**.

5.7.2 Obtaining the Project ID, Account ID, and Organization URN

Scenarios

Before a tenant shares an image with you, you need to provide your project ID, account ID, or organization URN. For details about how to obtain a project ID or an account ID, see **Procedure**. For details about how to obtain an organization URN, see **Viewing Details About an Organization**.

NOTE

Currently, image sharing with an account or organization is available only in certain regions.

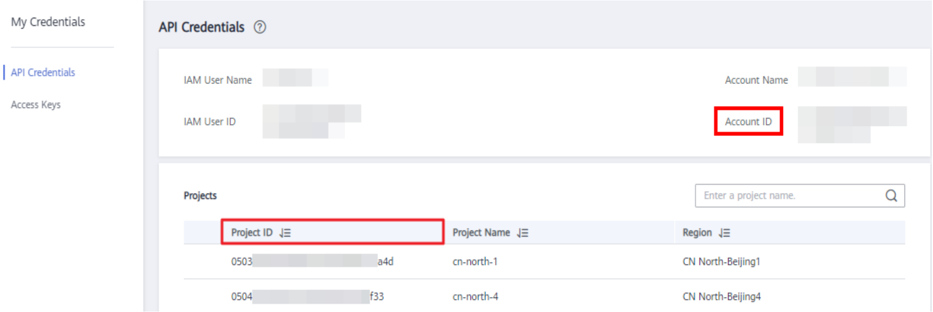
Procedure

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

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

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

Figure 5-7 Viewing the project ID or account ID



IAM User Name [redacted]
IAM User ID [redacted]
Account Name [redacted]
Account ID [redacted]

Projects

Project ID	Project Name	Region
0503[redacted]a4d	cn-north-1	CN North-Beijing1
0504[redacted]f33	cn-north-4	CN North-Beijing4

5.7.3 Sharing Specified Images

Scenarios

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

Prerequisites

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

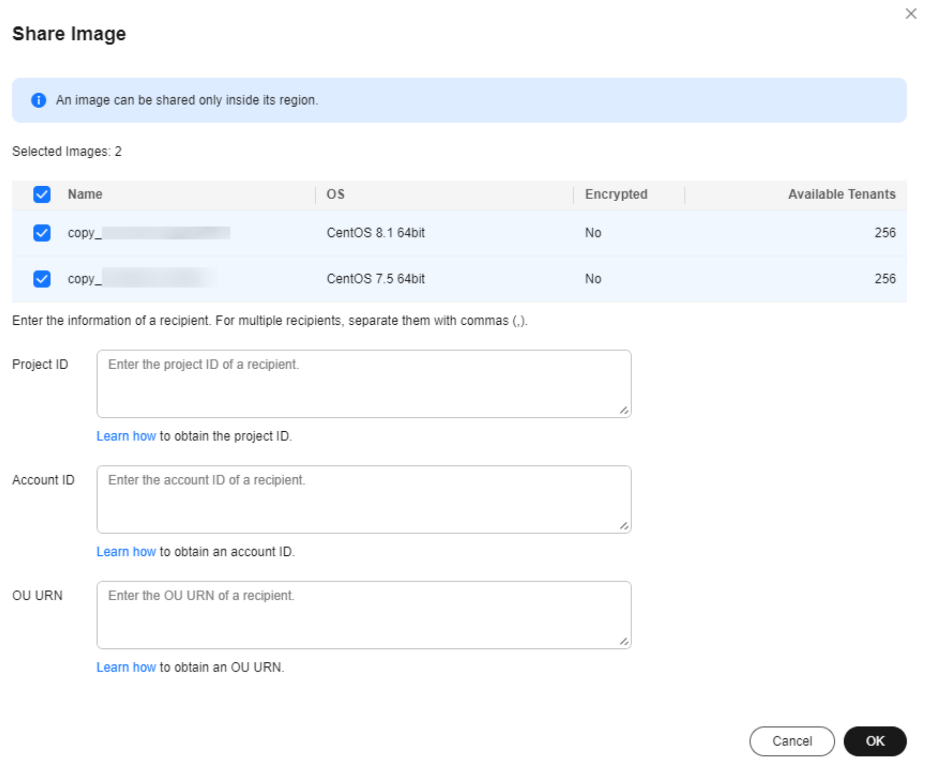
Procedure

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

     NOTE

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

Figure 5-8 Sharing images



Share Image

An image can be shared only inside its region.

Selected Images: 2

☑	Name	OS	Encrypted	Available Tenants
☑	copy_[redacted]	CentOS 8.1 64bit	No	256
☑	copy_[redacted]	CentOS 7.5 64bit	No	256

Enter the information of a recipient. For multiple recipients, separate them with commas (,).

Project ID: Enter the project ID of a recipient.

Learn how to obtain the project ID.

Account ID: Enter the account ID of a recipient.

Learn how to obtain an account ID.

OU URN: Enter the OU URN of a recipient.

Learn how to obtain an OU URN.

e. Click **OK**.

- Share a single image.

a. Access the IMS console.

i. Log in to the management console.

ii. Under **Compute**, click **Image Management Service**.

The IMS console is displayed.

b. Click the **Private Images** tab.

c. Locate the row that contains the private image you are to share, click **More** in the **Operation** column, and select **Share** from the drop-down list.

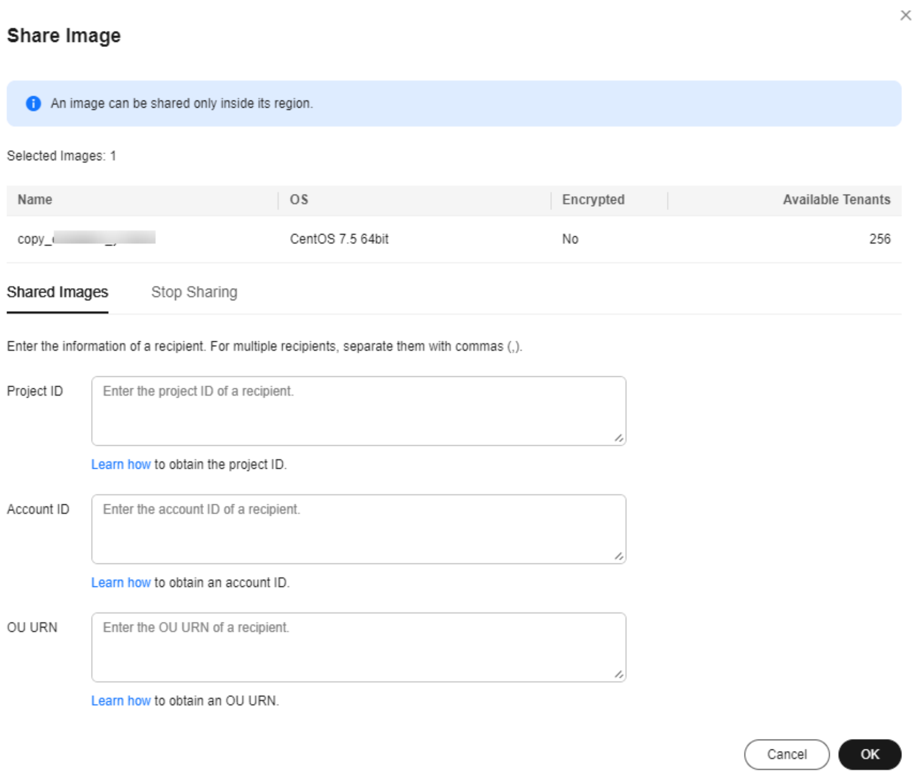
d. In the **Share Image** dialog box, enter the project ID of the target tenant.

To share an image with more than one tenant, separate their project IDs with commas (,).

NOTE

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

Figure 5-9 Sharing an image



Share Image

An image can be shared only inside its region.

Selected Images: 1

Name	OS	Encrypted	Available Tenants
copy_[redacted]	CentOS 7.5 64bit	No	256

Shared Images | Stop Sharing

Enter the information of a recipient. For multiple recipients, separate them with commas (,).

Project ID: Enter the project ID of a recipient.
Learn how to obtain the project ID.

Account ID: Enter the account ID of a recipient.
Learn how to obtain an account ID.

OU URN: Enter the OU URN of a recipient.
Learn how to obtain an OU URN.

e. Click **OK**.

Related Operations

After you share images with a tenant, the tenant can accept the shared images on the **Images Shared with Me** page on the IMS console. For details, see **Accepting or Rejecting Shared Images**.

5.7.4 Accepting or Rejecting Shared Images

Scenarios

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

NOTE

- If you are not in the same region as the tenant sharing the images with you, you will not receive the message.
- If images are shared with your account or organization, skip this section.

  Currently, image sharing with an account or organization is available only in certain regions.

Prerequisites

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

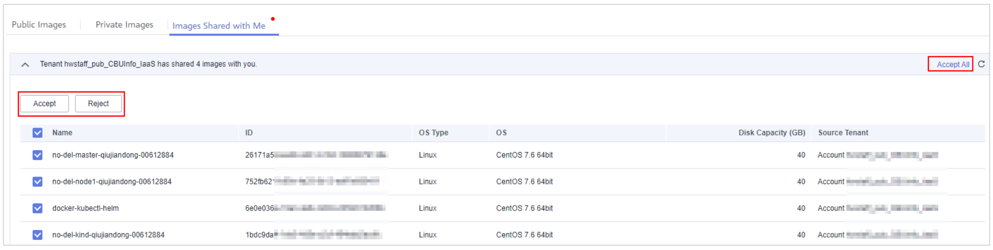
Procedure

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

      The IMS console is displayed.
2. In the upper left corner, switch to the region where the target project is and then select the project.
3. Click the **Images Shared with Me** tab.

   A message is displayed above the image list asking you whether to accept the shared images.
   - To accept all the shared images, click **Accept All** in the upper right corner.
   - To accept some images, select the images and click **Accept**.
   - To reject some images, select the images and click **Reject**.

Figure 5-10 Accepting or rejecting shared images



Tenant hwstaff_pub_CBUInfo_IaaS has shared 4 images with you.

☑ Name	ID	OS Type	OS	Disk Capacity (GB)	Source Tenant
☑ no-del-master-qiujiandong-00612884	26171a5[redacted]	Linux	CentOS 7.6 64bit	40	Account [redacted]
☑ no-del-node1-qiujiandong-00612884	752fb62[redacted]	Linux	CentOS 7.6 64bit	40	Account [redacted]
☑ docker-kubectl-helm	6e0e036[redacted]	Linux	CentOS 7.6 64bit	40	Account [redacted]
☑ no-del-kind-qiujiandong-00612884	1bdc9da[redacted]	Linux	CentOS 7.6 64bit	40	Account [redacted]

NOTE

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

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

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

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

   NOTE

   For more information about server backup vaults, see **What Is CBR?**

Results

- **Pending**: If you do not immediately accept or reject a shared image, the image is in the **Pending** state.

  A pending shared image is not displayed in the shared image list.

- **Accepted**: After an image is accepted, it is displayed in the shared image list. You can use the image to create ECSs.
- **Rejected**: After an image is rejected, it is not displayed in the shared image list. You can click **Rejected Images** to view the images you have rejected and you can still choose to accept them.

  NOTE

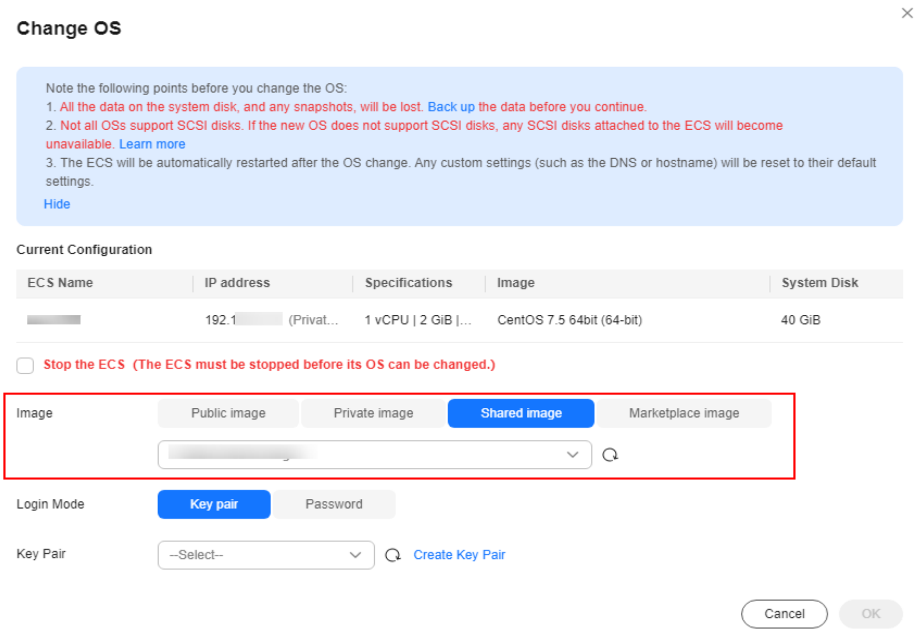
  - If an image is shared with both your project and account, the image can be displayed in the shared image list and you can use it even if the sharing with your project is neither accepted nor rejected.
  - If an image is shared with both your project and organization, the image can be displayed in the shared image list and you can use it even if the sharing with your project is neither accepted nor rejected.

Follow-up Procedure

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

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

Figure 5-11 Changing the OS



Change OS

Note the following points before you change the OS:
1. All the data on the system disk, and any snapshots, will be lost. Back up the data before you continue.
2. Not all OSs support SCSI disks. If the new OS does not support SCSI disks, any SCSI disks attached to the ECS will become unavailable. Learn more
3. The ECS will be automatically restarted after the OS change. Any custom settings (such as the DNS or hostname) will be reset to their default settings.

Hide

Current Configuration

ECS Name	IP address	Specifications	Image	System Disk
[redacted]	192.1[redacted] (Privat...	1 vCPU | 2 GiB |...	CentOS 7.5 64bit (64-bit)	40 GiB

□ Stop the ECS (The ECS must be stopped before its OS can be changed.)

Image: Public image | Private image | Shared image | Marketplace image
[redacted]

Login Mode: Key pair | Password

Key Pair: --Select-- Create Key Pair

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

5.7.5 Rejecting Accepted Images

Scenarios

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

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

Prerequisites

You have accepted images shared by other users.

Procedure

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

5.7.6 Accepting Rejected Images

Scenarios

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

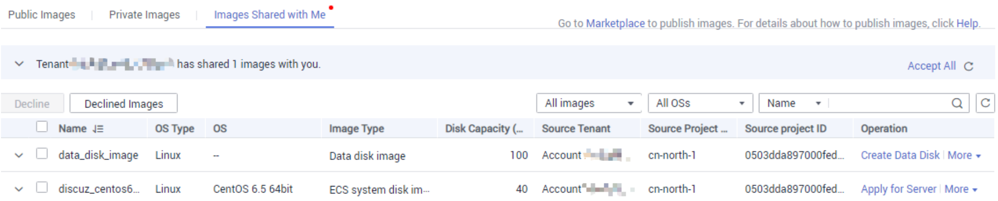
Prerequisites

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

Procedure

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

Figure 5-12 Images Shared with Me



Tenant[redacted] has shared 1 images with you.

Name	OS Type	OS	Image Type	Disk Capacity (...	Source Tenant	Source Project ...	Source project ID	Operation
data_disk_image	Linux	--	Data disk image	100	Account[redacted]	cn-north-1	0503dda897000fed...	Create Data Disk | More
discuz_centos6...	Linux	CentOS 6.5 64bit	ECS system disk im...	40	Account[redacted]	cn-north-1	0503dda897000fed...	Apply for Server | More

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

5.7.7 Stopping Sharing Images

Scenarios

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

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

NOTE

If an image is shared with a project, an account, and also an organization which may be included with each other, you must stop sharing the image with all of them to completely stop the sharing.

Prerequisites

You have shared private images with others.

Procedure

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

5.7.8 Adding Tenants Who Can Use Shared Images

Scenarios

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

Prerequisites

- You have shared private images.
- You have obtained the project IDs, account IDs, or organization URNs of the tenants to be added.

Procedure

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

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

NOTE

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

5.7.9 Deleting Image Recipients Who Can Use Shared Images

Scenarios

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

Prerequisites

- You have shared private images.
- You have obtained the project IDs, account IDs, or organization URNs of the image recipients.

Procedure

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

5.7.10 Replicating a Shared Image

Scenarios

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

Constraints

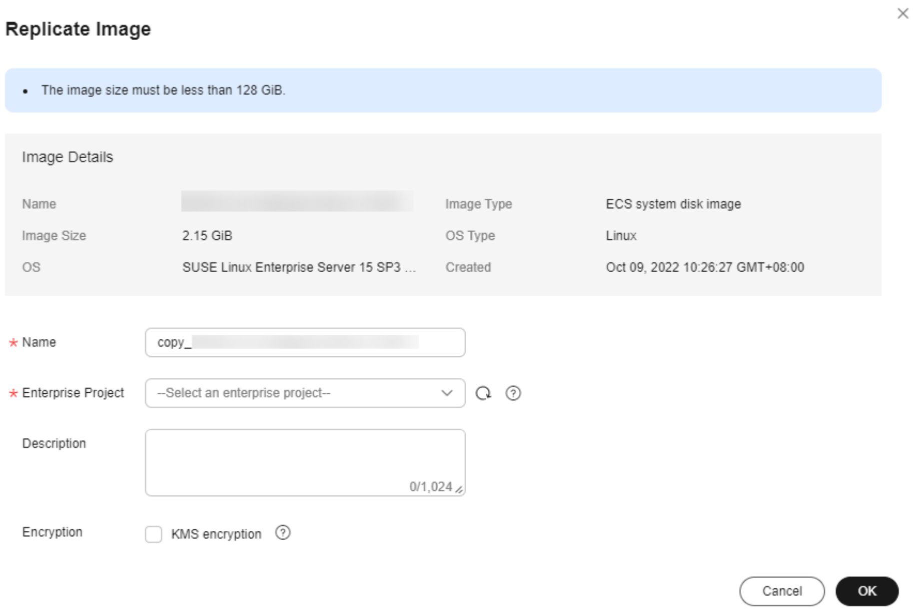
- Currently, only system and data disk images can be replicated. Full-ECS images are not supported.
- Currently, images can only be replicated within a region.

- An image to be replicated cannot be larger than 128 GB.
- An image cannot be replicated to generate an encrypted image.

Procedure

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

Figure 5-13 Replicating an image



Replicate Image

- The image size must be less than 128 GiB.

Image Details

Name		Image Type	ECS system disk image
Image Size	2.15 GiB	OS Type	Linux
OS	SUSE Linux Enterprise Server 15 SP3 ...	Created	Oct 09, 2022 10:26:27 GMT+08:00

* Name: copy_
* Enterprise Project: --Select an enterprise project--
Description: 0/1,024
Encryption: □ KMS encryption

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

5.8 Encrypting Images

You can create encrypted images to securely store data.

NOTE

- To use image encryption, you must apply for KMS Administrator permissions.
- An encrypted full-ECS image may contain multiple disks. The encryption status of each disk may be different. So, the encryption status of a full-ECS image is displayed as - in the image list.
- An encrypted full-ECS image inherits the encryption status of each disk of the ECS used to create the image. The inherited status cannot be changed.
- For how to check the encryption status of a disk in an encrypted full-ECS image, see **How Do I Check the Encryption Status of a Disk in an Encrypted Full-ECS Image?**
- When you share an encrypted image with a user, ensure that the user has permissions for the key used to encrypt the image.

Constraints

- DEW must be enabled.
- An image encrypted using the default key cannot be shared with other users.
- Encrypted images cannot be published in KooGallery.
- The system disk of an ECS created from an encrypted image is also encrypted, and its key is the same as the image key.
- If an ECS has an encrypted system disk, private images created from the ECS are also encrypted.
- The key used for encrypting an image cannot be changed.
- If the key used for encrypting an image is disabled or deleted, the image is unavailable.
- Encrypted full-ECS images cannot be replicated across regions.

Introduction

You can create an encrypted image from an image file or an encrypted ECS.

- Create an encrypted image from an image file.

  When you register an image file as a private image, select **KMS encryption** and select a key. For details, see **Creating a System Disk Image from an Image File**.
- Create an encrypted image from an encrypted ECS.

  When you use an ECS to create a private image, if the system disk of the ECS is encrypted, the private image created from this ECS will also be encrypted. The key used for encrypting the image is the same as that used for encrypting the system disk. For details, see **Creating a System Disk Image from an ECS**.

5.9 Replicating Images Within a Region

Scenarios

You can convert encrypted and unencrypted images into each other or enable some advanced features (such as fast ECS creation from an image) using in-region image replication. You may need to replicate an image to:

- Replicate an encrypted image to an unencrypted one.

Encrypted images cannot be shared with other tenants or published in KooGallery. If you want to publish or share an encrypted image, you can replicate it to an unencrypted one.

- Replicate an encrypted image to an encrypted one.

  Keys for encrypting the images cannot be changed. If you want to change the key of an encrypted image, you can replicate this image to a new one and encrypt the new image using an encryption key.

- Replicate an unencrypted image to an encrypted one.

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

- Optimize a system disk image so that it can be used to quickly create ECSs.

  Fast Create greatly reduces the time required for creating ECSs from a system disk image. Currently, this feature is supported by all newly created system disk images by default. Existing system disk images may not support it. You can enable them to support this feature through in-region image replication. For example, if image A does not support fast ECS creation, you can replicate it to generate image copy_A that supports fast ECS creation.

Constraints

- Full-ECS images cannot be replicated within the same region.
- Private images created using ISO files do not support in-region replication.

Prerequisites

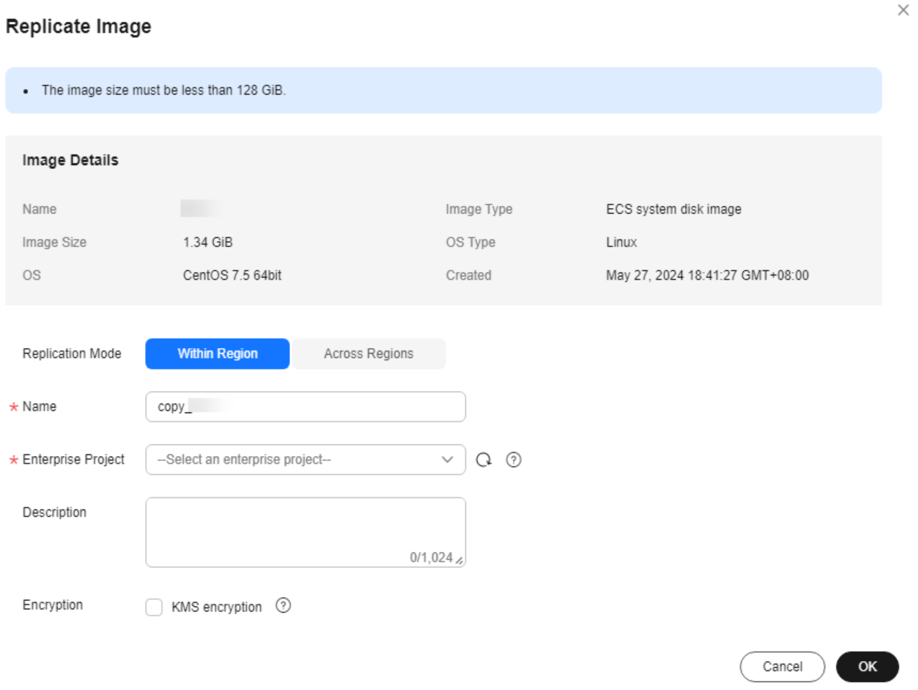
The images to be replicated are in the **Normal** state.

Procedure

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

      The IMS console is displayed.
2. Locate the row that contains the image to be replicated, click **More** in the **Operation** column, and select **Replicate**.
3. In the displayed **Replicate Image** dialog box, set the following parameters:

Figure 5-14 Replicating images within a region



Replicate Image

- The image size must be less than 128 GiB.

Image Details

Name	[redacted]	Image Type	ECS system disk image
Image Size	1.34 GiB	OS Type	Linux
OS	CentOS 7.5 64bit	Created	May 27, 2024 18:41:27 GMT+08:00

Replication Mode: Within Region | Across Regions

* Name: copy_[redacted]

* Enterprise Project: --Select an enterprise project--

Description: 0/1,024

Encryption: □ KMS encryption

- **Replication Mode**: Select **Within Region**.

  NOTE

  This parameter is available only when the current region also supports cross-region replication.

- **Name**: Enter a name that is easy to identify.
- **Enterprise Project**: Select an enterprise project from the drop-down list. This parameter is available only if you have enabled enterprise projects or your account is an enterprise account. To enable this function, contact your customer manager.
- (Optional) **Description**: Describe the replication.
- **Encryption**: If you want to encrypt the image or change a key, select **KMS encryption** and select the key you want to use from the drop-down list.

4. Click **OK**.

   On the **Private Images** page, view the replication progress. If the status of the new image becomes **Normal**, the image replication is successful.

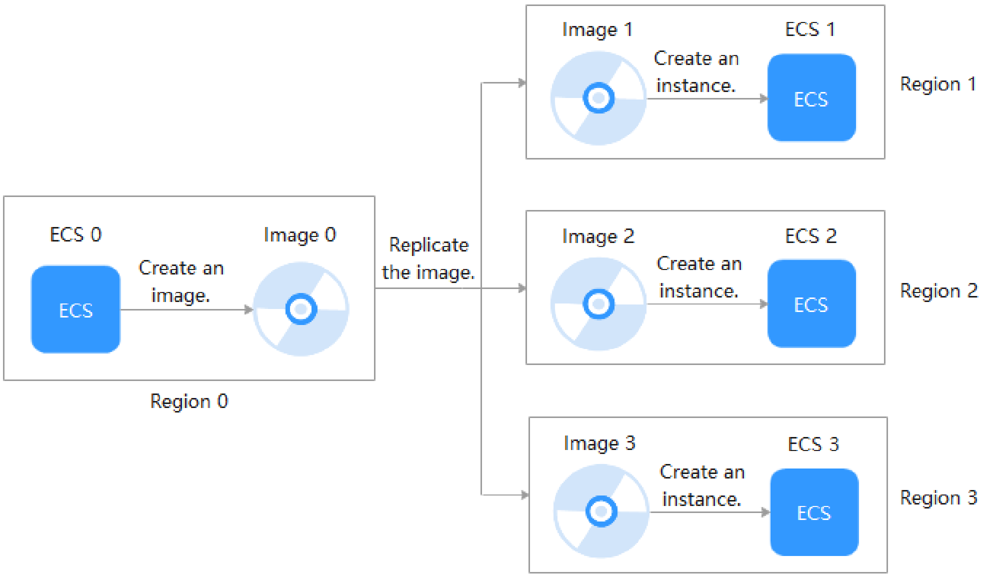
5.10 Replicating Images Across Regions

Scenarios

An image is a regional resource. If you want to use a private image in another region, you can replicate it to the target region.

Cross-region image replication is required for system HA typically when your system is deployed in multiple regions. In most cases, ECSs are deployed in multiple regions (including regions outside the Chinese mainland). If you want to clone an ECS across regions, you can replicate its image across the regions and then use the image to create identical ECSs in the target region.

Figure 5-15 Typical cross-region replication



Video Tutorial

Background

- Cross-region replication is applicable to cross-region server deployment or data backup. It is often used together with image sharing for cross-region, cross-account image replication. The following table describes image replication in different scenarios.

Scenario	Description	Procedure
Cross-region replication under the same account	After the replication is complete, a new image is generated in the target region. The new image has an ID that is different from the source image ID.	See this section.
Cross-region, cross-account replication	Replicate the image to the target region and share it with other accounts.	See this section and **Sharing Specified Images**.

Scenario	Description	Procedure
Cross-account replication in the same region	After the replication is complete, the image is shared with the target tenant. The target tenant can use the image (with the same ID as the source image) but the image owner is still the tenant who shared it.	See **Sharing Specified Images**.

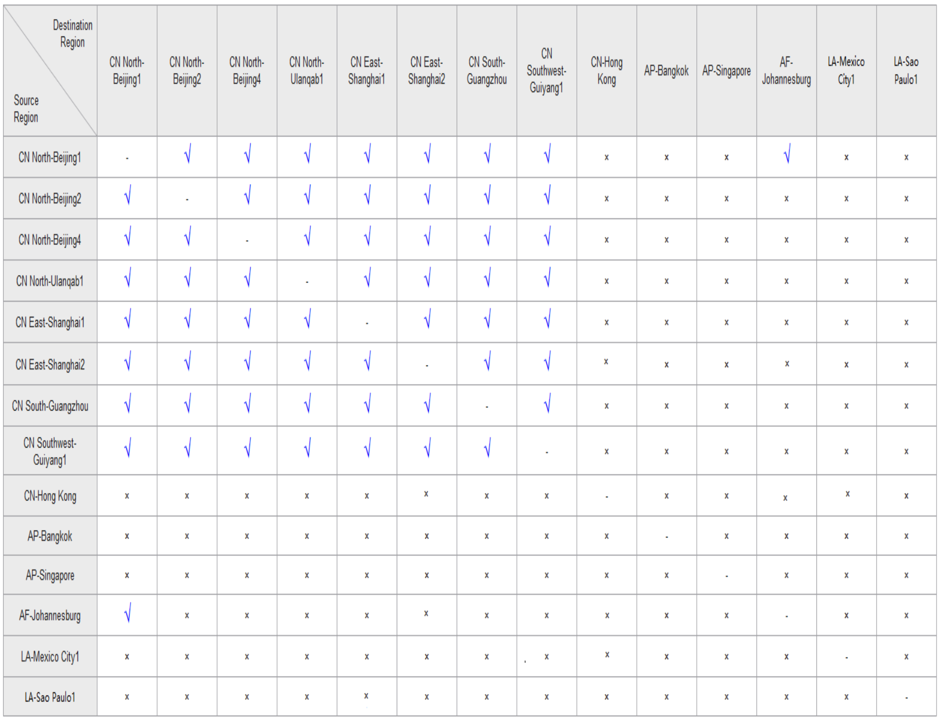
- When a full-ECS image is replicated across regions, the associated CSBS or CBR backups will also be replicated. Therefore, you will be charged for these backups in the target region.
- It takes a while to complete a cross-region replication task. The time required for replicating an image across regions depends on the network speed, image size, and number of concurrent tasks.
- You can select multiple images for cross-region replication at a time. However, you are not allowed to select an ISO image, encrypted image, full-ECS image, frozen image, or the image that is being created.
- An agency is required for cross-region image replication. This agency has the permissions of IMS Administrator, allowing you to perform operations on the projects in the destination region.

  For example, if you want to replicate an image from region A to region B, the agency must have the permissions of IMS Administrator in region B. For how to create an agency, see **Create an Agency**.

Constraints

- Cross-region replication of system and data disk images is only available in certain regions. For details, see the following figure.

Figure 5-16 Cross-region replication of system and data disk images



Destination Region / Source Region	CN North-Beijing1	CN North-Beijing2	CN North-Beijing4	CN North-Ulanqab1	CN East-Shanghai1	CN East-Shanghai2	CN South-Guangzhou	CN Southwest-Guiyang1	CN-Hong Kong	AP-Bangkok	AP-Singapore	AF-Johannesburg	LA-Mexico City1	LA-Sao Paulo1
CN North-Beijing1	-	√	√	√	√	√	√	√	x	x	x	√	x	x
CN North-Beijing2	√	-	√	√	√	√	√	√	x	x	x	x	x	x
CN North-Beijing4	√	√	-	√	√	√	√	√	x	x	x	x	x	x
CN North-Ulanqab1	√	√	√	-	√	√	√	√	x	x	x	x	x	x
CN East-Shanghai1	√	√	√	√	-	√	√	√	x	x	x	x	x	x
CN East-Shanghai2	√	√	√	√	√	-	√	√	x	x	x	x	x	x
CN South-Guangzhou	√	√	√	√	√	√	-	√	x	x	x	x	x	x
CN Southwest-Guiyang1	√	√	√	√	√	√	√	-	x	x	x	x	x	x
CN-Hong Kong	x	x	x	x	x	x	x	x	-	x	x	x	x	x
AP-Bangkok	x	x	x	x	x	x	x	x	x	-	x	x	x	x
AP-Singapore	x	x	x	x	x	x	x	x	x	x	-	x	x	x
AF-Johannesburg	√	x	x	x	x	x	x	x	x	x	x	-	x	x
LA-Mexico City1	x	x	x	x	x	x	x	x	x	x	x	x	-	x
LA-Sao Paulo1	x	x	x	x	x	x	x	x	x	x	x	x	x	-

NOTE

- √ indicates replication is supported.
- × indicates replication is not supported. You can export the desired image and then import it to the target region.
- - indicates that the source and destination regions are the same.
- Region adjustment may affect cross-region image replication of users that are registered after the adjustment. The users that were registered before the adjustment are not affected. You can see on the console if cross-region can be performed for a given region.
- Regions not listed in the figure above do not support cross-region replication of system or data disk images.

- Cross-region replication of full-ECS images is only available for certain regions. You can see on the console if it is available for a given region.

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

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

  If cross-region replication of system and data disk images is not available in a region, cross-region replication of full-ECS images is not available in that region, either.

- You can replicate only private images across regions. If you want to replicate an image of another type (for example, a public image) across regions, you can use the image to create an ECS, use the ECS to create a private image, and then replicate the private image across regions.

NOTE

A private image cannot be replicated across regions after it is published in KooGallery.

If you use a KooGallery image to create an ECS and then use the ECS to create a private image (for example, a Windows image), this private image cannot be replicated across regions.

- To perform cross-region replication, IAM users must have the IAM ReadOnlyAccess permission and the IMS FullAccess permission in both the source and destination regions.
- The size of each image to be replicated across regions cannot be larger than 128 GB.
- You can replicate only five images across regions at a time.
- ISO images and encrypted images cannot be replicated across regions.

Procedure

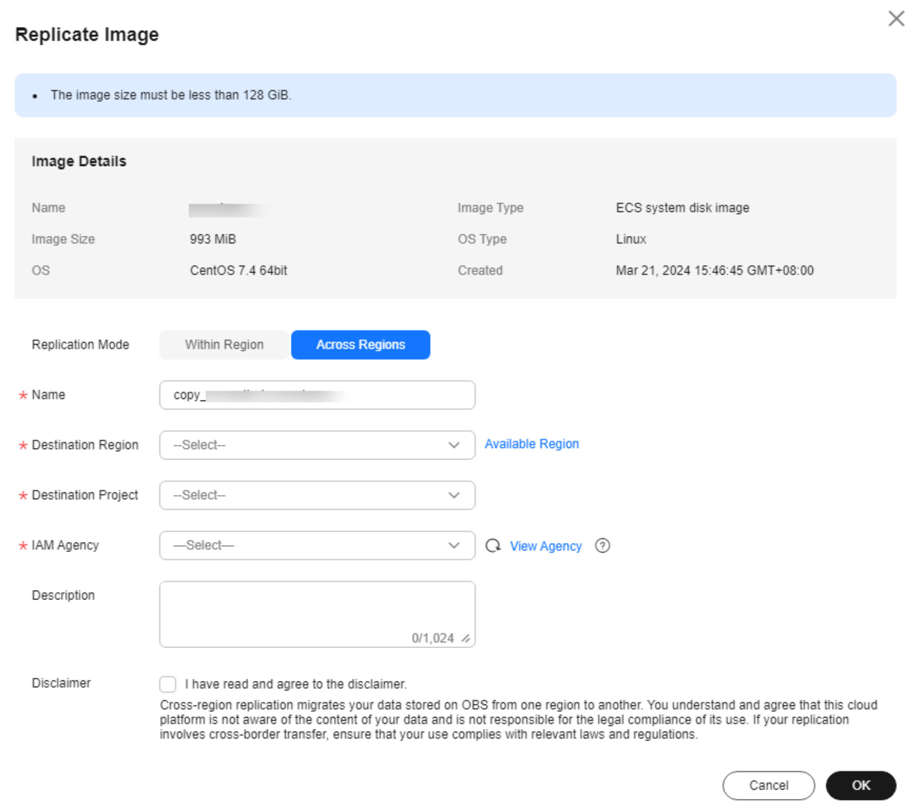
1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.

   The IMS console is displayed.
3. Locate the row that contains the image to be replicated, click **More** in the **Operation** column, and select **Replicate**.
4. In the displayed **Replicate Image** dialog box, set the following parameters.

   NOTE

   If the current region does not support cross-region replication, set the parameters by referring to **Replicating Images Within a Region**.

Figure 5-17 Replicating an image across regions



Replicate Image

- The image size must be less than 128 GiB.

Image Details

Name	[redacted]	Image Type	ECS system disk image
Image Size	993 MiB	OS Type	Linux
OS	CentOS 7.4 64bit	Created	Mar 21, 2024 15:46:45 GMT+08:00

Replication Mode: Within Region / **Across Regions**

* Name: copy_[redacted]

* Destination Region: --Select-- Available Region

* Destination Project: --Select--

* IAM Agency: —Select— View Agency

Description: 0/1,024

Disclaimer: □ I have read and agree to the disclaimer.
Cross-region replication migrates your data stored on OBS from one region to another. You understand and agree that this cloud platform is not aware of the content of your data and is not responsible for the legal compliance of its use. If your replication involves cross-border transfer, ensure that your use complies with relevant laws and regulations.

Cancel OK

- **Replication Mode**: Select **Across Regions**.
- **Name**: Enter a name that is easy to identify. The image name is in the following format: **copy_***Name of the source region where the image is located_Source image name*.
- **Destination Region**: Select the region where you want to use the image.
- **Destination Project**: Select a project in the destination region. After you select the destination region, the system automatically displays available projects.
- **Target Server Backup Vault**: This parameter is available only for full-ECS images created using CBR backups. Select a vault for storing backups.

  If no CBR backup vault is available in the destination region, click **Create Server Backup Vault** to create one. Ensure that you select **Replication** for **Protection Type**. For other parameters, see **Purchasing a Server Backup Vault**. After the vault is created, click ↻ to refresh the page and select the vault from the drop-down list box.
- **IAM Agency**: Select an IAM agency.
- (Optional) **Description**: Describe the replication.
- **Disclaimer**: Read the disclaimer and select **I have read and agree to the disclaimer**.

5. Click **OK**.

   Switch to the destination region. If the image status becomes **Normal**, the image replication is successful.

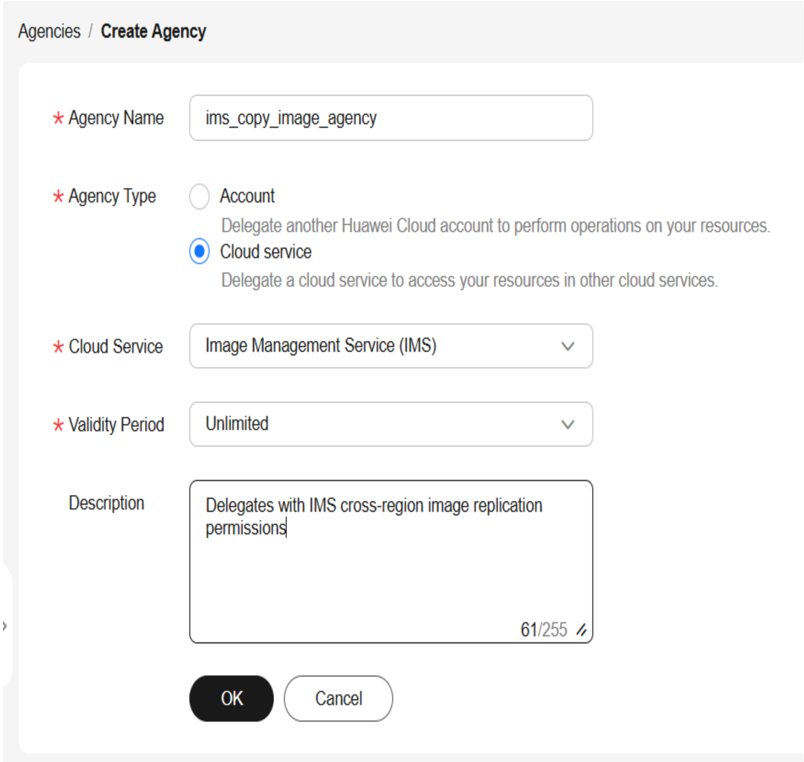
NOTE

The time required for replicating an image across regions depends on the network speed, image size, and the number of concurrent tasks.

Create an Agency

1. Log in to the management console.
2. In the upper right corner of the page, click the username and select **Identity and Access Management**.
3. In the navigation pane, choose **Agencies**.
4. Click **Create Agency**.
5. Set the following parameters:
   - **Agency Name**: Enter an agency name, for example, **ims_copy_image_agency**.

     Figure 5-18 Creating an agency

     Agencies / Create Agency

     * Agency Name: ims_copy_image_agency

     * Agency Type: ○ Account
     Delegate another Huawei Cloud account to perform operations on your resources.
     ● Cloud service
     Delegate a cloud service to access your resources in other cloud services.

     * Cloud Service: Image Management Service (IMS)

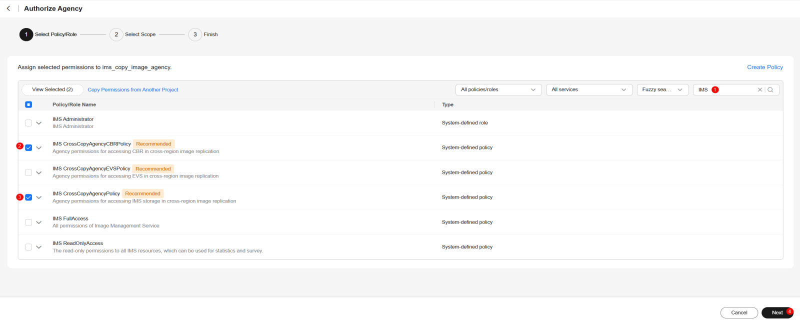
     * Validity Period: Unlimited

     Description: Delegates with IMS cross-region image replication permissions

     61/255

   - **Agency Type**: Select **Cloud service**.
   - **Cloud Service**: This parameter is available only if you select **Cloud service** for **Agency Type**. Select **Image Management Service (IMS)** from the drop-down list.
   - **Validity Period**: Select **Unlimited**.
   - **Description**: This parameter is optional. You can enter "Delegates with IMS cross-region replication permissions".
6. Click **OK**. In the displayed dialog box, click **Authorize**. Select the permissions to be granted to the agency based on the image type.

Figure 5-19 Granting permissions to an agency



Authorize Agency

1 Select Policy/Role — 2 Select Scope — 3 Finish

Assign selected permissions to ims_copy_image_agency.

Create Policy

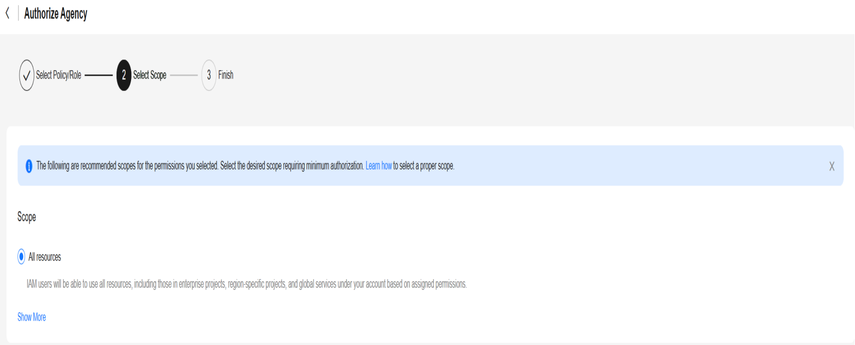
View Selected (2)   Copy Permissions from Another Project   All policies/roles   All services   Fuzzy sea...   IMS

	Policy/Role Name	Type
☐	IMS Administrator IMS Administrator	System-defined role
☑	IMS CrossCopyAgencyCBRPolicy Recommended Agency permissions for accessing CBR in cross-region image replication	System-defined policy
☐	IMS CrossCopyAgencyEVSPolicy Recommended Agency permissions for accessing EVS in cross-region image replication	System-defined policy
☑	IMS CrossCopyAgencyPolicy Recommended Agency permissions for accessing IMS storage in cross-region image replication	System-defined policy
☐	IMS FullAccess All permissions of Image Management Service	System-defined policy
☐	IMS ReadOnlyAccess The read-only permissions to all IMS resources, which can be used for statistics and survey.	System-defined policy

Cancel   Next

7. Click **Next** and specify the authorization scope.

Figure 5-20 Specifying the authorization scope



Authorize Agency

Select Policy/Role — 2 Select Scope — 3 Finish

The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization. Learn how to select a proper scope.

Scope

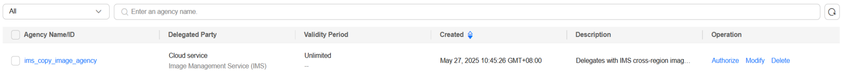
● All resources

IAM users will be able to use all resources, including those in enterprise projects, region-specific projects, and global services under your account based on assigned permissions.

Show More

8. Click **OK**.

Figure 5-21 New agency



All   Enter an agency name.

Agency Name/ID	Delegated Party	Validity Period	Created	Description	Operation
ims_copy_image_agency	Cloud service Image Management Service (IMS)	Unlimited --	May 27, 2025 10:45:26 GMT+08:00	Delegates with IMS cross-region imag...	Authorize Modify Delete

NOTE

If the Tenant Administrator or IMS Administrator role is in the permission list, you are advised to delete them to avoid risks caused by excessive permissions. IMS provides fine-grained system policies to allow you to minimize permissions. For example, if the permissions of the agent for cross-region image replication are excessive, you are advised to grant only permissions in the following table.

Table 5-1 Permissions required for cross-region image replication

Scenario	System-defined Policy
Cross-region replication of a system or data disk image	IMS CrossCopyAgencyPolicy
Cross-region replication of a full-ECS image	IMS CrossCopyAgencyCBRPolicy

6 Managing Public Images

6.1 Overview

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

Public Image Types

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

For more information, see **Differences Between openEuler, EulerOS, and Huawei Cloud EulerOS**.

Table 6-1 Public image types

Image Type	Description
Huawei Cloud EulerOS	Huawei Cloud EulerOS (HCE) is an openEuler-based cloud operating system. HCE provides a secure cloud native OS environment with high performance. It is easy to migrate from other OS to HCEOS. This accelerates service migration to the cloud and promotes application innovation. You can use it to replace operating systems such as CentOS and EulerOS.

Image Type	Description
EulerOS	EulerOS is an enterprise-class commercial Linux distribution. It features high security, scalability, and performance, meeting customers' requirements for IT infrastructure and cloud computing services. **NOTE** EulerOS is developed based on openEuler and is a Huawei internal OS.
Third-party commercial image	Third-party images have been rigorously tested and licensed before they are released on Huawei Cloud to ensure that they are highly secure and stable. Third-party public images include: ● Windows: Windows Server ● Linux: Ubuntu, CentOS, openSUSE, Debian, Fedora, FreeBSD, and CoreOS

NOTE

The available image OSs vary depending on server flavors:

- **OSs Supported by Different Types of ECSs**
- **OSs Supported by Different Types of BMSs**

Public Image Characteristics

- OS types: Linux and Windows OSs that are updated and maintained periodically

  For details about the public image update history, see **Image Update History (x86)**.

- Supported software: Public images contain some plug-ins on which server networks and basic functions depend.

  NOTE

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

Table 6-2 Supported software

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

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

Differences Between openEuler, EulerOS, and Huawei Cloud EulerOS

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

6.2 Image Update History (x86)

This section describes the update history of public images (x86).

2025-05-31

OS	Image	Details
Debian	Image names: ● Debian 12.0.0 64bit ● Debian 11.6.0 64bit ● Debian 11.1.0 64 bit	● Upgraded the OS kernel version to rectify security vulnerabilities. ● Updated plug-ins, such as the one-click password reset plug-in and HSS plug-ins.
	Kernel versions: ● Debian 12.0.0: 6.1.0-35-amd64 ● Debian 11.6.0: 5.10.0-34-amd64 ● Debian 11.1.0: 5.10.0-34-amd64	
	Regions: all	
Rocky Linux	Image names: ● Rocky Linux 9.5 64bit ● Rocky Linux 9.4 64bit ● Rocky Linux 9.3 64bit ● Rocky Linux 9.2 64bit ● Rocky Linux 9.0 64bit ● Rocky Linux 8.8 64bit ● Rocky Linux 8.5 64bit ● Rocky Linux 8.4 64bit	● Launched the Rocky Linux 9.5, Rocky Linux 9.4, and Rocky Linux 9.3 images. ● Upgraded the OS kernel version of other images to rectify security vulnerabilities. ● Updated plug-ins, such as the one-click password reset plug-in and HSS plug-ins.
	Kernel versions: ● Rocky 9.5: 5.14.0-503.40.1.el9_5.x86_64 ● Rocky 9.4: 5.14.0-503.40.1.el9_5.x86_64 ● Rocky 9.3: 5.14.0-503.38.1.el9_5.x86_64 ● Rocky 9.2: 5.14.0-503.38.1.el9_5.x86_64 ● Rocky 9.0: 5.14.0-503.40.1.el9_5.x86_64 ● Rocky 8.8: 4.18.0-553.54.1.el8_10.x86_64 ● Rocky 8.5: 4.18.0-553.54.1.el8_10.x86_64 ● Rocky 8.4: 4.18.0-553.54.1.el8_10.x86_64	

OS	Image	Details
	Regions: all	
Ubuntu	Image names: ● Ubuntu 24.04 64bit ● Ubuntu 22.04 64bit	● Upgraded the OS kernel version to rectify security vulnerabilities. ● Updated plug-ins, such as the one-click password reset plug-in and HSS plug-ins.
	Kernel versions: ● Ubuntu 24.04: 6.8.0-59-generic ● Ubuntu 22.04: 5.15.0-138-generic	
	Regions: all	
Huawei Cloud EulerOS 2.0	Image name: Huawei Cloud EulerOS 2.0 Standard 64 bit	● Upgraded the OS kernel version to rectify security vulnerabilities. ● Updated plug-ins, such as the one-click password reset plug-in and HSS plug-ins.
	Kernel version: 5.10.0-182.0.0.95.r2673_211.hce2.x86_64	
	Regions: all	
AlmaLinux	Image names: ● AlmaLinux 9.0 64bit ● AlmaLinux 8.4 64bit ● AlmaLinux 8.3 64bit	● Upgraded the OS kernel version to rectify security vulnerabilities. ● Updated plug-ins, such as the one-click password reset plug-in and HSS plug-ins.
	Kernel versions: ● AlmaLinux 9.0: 5.14.0-503.40.1.el9_5.x86_64 ● AlmaLinux 8.4: 4.18.0-553.54.1.el8_10.x86_64 ● AlmaLinux 8.3: 4.18.0-553.54.1.el8_10.x86_64	
	Regions: all	
CentOS Stream	Image names: CentOS Stream 9 64bit	● Upgraded the OS kernel version to rectify security vulnerabilities. ● Updated plug-ins, such as the one-click password reset plug-in and HSS plug-ins.
	Kernel version: CentOS Stream 9 64bit: 5.14.0-587.el9.x86_64	
	Regions: all	

2024-05-31

OS	Image	Details
Debian	Image names: - Debian 11.1.0 64bit - Debian 10.0.0 64bit	- Upgraded the OS kernel versions to rectify security vulnerabilities. - Updated plug-ins, such as the one-click password reset plug-in and Cloud Eye plug-ins.
	Kernel versions: - Debian 11.1.0: 5.10.0-28-amd64 - Debian 10.0.0: 4.19.0-26-amd64	
	Regions: all	
Rocky Linux	Image names: - Rocky Linux 9.0 64bit - Rocky Linux 8.5 64bit - Rocky Linux 8.4 64bit	- Upgraded the OS kernel versions to rectify security vulnerabilities. - Updated plug-ins, such as the one-click password reset plug-in and Cloud Eye plug-ins.
	Kernel versions: - Rocky 9.0: 5.14.0-362.24.1.el9_3.x86_64 - Rocky 8.5: 4.18.0-513.18.1.el8_9.x86_64 - Rocky 8.4: 4.18.0-513.18.1.el8_9.x86_64	
	Regions: all	
AlmaLinux	Image names: - AlmaLinux 9.0 64bit - AlmaLinux 8.4 64bit - AlmaLinux 8.3 64bit	- Upgraded the OS kernel versions to rectify security vulnerabilities. - Updated plug-ins, such as the one-click password reset plug-in and Cloud Eye plug-ins.
	Kernel versions: - AlmaLinux 9.0: 5.14.0-362.18.1.el9_3.x86_64 - AlmaLinux 8.4: 4.18.0-513.18.1.el8_9.x86_64 - AlmaLinux 8.3: 4.18.0-513.18.1.el8_9.x86_64	
	Regions: all	

OS	Image	Details
CentOS Stream	Image names: - CentOS Stream 8 64bit - CentOS Stream 9 64bit	- Upgraded the OS kernel versions to rectify security vulnerabilities. - Updated plug-ins, such as the one-click password reset plug-in and Cloud Eye plug-ins.
	Kernel versions: CentOS Stream 8 64bit: 4.18.0-544.el8.x86_64 CentOS Stream 9 64bit: 5.14.0-437.el9.x86_64	
	Regions: all	

2024-04-18

OS	Image	Details
CentOS	Image names: - CentOS 7.4 64bit - CentOS 7.5 64bit - CentOS 7.6 64bit - CentOS 7.7 64bit - CentOS 7.8 64bit - CentOS 7.9 64bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Updated plug-ins, such as the one-click password reset plug-in and Cloud Eye plug-ins.
	Kernel version: CentOS 7: 3.10.0-1160.108.1.el7.x86_64	
	Regions: all	
Ubuntu	Image names: - Ubuntu 20.04 server 64bit - Ubuntu 22.04 server 64bit	- Upgraded the OS kernel versions to rectify security vulnerabilities. - Updated plug-ins, such as the one-click password reset plug-in and Cloud Eye plug-ins.
	Kernel versions: - Ubuntu 20.04: 5.4.0-170-generic - Ubuntu 22.04: 5.15.0-92-generic	
	Regions: all	

OS	Image	Details
Huawei Cloud EulerOS 2.0	Image name: Huawei Cloud EulerOS 2.0 Standard 64 bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Updated plug-ins, such as the one-click password reset plug-in and Cloud Eye plug-ins.
	Kernel version: 5.10.0-60.18.0.50.r1083_58.hce2.x86_64	
	Regions: all	

2024-03-29

OS	Image	Details
Debian	Image name: Debian 12.0.0	Released the image.
	Kernel version: Debian 12.0.0: 6.1.0-18-amd64	
	Regions: all	

2023-09-07

OS	Image	Details
openEuler	Image name: openEuler 22.03 64bit	Released the image.
	Kernel version: 5.10.0-60.109.0.136.oe2203.x86_64	
	Regions: all	

2023-08-23

OS	Image	Details
Debian	Image names: ● Debian 11.1.0 64bit ● Debian 10.0.0 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Deleted the kernel parameter **kernel.unknown_nmi_panic**. ● Updated the one-click password reset plug-in.
	Kernel versions: ● Debian 11.1.0: 5.10.0-23-amd64 ● Debian 10.0.0: 4.19.0-25-amd64	
	Regions: all	
Rocky Linux	Image names: ● Rocky Linux 9.0 64bit ● Rocky Linux 8.5 64bit ● Rocky Linux 8.4 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Deleted the kernel parameter **kernel.unknown_nmi_panic**. ● Updated the one-click password reset plug-in.
	Kernel versions: ● Rocky 9.0: 5.14.0-284.25.1.el9_2.x86_64 ● Rocky 8.5: 4.18.0-477.15.1.el8_8.x86_64 ● Rocky 8.4: 4.18.0-477.15.1.el8_8.x86_64	
	Regions: all	
AlmaLinux	Image names: ● AlmaLinux 9.0 64bit ● AlmaLinux 8.4 64bit ● AlmaLinux 8.3 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Deleted the kernel parameter **kernel.unknown_nmi_panic**. ● Updated the one-click password reset plug-in.
	Kernel versions: ● AlmaLinux 9.0: 5.14.0-284.25.1.el9_2.x86_64 ● AlmaLinux 8.4: 4.18.0-477.21.1.el8_8.x86_64 ● AlmaLinux 8.3: 4.18.0-477.21.1.el8_8.x86_64	

OS	Image	Details
	Regions: all	
CentOS	Image names: ● CentOS 8.0 64bit ● CentOS 8.1 64bit ● CentOS 8.2 64bit	● Deleted the kernel parameter **kernel.unknown_nmi_panic**. ● Updated the one-click password reset plug-in.
	Kernel versions: ● CentOS 8.0: 4.18.0-348.7.1.el8_5.x86_64 ● CentOS 8.1: 4.18.0-348.7.1.el8_5.x86_64 ● CentOS 8.2: 4.18.0-348.7.1.e18_5.x86_64	
	Regions: all	

2023-08-16

OS	Image	Details
CentOS Stream	Image names: ● CentOS Stream 9 64bit ● CentOS Stream 8 64bit	Released the images.
	Kernel versions: ● CentOS Stream 9: 5.14.0-352.el9.x86_64 ● CentOS Stream 8: 4.18.0-500.el8.x86_64	
	Regions: all	

2023-07-29

OS	Image	Details
CentOS	Image names: ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit ● CentOS 7.7 64bit ● CentOS 7.8 64bit ● CentOS 7.9 64bit	● Upgraded the OS kernel version to rectify security vulnerabilities. ● Deleted the kernel parameter **kernel.unknown_nmi_panic**. ● Updated the one-click password reset plug-in.

OS	Image	Details
	Kernel version: CentOS 7: 3.10.0-1160.92.1.el7.x86_64	
	Regions: all	
Ubuntu	Image names: - Ubuntu 16.04 server 64bit - Ubuntu 18.04 server 64bit - Ubuntu 20.04 server 64bit - Ubuntu 22.04 server 64bit	- Upgraded the OS kernel versions to rectify security vulnerabilities. - Deleted the kernel parameter **kernel.unknown_nmi_panic**. - Updated the one-click password reset plug-in.
	Kernel versions: - Ubuntu 16.04: 4.4.0-210-generic - Ubuntu 18.04: 4.15.0-213-generic - Ubuntu 20.04: 5.4.0-153-generic - Ubuntu 22.04: 5.15.0-76-generic	
	Regions: all	
EulerOS	Image name: EulerOS 2.5 64bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Deleted the kernel parameter **kernel.unknown_nmi_panic**. - Updated the one-click password reset plug-in.
	Kernel version: EulerOS 2.5: 3.10.0-862.14.1.5.757.eulerosv2r7.x86_64	
	Regions: all	
Huawei Cloud EulerOS 1.1	Image name: Huawei Cloud EulerOS 1.1 64bit for CentOS	- Upgraded the OS kernel version to rectify security vulnerabilities. - Deleted the kernel parameter **kernel.unknown_nmi_panic**. - Updated the one-click password reset plug-in.
	Kernel version: 5.10.0-60.18.0.50.r865_35.hce2.x86_64	
	Region: AP-Singapore	

2023-06-15

OS	Image	Details
Huawei Cloud EulerOS 2.0	Image name: Huawei Cloud EulerOS 2.0 Standard 64 bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Deleted the kernel parameter **kernel.unknown_nmi_panic**. - Updated the one-click password reset plug-in.
	Kernel version: 5.10.0-60.18.0.50.r865_35.hce2.x86_64	
	Regions: all	

2022-09-30

OS	Image	Details
Huawei Cloud EulerOS 2.0	Image name: Huawei Cloud EulerOS 2.0 Standard 64 bit for ARM	Released the image.
	Kernel version: 5.10.0-60.18.0.50.r509_2.hce2.x86_64	
	Region: AP-Singapore	
Huawei Cloud EulerOS 2.0	Image name: Huawei Cloud EulerOS 2.0 Standard 64 bit	Released the image.
	Kernel version: 5.10.0-60.18.0.50.h322_1.hce2.x86_64	
	Region: AP-Singapore	
Huawei Cloud EulerOS 1.1	Image name: Huawei Cloud EulerOS 1.1 64bit for CentOS	Released the image.
	Kernel versions: 3.10.0-1160.66.1.hce1c.x86_64 5.10.0-60.18.0.50.h322_1.hce2.x86_64 (default)	
	Region: AP-Singapore	

2022-03-22

OS	Image	Details
CentOS	Image names: • CentOS 6.10 64bit • CentOS 7.2 64bit • CentOS 7.3 64bit • CentOS 7.4 64bit • CentOS 7.5 64bit • CentOS 7.6 64bit • CentOS 7.7 64bit • CentOS 7.8 64bit • CentOS 7.9 64bit • CentOS 8.0 64bit • CentOS 8.1 64bit • CentOS 8.2 64bit	• Upgraded the OS kernel versions to rectify security vulnerabilities. • Updated the one-click password reset plug-in.
	Kernel versions: • CentOS 6: 2.6.32-754.35.1.el6.x86_64 • CentOS 7: 3.10.0-1160.53.1.el7.x86_64 • CentOS 8: 4.18.0-348.7.1.el8_5.x86_64	
	Regions: all	
Ubuntu	Image names: • Ubuntu 16.04 server 64bit • Ubuntu 18.04 server 64bit • Ubuntu 20.04 server 64bit	• Upgraded the OS kernel versions to rectify security vulnerabilities. • Updated the one-click password reset plug-in.
	Kernel versions: Ubuntu 16.04: 4.4.0-210-generic Ubuntu 18.04: 4.15.0-167-generic Ubuntu 20.04: 5.4.0-99-generic	
	Regions: all	
Debian	Image names: • Debian 9.0.0 64bit • Debian 10.0.0 64bit	• Upgraded the OS kernel versions to rectify security vulnerabilities. • Updated the one-click password reset plug-in.

OS	Image	Details
	Kernel versions: - Debian 9: 4.9.0-17-amd64 - Debian 10: 4.19.0-18-amd64	
	Regions: all	
EulerOS	Image name: EulerOS 2.5 64bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Updated the one-click password reset plug-in.
	Kernel version: EulerOS 2.5: 3.10.0-862.14.1.5.h654.eulerosv2r7.x86_64	
	Regions: all	

2021-05-21

OS	Image	Details
CentOS	Image names: - CentOS 7.2 64bit - CentOS 7.3 64bit - CentOS 7.4 64bit - CentOS 7.5 64bit - CentOS 7.6 64bit - CentOS 8.0 64bit - CentOS 8.1 64bit - CentOS 8.2 64bit	- Upgraded the OS kernel versions to rectify security vulnerabilities. - Installed/Updated the HSS plug-in. - Updated the one-click password reset plug-in. - Optimized the repo source configuration. - Fixed sudo vulnerabilities.
	Kernel versions: - CentOS 7: 3.10.0-1160.15.2.el7.x86_64 - CentOS 8: 4.18.0-240.10.1.el8_3.x86_64	
	Regions: all	

OS	Image	Details
Ubuntu	Image names: ● Ubuntu 16.04 server 64bit ● Ubuntu 18.04 server 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Installed/Updated the HSS plug-in. ● Updated the one-click password reset plug-in. ● Optimized the repo source configuration. ● Fixed sudo vulnerabilities.
	Kernel versions: Ubuntu 16.04: 4.4.0-201-generic Ubuntu 18.04: 4.15.0-136-generic	
	Regions: all	
Debian	Image names: ● Debian 9.0.0 64bit ● Debian 10.0.0 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Installed/Updated the HSS plug-in. ● Updated the one-click password reset plug-in. ● Optimized the repo source configuration. ● Fixed sudo vulnerabilities.
	Kernel versions: ● Debian 9: 4.9.0-14-amd64 ● Debian 10: 4.19.0-14-amd64	
	Regions: all	
EulerOS	Image names: ● EulerOS 2.5 64bit ● EulerOS 2.2 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Installed/Updated the HSS plug-in. ● Updated the one-click password reset plug-in. ● Optimized the repo source configuration. ● Fixed sudo vulnerabilities.
	Kernel versions: ● EulerOS 2.5: 3.10.0-862.14.1.5.h520 ● EulerOS 2.2: 3.10.0-327.62.59.83.h255	
	Regions: all	

2021-04-28

OS	Image	Details
CentOS	Image names: ● CentOS 7.9 64bit ● CentOS 7.8 64bit ● CentOS 7.7 64bit	Released the images.

OS	Image	Details
	Kernel version: 3.10.0-1160.15.2.el7.x86_64	
	Regions: all	

2020-12-25

OS	Image	Details
CentOS	Image names: ● CentOS 8.1 64bit ● CentOS 8.2 64bit	Released the images.
	Kernel version: 4.18.0-240.1.1.el8_3.x86_64	
	Regions: all	
CentOS	Image names: ● CentOS 7.2 64bit ● CentOS 7.3 64bit ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit ● CentOS 8.0 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Installed/Updated the UniAgent plug-in. ● Upgraded Cloud-Init to 19.1. ● Optimized configurations in resolv.conf.
	Kernel versions: ● CentOS 7: 3.10.0-1160.6.1.el7.x86_64 ● CentOS 8: 4.18.0-240.1.1.el8_3.x86_64	
	Regions: all	
Ubuntu	Image names: ● Ubuntu 16.04 server 64bit ● Ubuntu 18.04 server 64bit ● Ubuntu 20.04 server 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Installed/Updated the UniAgent plug-in. ● Upgraded Cloud-Init to 19.1. ● Optimized configurations in resolv.conf.
	Kernel versions: ● Ubuntu 16.04: 4.4.0-197-generic ● Ubuntu 18.04: 4.15.0-128-generic ● Ubuntu 20.04: 5.4.0-58-generic	

OS	Image	Details
	Regions: all	

2020-10-09

OS	Image	Details
Ubuntu	Image name: Ubuntu 20.04 64bit	Released the image.
	Kernel version: 5.4.0-47-generic	
	Regions: all	

2020-07-23

OS	Image	Details
Windows Server 2012 R2	Image names: ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter	● Updated OS patches. ● Updated the HSS plug-in. ● Updated the one-click password reset plug-in. ● Deleted the script task of automatically initializing disks.
	Regions: all	
Windows Server 2016	Image names: ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter	
	Regions: all	
Windows Server 2019	Image name: Windows Server 2019 Datacenter	
	Regions: all	

2020-07-15

OS	Image	Details
Windows Server 2008 R2	Image names: ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 R2 Web	Taken the images offline.
	Regions: all	

2020-05-18

OS	Image	Details
openEuler	Image name: openEuler 20.03 64bit	Released the image.
	Kernel version: 4.19.90-2003.4.0.0036.oel.x86_64	
	Regions: all	

2020-04-30

OS	Image	Details
CentOS	Image names: ● CentOS 6.5 64bit ● CentOS 6.8 64bit ● CentOS 6.9 64bit ● CentOS 6.10 64bit ● CentOS 7.2 64bit ● CentOS 7.3 64bit ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Updated the one-click password reset plug-in. ● Updated the HSS plug-in. ● Optimized kernel parameters related to serial ports. ● Disabled NTP and enabled chrony.

OS	Image	Details
	Kernel versions: ● CentOS 6: 2.6.32-754.27.1.el6.x86_64 ● CentOS 7: 3.10.0-1062.12.1.el7.x86_64	
	Regions: all	

2020-04-24

OS	Image	Details
Debian	Image names: ● Debian 9.0.0 64bit ● Debian 10.0.0 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Updated the one-click password reset plug-in. ● Updated the HSS plug-in. ● Optimized kernel parameters related to serial ports. ● Disabled NTP and enabled chrony.
	Kernel versions: ● Debian 10: 4.19.0-8-amd64 ● Debian 9: 4.9.0-12-amd64	
	Regions: all	
Ubuntu	Image names: ● Ubuntu 18.04 64bit ● Ubuntu 16.04 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Updated the one-click password reset plug-in. ● Updated the HSS plug-in. ● Optimized kernel parameters related to serial ports. ● Disabled NTP and enabled chrony.
	Kernel versions: ● Ubuntu 18: 4.15.0-91-generic ● Ubuntu 16: 4.4.0-176-generic	
	Regions: all	

OS	Image	Details
EulerOS	Image names: ● EulerOS 2.5 64bit ● EulerOS 2.3 64bit ● EulerOS 2.2 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Updated the one-click password reset plug-in. ● Updated the HSS plug-in. ● Optimized kernel parameters related to serial ports. ● Disabled NTP and enabled chrony.
	Kernel versions: ● EulerOS 2.2: 3.10.0-327.62.59.83.h195.x86_64 ● EulerOS 2.3: 3.10.0-514.44.5.10.h234.x86_64 ● EulerOS 2.5: 3.10.0-862.14.1.5.h428.eulerosv2r7.x86_64	
	Regions: all	
openSUSE	Image name: openSUSE 15.0 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Updated the one-click password reset plug-in. ● Updated the HSS plug-in. ● Optimized kernel parameters related to serial ports. ● Disabled NTP and enabled chrony.
	Kernel version: 4.12.14-lp150.12.82-default	
	Regions: all	
Fedora	Image name: Fedora 30 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Updated the one-click password reset plug-in. ● Updated the HSS plug-in. ● Optimized kernel parameters related to serial ports. ● Disabled NTP and enabled chrony.
	Kernel version: 5.5.10-100.fc30.x86_64	
	Regions: all	

2020-03-27

OS	Image	Details
CentOS	Image name: CentOS 8.0 64bit	Released the image.
	Kernel version: 4.18.0-147.5.1.e18_1.x86_64	
	Regions: all	

2020-03-24

OS	Image	Details
Debian	Image names: ● Debian 8.2.0 64bit ● Debian 8.8.0 64bit	● Updated the one-click password reset plug-in. ● Updated the HSS plug-in. ● Optimized kernel parameters related to serial ports. ● Disabled NTP and enabled chrony.
	Kernel version: 3.16.0-4-amd64	
	Regions: all	

2020-03-19

OS	Image	Details
Windows Server 2016	Image names: ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter	● Updated UVP VMTools and PV drivers. ● Updated the one-click password reset plug-in. ● Updated the HSS plug-in. ● Rectified the AD domain installation failure. ● Updated OS patches.
	Regions: all	
Windows Server 2019	Image name: Windows Server 2019 Datacenter	
	Regions: all	

2020-03-17

OS	Image	Details
Windows Server 2012 R2	Image names: ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter	● Updated the one-click password reset plug-in. ● Updated the HSS plug-in. ● Rectified the AD domain installation failure. ● Updated OS patches.
	Regions: all	

2019-12-13

OS	Image	Details
Windows Server 2012 R2	Image names: ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter	● Updated OS patches. ● Updated the HSS plug-in.
	Regions: all	
Windows Server 2016	Image names: ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter	
	Regions: all	
Windows Server 2019	Image name: Windows Server 2019 Datacenter	● Updated OS patches. ● Updated the HSS plug-in.
	Regions: all	
Windows Server 2008 R2	Image names: ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 Web	● Updated OS patches. ● Updated the HSS plug-in.
	Regions: all	

2019-11-06

OS	Image	Details
Debian	Image names: ● Debian 10.0.0 64bit ● Debian 8.8.0 64bit ● Debian 8.2.0 64bit	● Upgraded the OS kernel versions to rectify security vulnerabilities. ● Optimized Debian 10.0.0 kernel parameters.
	Kernel versions: ● Debian 10: 4.19.0-6-amd64 ● Debian 8: 3.16.0-10-amd64	
	Regions: all	
Fedora	Image name: Fedora 30 64bit	● Upgraded the OS kernel version to rectify security vulnerabilities. ● Optimized kernel parameters.
	Kernel version: 5.3.7-200.fc30.x86_64	
	Regions: all	
openSUSE	Image name: openSUSE 15.0 64bit	Upgraded the OS kernel version to rectify security vulnerabilities.
	Kernel version: 4.12.14-1p150.12.79-default	
	Regions: all	

2019-11-05

OS	Image	Details
CentOS	Image names: ● CentOS 6.5 64bit ● CentOS 6.8 64bit ● CentOS 6.9 64bit ● CentOS 6.10 64bit	Upgraded the OS kernel version to rectify security vulnerabilities.
	Kernel version: 2.6.32-754.23.1.e16.x86_64	
	Regions: all	

2019-10-15

OS	Image	Details
Debian	Image names: - Debian 9.0.0 64bit - Debian 8.8.0 64bit - Debian 8.2.0 64bit	- Updated OS patches to rectify security vulnerabilities. - Upgraded the Debian 9.0.0 kernel version. - Updated the NIC multi-queue plug-in. - Optimized kernel parameters.
	Kernel versions: - Debian 9: 4.9.0-11-amd64 - Debian 8: 3.16.0-9-amd64	
	Regions: all	
Fedora	Image name: Fedora 29 64bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Updated the NIC multi-queue plug-in. - Optimized kernel parameters.
	Kernel version: 5.1.11-200.fc29.x86_64	
	Regions: all	
openSUSE	Image name: openSUSE 15.0 64bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Updated the NIC multi-queue plug-in. - Optimized kernel parameters.
	Kernel version: 4.12.14-1p150.12.64-default	
	Regions: all	
Ubuntu	Image names: - Ubuntu 18.04 64bit - Ubuntu 16.04 64bit	- Upgraded the OS kernel versions to rectify security vulnerabilities. - Updated the NIC multi-queue plug-in. - Optimized kernel parameters.
	Kernel versions: - Ubuntu 18.04: 4.15.0-65-generic - Ubuntu 16.04: 4.4.0-165-generic	
	Regions: all	

2019-10-10

OS	Image	Details
CentOS	Image names: - CentOS 6.5 64bit - CentOS 6.8 64bit - CentOS 6.9 64bit - CentOS 6.10 64bit	- Updated OS patches to rectify security vulnerabilities. - Updated the NIC multi-queue plug-in. - Optimized kernel parameters.
	Kernel version: 2.6.32-754.15.3.e16.x86_64	
	Regions: all	

2019-09-29

OS	Image	Details
CentOS	Image names: - CentOS 7.2 64bit - CentOS 7.3 64bit - CentOS 7.4 64bit - CentOS 7.5 64bit - CentOS 7.6 64bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Updated the NIC multi-queue plug-in. - Optimized kernel parameters.
	Kernel version: 3.10.0-1062.1.1.e17.x86_64	
	Regions: all	

2019-08-29

OS	Image	Details
Debian	Image names: - Debian 9.0.0 64bit - Debian 8.8.0 64bit - Debian 8.2.0 64bit	- Updated the NIC multi-queue plug-in. - Rectified the apt source in the Debian OS.
	Kernel versions: - Debian 9: 4.9.0-9-amd64 - Debian 8: 3.16.0-9-amd64	
	Regions: all	

2019-08-26

OS	Image	Details
Windows Server 2008 R2	Image names: ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 Web	● Updated UVP VMTools and PV drivers. ● Updated OS patches. ● Optimized the timeout duration of Cloudbase-Init.
	Regions: all	

2019-08-21

OS	Image	Details
Windows Server 2016	Image names: ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter	● Updated UVP VMTools and PV drivers. ● Updated OS patches.
	Regions: all	
Windows Server 2019	Image name: Windows Server 2019 Datacenter	
	Regions: all	

2019-08-19

OS	Image	Details
Windows Server 2012 R2	Image names: ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter	● Updated UVP VMTools and PV drivers. ● Updated OS patches.
	Regions: all	

2019-06-29

OS	Image	Details
EulerOS	Image names: - EulerOS 2.2 64bit - EulerOS 2.3 64bit	Updated OS patches to rectify the SACK vulnerability of the Linux kernel.
	Kernel versions: - EulerOS 2.2: 3.10.0-327.62.59.83.h162.x86_64 - EulerOS 2.3: 3.10.0-514.44.5.10.h198.x86_64	
	Regions: all	

2019-06-27

OS	Image	Details
Fedora	Image name: Fedora 29 64bit	Updated OS patches to rectify the SACK vulnerability of the Linux kernel.
	Kernel version: 5.1.11-200.fc29.x86_64	
	Regions: all	
openSUSE	Image name: openSUSE 15.0 64bit	Updated OS patches to rectify the SACK vulnerability of the Linux kernel.
	Kernel version: 4.12.14-1p150.12.64-default	
	Regions: all	

2019-06-26

OS	Image	Details
CentOS	Image names: ● CentOS 6.5 64bit ● CentOS 6.8 64bit ● CentOS 6.9 64bit ● CentOS 6.10 64bit ● CentOS 7.2 64bit ● CentOS 7.3 64bit ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit	Updated OS patches to rectify the SACK vulnerability of the Linux kernel.
	Kernel versions: ● CentOS 6: 2.6.32-754.15.3.e16.x86_64 ● CentOS 7: 3.10.0-957.21.3.e17.x86_64	
	Regions: all	
Ubuntu	Image names: ● Ubuntu 18.04 64bit ● Ubuntu 16.04 64bit	Updated OS patches to rectify the SACK vulnerability of the Linux kernel.
	Kernel versions: ● Ubuntu 18.04: 4.15.0-52-generic ● Ubuntu 16.04: 4.4.0-151-generic	
	Regions: all	
Debian	Image names: ● Debian 9.0.0 64bit ● Debian 8.8.0 64bit ● Debian 8.2.0 64bit	Updated OS patches to rectify the SACK vulnerability of the Linux kernel.
	Kernel versions: ● Debian 9: 4.9.0-9-amd64 ● Debian 8: 3.16.0-9-amd64	
	Regions: all	

2019-06-23

OS	Image	Details
Windows Server 2012 R2	Image names: ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter	Updated OS patches.
	Regions: all	
Windows Server 2016	Image names: ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter	Updated OS patches.
	Regions: all	
Windows Server 2019	Image name: Windows Server 2019 Datacenter	Updated OS patches.
	Regions: all	

2019-06-19

OS	Image	Details
Windows Server 2008 R2	Image names: ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 Web	Updated OS patches.
	Regions: all	

2019-06-05

OS	Image	Details
CentOS	Image names: - CentOS 6.5 64bit - CentOS 6.8 64bit - CentOS 6.9 64bit - CentOS 6.10 64bit - CentOS 7.2 64bit - CentOS 7.3 64bit - CentOS 7.4 64bit - CentOS 7.5 64bit - CentOS 7.6 64bit	- Optimized DNS configuration. - Updated the one-click password reset plug-in. - Rectified NIC name disorder of CentOS 6. - Uninstalled the CentOS 7 qemu-guest-agent software package.
	Kernel versions: - CentOS 6: 2.6.32-754.10.1.e16.x86_64 - CentOS 7: 3.10.0-957.5.1.e17.x86_64	
	Regions: all	
EulerOS	Image names: - EulerOS 2.2 64bit - EulerOS 2.3 64bit	- Optimized DNS configuration. - Updated the one-click password reset plug-in. - Rectified the issue that the hot swap of the EulerOS image NIC does not take effect.
	Kernel versions: - EulerOS 2.2: 3.10.0-327.62.59.83.h128.x86_64 - EulerOS 2.3: 3.10.0-514.44.5.10.h142.x86_64	
	Regions: all	

2019-06-03

OS	Image	Details
Ubuntu	Image names: - Ubuntu 18.04 64bit - Ubuntu 16.04 64bit - Ubuntu 14.04 64bit - Ubuntu 14.04 32bit	- Optimized DNS configuration. - Updated the one-click password reset plug-in. - Optimized kernel parameters of Ubuntu images.
	Kernel versions: - Ubuntu 18.04: 4.15.0-45-generic - Ubuntu 16.04: 4.4.0-142-generic - Ubuntu 14.04: 4.4.0-141-generic	
	Regions: all	
Debian	Image names: - Debian 9.0.0 64bit - Debian 8.8.0 64bit - Debian 8.2.0 64bit	- Optimized DNS configuration. - Updated the one-click password reset plug-in. - Rectified some invalid configurations of the apt source in Debian 8.
	Kernel versions: - Debian 9: 4.9.0-8-amd64 - Debian 8: 3.16.0-7-amd64	
	Regions: all	

2019-05-24

OS	Image	Details
Windows Server 2012 R2	Image names: - Windows Server 2012 R2 Standard - Windows Server 2012 R2 Datacenter	Rectified the issue that the first backup of an ECS is too large in size.
	Regions: all	

2019-05-23

OS	Image	Details
Windows Server 2008 R2	Image names: • Windows Server 2008 R2 Standard • Windows Server 2008 R2 Datacenter • Windows Server 2008 R2 Enterprise • Windows Server 2008 Web	Rectified the issue that the first backup of an ECS is too large in size.
	Regions: all	

2019-05-22

OS	Image	Details
Windows Server 2016	Image names: • Windows Server 2016 Standard • Windows Server 2016 Datacenter	• Rectified the issue that the first backup of an ECS is too large in size. • Updated OS patches.
	Regions: all	

2019-05-16

OS	Image	Details
Windows Server 2008 R2	Image names: • Windows Server 2008 R2 Standard • Windows Server 2008 R2 Datacenter • Windows Server 2008 R2 Enterprise • Windows Server 2008 Web	• Updated OS patches. • Rectified the remote code execution vulnerability (CVE-2019-0708) of the Windows remote desktop service.
	Regions: all	

2019-04-25

OS	Image	Details
Windows Server 2019	Image names: ● Windows Server 2019 Standard ● Windows Server 2019 Datacenter	Released the images.
	Regions: all	

2019-04-19

OS	Image	Details
Windows Server 2008 R2	Image names: ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 Web	● Updated OS patches. ● Updated UVP VMTools drivers to enable online capacity expansion.
	Regions: all	
Windows Server 2012 R2	Image names: ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter	● Updated OS patches. ● Updated UVP VMTools drivers to enable online capacity expansion.
	Regions: all	
Windows Server 2016	Image names: ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter	● Updated OS patches. ● Updated UVP VMTools drivers to enable online capacity expansion.
	Regions: all	

6.3 Image Update History (Arm)

This section describes the update history of public images (Arm).

2025-05-31

OS	Image	Details
Huawei Cloud EulerOS 2.0	Image name: Huawei Cloud EulerOS 2.0 Standard 64 bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Updated plug-ins, such as the one-click password reset plug-in and HSS plug-ins.
	Kernel version: 5.10.0-182.0.0.95.r2673_211.hce2.aarch64	
	Regions: all	

2024-04-18

OS	Image	Details
Huawei Cloud EulerOS 2.0	Image name: Huawei Cloud EulerOS 2.0 Standard 64 bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Updated plug-ins, such as the one-click password reset plug-in.
	Kernel version: 5.10.0-60.18.0.50.r1083_58.hce2.aarch64	
	Regions: all	

2023-06-15

OS	Image	Details
EulerOS	Image name: EulerOS 2.8 64bit with ARM	- Upgraded the OS kernel version to rectify security vulnerabilities. - Updated the one-click password reset plug-in.
	Kernel version: 4.19.36-vhulk1907.1.0.h1393.eulerosv2r8.aarch64	
	Regions: CN-Hong Kong and AP-Bangkok	
Huawei Cloud EulerOS 2.0	Image name: Huawei Cloud EulerOS 2.0 Standard 64 bit	- Upgraded the OS kernel version to rectify security vulnerabilities. - Updated the one-click password reset plug-in.

OS	Image	Details
	Kernel version: 5.10.0-60.18.0.50.r865_35.hce2.aarch64	
	Regions: all	

2022-09-30

OS	Image	Details
Huawei Cloud EulerOS 2.0	Image name: Huawei Cloud EulerOS 2.0 Standard 64 bit	Released the image.
	Kernel version: 5.10.0-60.18.0.50.h322_1.hce2.aarch64	
	Region: AP-Singapore	

2021-05-24

OS	Image	Details
EulerOS	Image name: EulerOS 2.8 64bit with ARM	● Upgraded the OS kernel version to rectify security vulnerabilities. ● Updated the one-click password reset plug-in. ● Updated the HSS plug-in. ● Configured the default repo source. ● Disabled the dnf-makecache.timer service.
	Kernel version: 4.19.36-vhulk1907.1.0.h748.eulerosv2r8.aarch64	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, CN North-Beijing4, and LA-Sao Paulo1	

2021-04-01

OS	Image	Details
CentOS	Image names: - CentOS 8.0 64bit with ARM - CentOS 7.6 64bit with ARM - CentOS 7.5 64bit with ARM - CentOS 7.4 64bit with ARM	- Optimized configurations in resolv.conf. - Installed the HSS plug-in. - Updated the one-click password reset plug-in. - Optimized the repo source configuration. - Fixed sudo vulnerabilities.
	Kernel versions: - CentOS 8: 4.18.0-147.5.1.e18_1.aarch64 - CentOS 7: 4.18.0-80.7.2.e17.aarch64	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	
Ubuntu	Image name: Ubuntu 18.04 64bit with ARM	- Optimized configurations in resolv.conf. - Installed the HSS plug-in. - Updated the one-click password reset plug-in. - Optimized the repo source configuration. - Fixed sudo vulnerabilities.
	Kernel version: 4.15.0-70-generic	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	
OpenEuler	Image name: openEuler 20.03 64bit with ARM	- Optimized configurations in resolv.conf. - Installed the HSS plug-in. - Updated the one-click password reset plug-in. - Optimized the repo source configuration. - Fixed sudo vulnerabilities.
	Kernel version: 4.19.90-2003.4.0.0036.oel.aarch64	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	

2020-07-07

OS	Image	Details
EulerOS	Image name: EulerOS 2.8 64bit with ARM	• Upgraded the OS kernel version to rectify security vulnerabilities. • Updated the one-click password reset plug-in. • Updated the HSS plug-in. • Configured the default repo source. • Disabled the dnf-makecache.timer service.
	Kernel version: 4.19.36-vhulk1907.1.0.h748.eulerosv2r8.aarch64	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	

2020-05-18

OS	Image	Details
openEuler	Image name: openEuler 20.03 64bit with ARM	Released the image.
	Kernel version: 4.19.90-2003.4.0.0036.oel.aarch6	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	

2020-03-12

OS	Image	Details
CentOS	Image name: CentOS 8.0 64bit with ARM	Released the image.
	Kernel version: 4.18.0-147.5.1.e18_1.aarch64	

OS	Image	Details
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	
Debian	Image name: Debian 10.2.0 64bit with ARM	Released the image.
	Kernel version: 4.19.0-8-arm64	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	

2020-01-03

OS	Image	Details
CentOS	Image names: ● CentOS 7.6 64bit with ARM ● CentOS 7.5 64bit with ARM ● CentOS 7.4 64bit with ARM	● Updated NIC multi-queue. ● Optimized kernel parameters. ● Set the screen saver duration to 10s. ● Upgraded the OS kernel version to rectify security vulnerabilities. ● Installed gdisk, wget, and javac. ● Enabled the chrony service and disabled the NTP service. ● Configured four NIC configuration files for CentOS 7.6 64bit with ARM.
	Kernel version: 4.18.0-80.7.2.e17.aarch64	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	

OS	Image	Details
Ubuntu	Image name: Ubuntu 18.04 64bit with ARM	- Updated NIC multi-queue. - Optimized kernel parameters. - Upgraded the OS kernel version to rectify security vulnerabilities. - Enabled the chrony service and disabled the NTP service. - Configured DNS.
	Kernel version: 4.15.0-70-generic	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	
EulerOS	Image name: EulerOS 2.8 64bit with ARM	- Updated NIC multi-queue. - Optimized kernel parameters. - Set the screen saver duration to 10s. - Added Kernel parameters so that related logs can be viewed during ECS startup. - Upgraded the OS kernel version to rectify security vulnerabilities. - Enabled the chrony service and disabled the NTP service. - Set the password validity period to **99999**.
	Kernel version: 4.19.36-vhulk1907.1.0.h475.eulerosv2r8.aarch64	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	
openSUSE	Image name: openSUSE 15.0 64bit with ARM	- Updated NIC multi-queue. - Optimized kernel parameters. - Set the screen saver duration to 10s. - Upgraded the OS kernel version to rectify security vulnerabilities. - Enabled the chrony service and disabled the NTP service.
	Kernel version: 4.12.14-lp150.12.67-default	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	

OS	Image	Details
Fedora	Image name: Fedora 29 64bit with ARM	• Updated NIC multi-queue. • Optimized kernel parameters. • Set the screen saver duration to 10s. • Upgraded the OS kernel version to rectify security vulnerabilities. • Enabled the chrony service and disabled the NTP service. • Configured environment variables to display the execution time and operator name of each historical command.
	Kernel version: 4.18.16-300.fc29.aarch64	
	Regions: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, and CN North-Beijing4	

6.4 Known Issues

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

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

Symptom:

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

Involved images:

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

Solutions:

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

   NOTE

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

   ipconfig /renew

Occasional System Errors Triggered By Adding or Deleting NICs

Symptom:

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

- Trigger a kernel panic, and the OS automatically restarts.
- Trigger frequent software interrupts, and the network may fail to receive or send packets.

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

Involved images:

CentOS 7 public and private images

Solutions:

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

Kernels Are Occasionally Disconnected from the TCP Network

Symptom:

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

The involved images are listed in the following table.

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

Solutions:

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

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

- Debian: **apt-get update && apt search linux-image && apt-get install linux-image-***xxx*

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

OS Parameter Settings Do Not Take Effect

Symptom:

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

The involved parameters are listed in the following table.

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

Involved images:

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

Solutions:

1. Delete the built-in configuration files.

   ```
   rm -rf /etc/sysctl.d/huawei.conf
   rm -rf /etc/security/limits.d/huawei-nofile.conf
   ```

2. Modify the kernel parameter configuration files (**limits.conf** and **sysctl.conf**).

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

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

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

Symptom:

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

Involved images:

Debian 8.2.0 64bit and Debian 8.8.0 public images

Solutions:

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

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

Symptom:

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

Involved images:

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

Solutions:

Upgrade VMTools of involved ECSs to 2.5.0.156 or later.

Service Interruptions Caused By Lingering CLOSE_WAIT Connections

Symptom:

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

Involved images:

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

Solutions:

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

7 Managing Tags

Scenarios

You can use tags to classify images. You can add, modify, or delete image tags, or search for required images by tag in the image list.

NOTE

- When adding predefined tags to an image or searching for an image using predefined tags, you must have permission to access the Tag Management Service (TMS).
- If your organization has pre-configured tag policies for images, you need to add tags to your images based on the policies. If you do not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies.
  - Each tag consists of a key and a value. A key contains a maximum of 36 characters, and a value contains a maximum of 43 characters. A key cannot be left blank or be an empty string. A value cannot be left blank but can be an empty string.
  - An image can have a maximum of 10 tags.

Constraints

An image can have a maximum of 10 tags.

Add, Delete, and Modify Image Tags

1. Access the IMS console.
   a. Log in to the management console.
   b. Under **Compute**, click **Image Management Service**.
      The IMS console is displayed.
2. Click the **Private Images** tab and click the image name to display the image details.
   - To modify an image tag, go to **3**.
   - To delete an image tag, go to **4**.
   - To add an image tag, go to **5**.
3. Click the **Tags** tab, locate the target tag, and click **Edit** in the **Operation** column. In the displayed dialog box, modify the tag.

4. Click the **Tags** tab, locate the target tag, and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.
5. Click the **Tags** tab and then **Add Tag**. In the displayed dialog box, add a tag.

Search for Private Images by Tag

1. Access the IMS console.
   a. Log in to the management console.
   b. Under **Compute**, click **Image Management Service**.
      The IMS console is displayed.
2. Click the **Private Images** tab and click the search box above the private image list. Specify tag keys and values under **Resource Tag** to search for private images.

Figure 7-1 Searching for images by tag

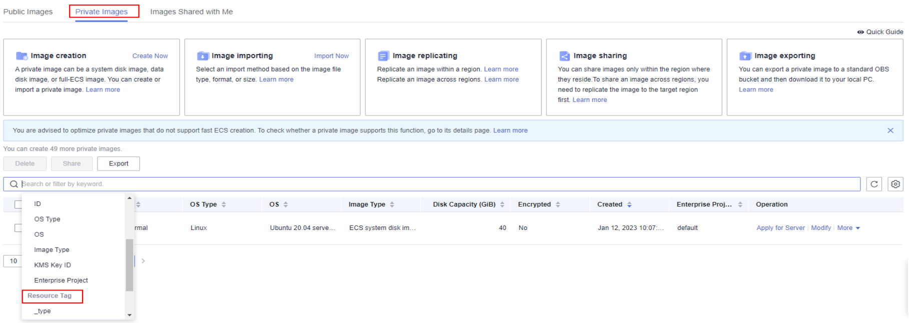


Image creation
A private image can be a system disk image, data disk image, or full-ECS image. You can create or import a private image. Learn more

Image importing
Select an import method based on the image file type, format, or size. Learn more

Image replicating
Replicate an image within a region. Learn more
Replicate an image across regions. Learn more

Image sharing
You can share images only within the region where they reside.To share an image across regions, you need to replicate the image to the target region first. Learn more

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

You are advised to optimize private images that do not support fast ECS creation. To check whether a private image supports this function, go to its details page. Learn more

You can create 49 more private images.

	OS Type	OS	Image Type	Disk Capacity (GiB)	Encrypted	Created	Enterprise Proj...	Operation
rmal	Linux	Ubuntu 20.04 serve...	ECS system disk im...	40	No	Jan 12, 2023 10:07:...	default	Apply for Server | Modify | More

NOTE

- Neither the tag key nor tag value can be empty. When the tag key and tag value are matched, the system automatically shows your desired private images.
- You can add multiple tags to search for shared images. The system will display private images that match all tags.

8 Managing Quotas

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECS or EVS disks that can be created.

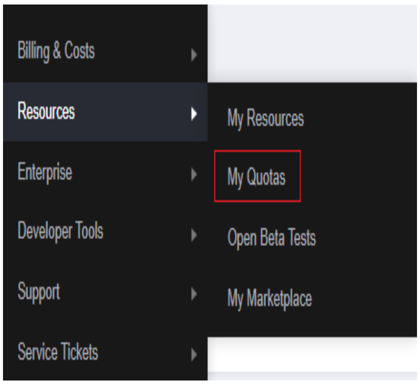
If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Quotas** page is displayed.

   Figure 8-1 My Quotas

4. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

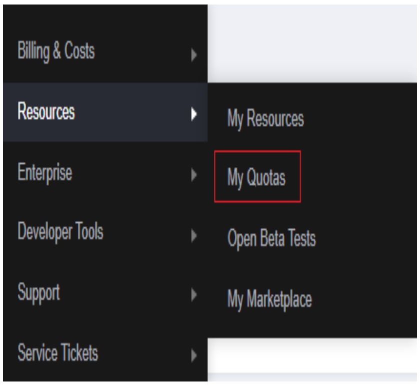
How Do I Apply for a Higher Quota?

1. Log in to the management console.

2. In the upper right corner of the page, choose **Resources** > **My Quotas**.

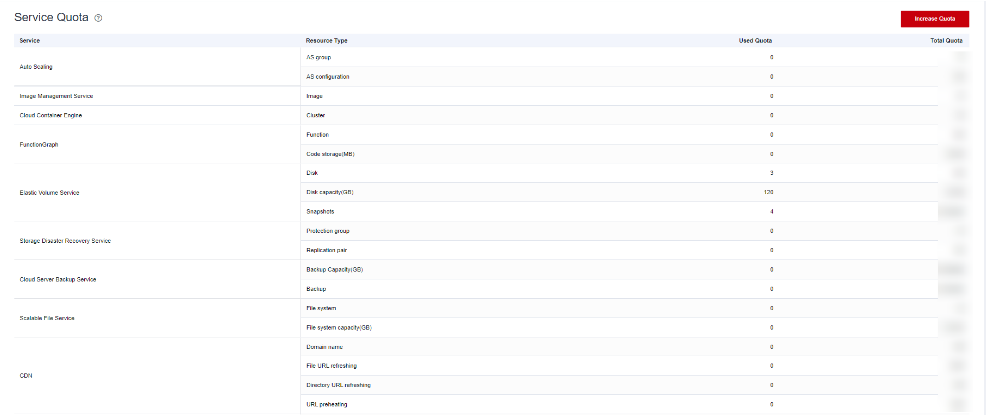
   The **Quotas** page is displayed.

   Figure 8-2 My Quotas

3. Click **Increase Quota** in the upper right corner of the page.

   Figure 8-3 Increasing quota

Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	[redacted]
	AS configuration	0	[redacted]
Image Management Service	Image	0	[redacted]
Cloud Container Engine	Cluster	0	[redacted]
FunctionGraph	Function	0	[redacted]
	Code storage(MB)	0	[redacted]
Elastic Volume Service	Disk	3	[redacted]
	Disk capacity(GB)	120	[redacted]
	Snapshots	4	[redacted]
Storage Disaster Recovery Service	Protection group	0	[redacted]
	Replication pair	0	[redacted]
Cloud Server Backup Service	Backup Capacity(GB)	0	[redacted]
	Backup	0	[redacted]
Scalable File Service	File system	0	[redacted]
	File system capacity(GB)	0	[redacted]
CDN	Domain name	0	[redacted]
	File URL refreshing	0	[redacted]
	Directory URL refreshing	0	[redacted]
	URL preheating	0	[redacted]

4. On the **Create Service Ticket** page, configure parameters as required.

   In the **Problem Description** area, fill in the content and reason for adjustment.

5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

9 Auditing Key Operations

9.1 IMS Operations Audited by CTS

Scenarios

Cloud Trace Service (CTS) is a log audit service provided by Huawei Cloud and intended for cloud security. It allows you to collect, store, and query cloud resource operation records and use these records for security analysis, compliance auditing, resource tracking, and fault locating.

You can use CTS to record IMS operations for later querying, auditing, and backtracking.

Prerequisites

You need to enable CTS before using it. If it is not enabled, IMS operations cannot be recorded. After being enabled, CTS automatically creates a tracker to record all your operations. The tracker stores only the operations of the last seven days. To store the operations for a longer time, store trace files in OBS buckets.

IMS Operations Recorded by CTS

Table 9-1 IMS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating an image	ims	createImage
Creating a data disk image	ims	createDataImage
Creating a full-ECS image	ims	createWholeImage
Modifying an image	ims	updateImage

Operation	Resource Type	Trace Name
Deleting images in a batch	ims	deleteImage
Querying details about an image	ims	queryImage
Querying details about images	ims	listImages
Replicating an image	ims	copyImage
Replicating an image across regions	ims	crossRegionCopyImage
Exporting an image	ims	exportImage
Adding a member	ims	addMember
Modifying members in a batch	ims	updateMember
Deleting members in a batch	ims	deleteMember
Querying details about a member	ims	queryMember
Querying details about members	ims	listMembers
Adding or modifying an image tag	ims	createOrUpdateTags
Adding or deleting image tags in a batch	ims	batchAddOrDeleteImageTag
Adding an image tag	ims	createTag
Deleting image tags in a batch	ims	deleteTags
Deleting an image tag	ims	deleteTag
Querying image tags	ims	listTags
Creating image metadata	ims	createImageMetadata
Register an image file as a private image	ims	registerImage
Uploading an image	ims	uploadImage
Querying an image schema	ims	queryImageSchema

Operation	Resource Type	Trace Name
Querying an image list schema	ims	queryImageListSchema
Querying an image member schema	ims	queryMemberSchema
Querying an image member list schema	ims	queryMemberListSchema
Querying OSs supported by images	ims	listOsVersions
Querying image quotas	ims	queryImageQuota

Table 9-2 Relationship between IMS operations and native OpenStack APIs

Operation	Trace Name	Service Type	Resource Type	OpenStack Component
Creating an Image	createImage	IMS	image	glance
Modifying/ Uploading an image	updateImage	IMS	image	glance
Deleting an image	deleteImage	IMS	image	glance
Tagging an image	addTag	IMS	image	glance
Deleting an image tag	deleteTag	IMS	image	glance
Adding a tenant that can use a shared image	addMember	IMS	image	glance
Modifying information about a tenant that can use a shared image	updateMember	IMS	image	glance

Operation	Trace Name	Service Type	Resource Type	OpenStack Component
Deleting a tenant from the group where the members can use a shared image	deleteMember	IMS	image	glance

9.2 Viewing Traces

Scenarios

After you enable Cloud Trace Service (CTS) and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, CTS starts recording operations on data in Object Storage Service (OBS) buckets. CTS stores operation records (traces) generated in the last seven days.

This section describes how to query or export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces 5 minutes later.
- These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.

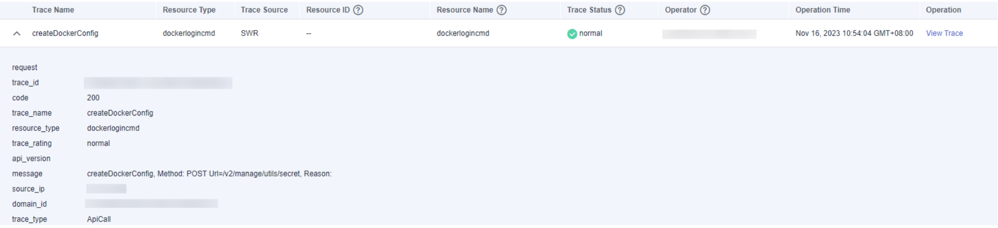
- **Trace Name**: Enter a trace name.
- **Trace ID**: Enter a trace ID.
- **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
- **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
- **Trace Source**: Select a cloud service name from the drop-down list.
- **Resource Type**: Select a resource type from the drop-down list.
- **Operator**: Select one or more operators from the drop-down list.
- **Trace Status**: Select **normal**, **warning**, or **incident**.
  - **normal**: The operation succeeded.
  - **warning**: The operation failed.
  - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
- **Enterprise Project ID**: Enter an enterprise project ID.
- **Access Key**: Enter a temporary or permanent access key ID.
- Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.

5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
   - Enter any keyword in the search box and press **Enter** to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
   - Click ⟳ to view the latest information about traces.
   - Click ⚙ to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (●), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.

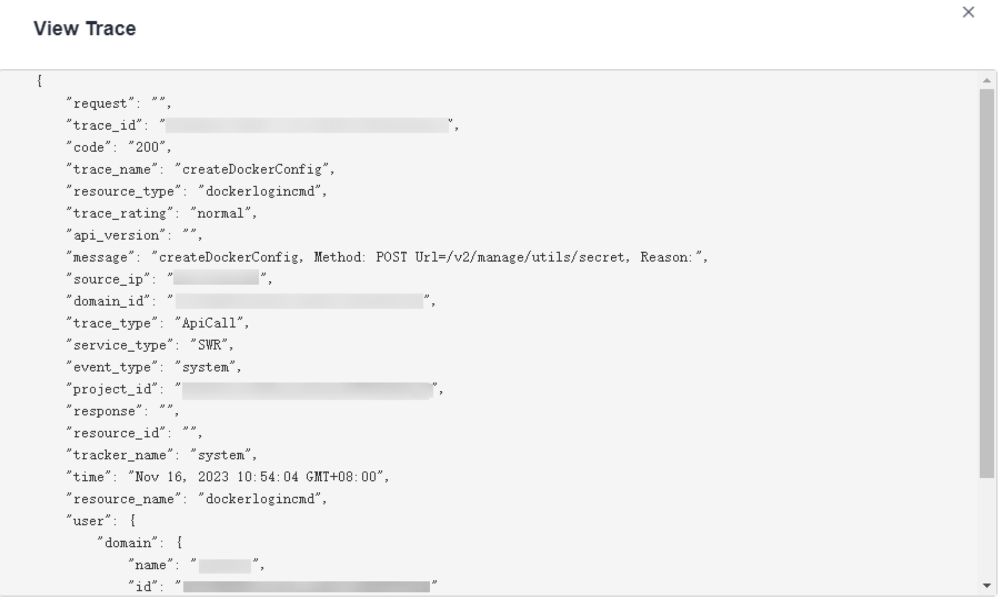
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available.
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
   - Click ↻ to view the latest information about traces.
8. Click ⌄ on the left of a trace to expand its details.



Trace Name	Resource Type	Trace Source	Resource ID ?	Resource Name ?	Trace Status ?	Operator ?	Operation Time	Operation
^ createDockerConfig	dockerlogincmd	SWR	--	dockerlogincmd	✓ normal	[redacted]	Nov 16, 2023 10:54:04 GMT+08:00	View Trace

request	
trace_id	[redacted]
code	200
trace_name	createDockerConfig
resource_type	dockerlogincmd
trace_rating	normal
api_version	
message	createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:
source_ip	[redacted]
domain_id	[redacted]
trace_type	ApiCall

9. Click **View Trace** in the **Operation** column. The trace details are displayed.



```
{
    "request": "",
    "trace_id": "[redacted]",
    "code": "200",
    "trace_name": "createDockerConfig",
    "resource_type": "dockerlogincmd",
    "trace_rating": "normal",
    "api_version": "",
    "message": "createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:",
    "source_ip": "[redacted]",
    "domain_id": "[redacted]",
    "trace_type": "ApiCall",
    "service_type": "SWR",
    "event_type": "system",
    "project_id": "[redacted]",
    "response": "",
    "resource_id": "",
    "tracker_name": "system",
    "time": "Nov 16, 2023 10:54:04 GMT+08:00",
    "resource_name": "dockerlogincmd",
    "user": {
        "domain": {
            "name": "[redacted]",
            "id": "[redacted]"
```

10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

10 Monitoring Events

10.1 Monitored IMS Events

Introduction

Event monitoring provides data collection, query, and alarm reporting for events. You can create alarm rules for events. When specific events occur, Cloud Eye generates alarms for you.

Namespace

SYS.IMS

Monitored Events

Table 10-1 IMS events

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Handling Suggestion	Impact
IMS	SYS.IMS	Creating an image	createImage	Minor	Creating a private image	None	This image can be used to create cloud servers.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Handling Suggestion	Impact
		Updating an image	updateImage	Minor	Updating metadata of an image	None	Cloud servers may fail to be created from this image if key image metadata is changed.
		Deleting an image	deleteImage	Minor	Deleting a private image	None	This image can no longer be used to create cloud servers.

10.2 Configuring Event Alarm Notifications

You can use Cloud Eye to monitor IMS. After IMS event notifications are configured, a notification will be sent when an image is created, updated, or deleted.

NOTE

Notifications are sent by the Simple Message Notification (SMN) service, which will incur charges.

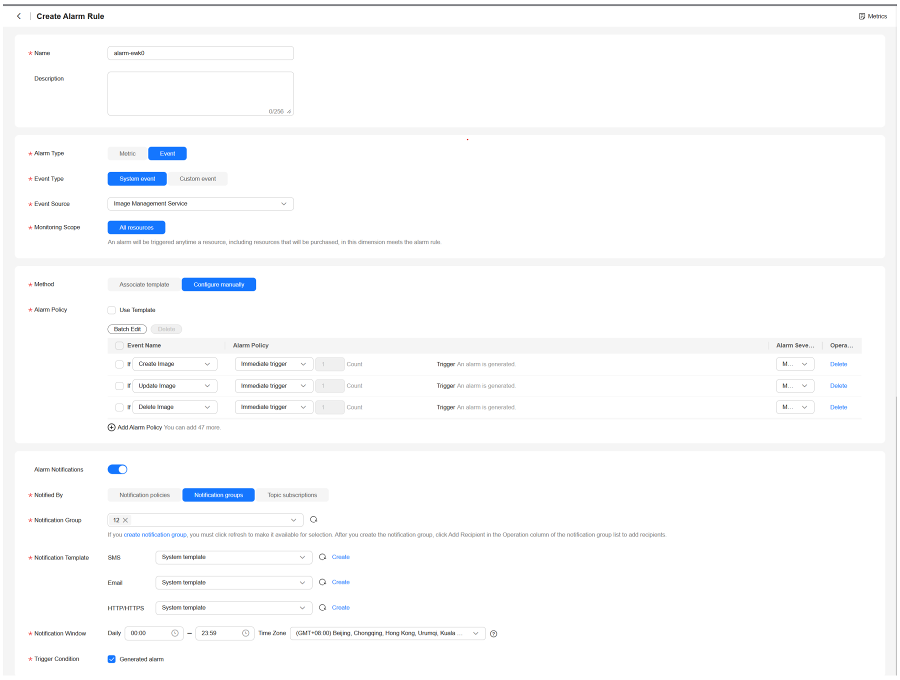
Configuring Event Alarm Notifications

1. Log in to the Huawei Cloud console.
2. Click ☰ in the upper left corner of the page. In the navigation pane, choose **Management & Governance** > **Cloud Eye**.
3. Use either of the methods:

   Method 1: In the navigation pane, choose **Event Monitoring**.

   Method 2: In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
4. In the upper right corner, click **Create Alarm Rule**.
5. Set alarm parameters by referring to **Table 10-2**.

Figure 10-1 Alarm parameters



Create Alarm Rule

Metrics

* Name: alarm-ewk0

Description: 0/256

* Alarm Type: Metric | **Event**

* Event Type: **System event** | Custom event

* Event Source: Image Management Service

* Monitoring Scope: **All resources**

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

* Method: Associate template | **Configure manually**

* Alarm Policy: □ Use Template

Batch Edit | Delete

□ Event Name	Alarm Policy			Alarm Seve...	Opera...
□ If Create Image	Immediate trigger	1 Count	Trigger An alarm is generated.	M...	Delete
□ If Update Image	Immediate trigger	1 Count	Trigger An alarm is generated.	M...	Delete
□ If Delete Image	Immediate trigger	1 Count	Trigger An alarm is generated.	M...	Delete

Add Alarm Policy You can add 47 more.

Alarm Notifications: on

* Notified By: Notification policies | **Notification groups** | Topic subscriptions

* Notification Group: 12

If you create notification group, you must click refresh to make it available for selection. After you create the notification group, click Add Recipient in the Operation column of the notification group list to add recipients.

* Notification Template: SMS: System template (Create); Email: System template (Create); HTTP/HTTPS: System template (Create)

* Notification Window: Daily 00:00 – 23:59 Time Zone (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Kuala ...

* Trigger Condition: ☑ Generated alarm

Table 10-2 Parameters

Parameter	Description
Name	Name of the rule. The system generates a random name and you can modify it.
Description	Description of the alarm rule.
Alarm Type	Select **Event**.
Event Type	Select **System event**.
Event Source	Select **Image Management Service**.
Monitoring Scope	Specify the resource scope that the alarm rule will apply to.
Method	Use the default value **Configure manually**.
Alarm Policy	Configure a policy for triggering an alarm. You can configure a policy for triggering an alarm when an image is created, updated, or deleted.
Notified By	Select an option as you need. **NOTE** Alarm messages are sent by SMN, which may incur a small charge.

6. Click **Create**. In the displayed dialog box, click **OK**.