Bare Metal Server

Private Image Creation Guide

Issue	02
Date	2023-09-04

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Overview

If you want to use a private BMS image, you can use an external image file to create one. This document describes the private image creation procedure (including creating a VM and installing the OS, software, and drivers on the VM) and uses multiple OSs as examples to provide instructions for you to create a private image. You can also install software as needed to customize your private image.

After you have created an image file, you need to register it on the cloud platform. For details, see **Creating a Private Image from an External Image File**. After successful registration, you can select this private image when creating a BMS.

Image Creation Process

The image creation process is as follows:

Figure 1-1 Process of image creation

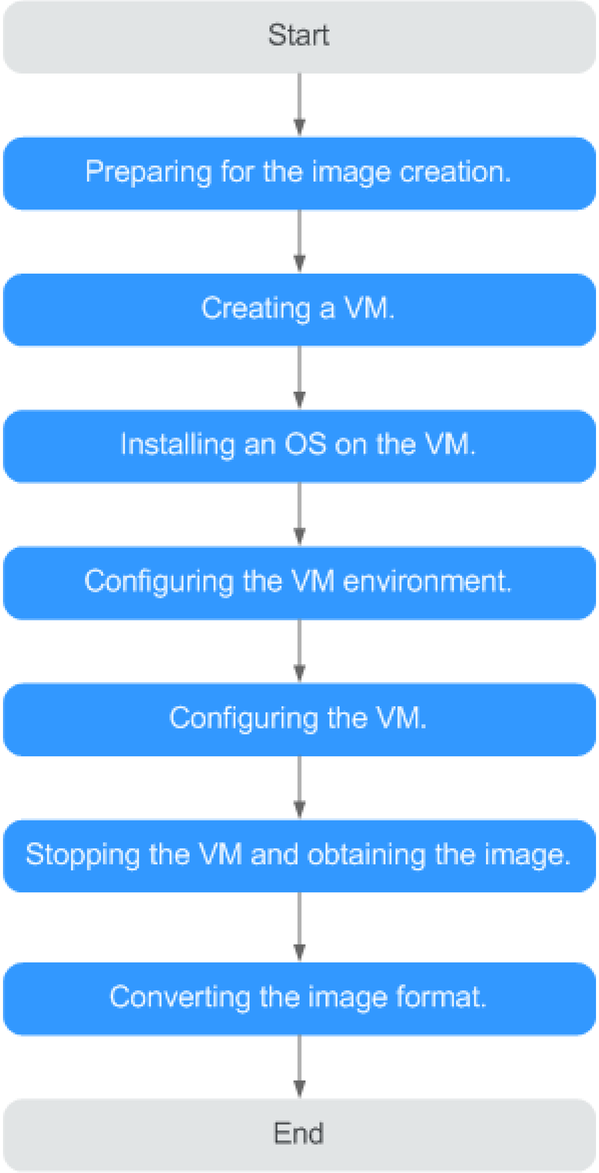

Start
Preparing for the image creation.
Creating a VM.
Installing an OS on the VM.
Configuring the VM environment.
Configuring the VM.
Stopping the VM and obtaining the image.
Converting the image format.
End

Table 1-1 Creation process description

Procedure	Description
Making preparations	Before you create an image, prepare: ● A Linux physical server or VM to be used as a host ● Software packages, such as the OS ISO file package, SDI driver package, and bms-network-config package ● Tools, such as the cross-platform remote access tool and file transfer tool
Creating a VM	Use virt-manager to create a VM.
Installing an OS on the VM	Install an OS on the VM as required.

Procedure	Description
Configuring the VM environment	Software packages need to be uploaded to the VM. Therefore, you need to configure the VM environment so that the VM can connect to the Internet.
Configuring the VM	Linux: ● Install and configure Cloud-Init. ● Modify the hardware device driver that boots the OS. ● Install bms-network-config. ● (Optional) Install the SDI driver. ● (Optional) Install the Hi1822 driver. ● (Optional) Install the IB driver. ● (Optional) Install x86 V5/TaiShan server drivers. ● (Optional) Install multipath software. ● Perform security configuration. ● Configure remote login. ● Configure automatic root partition expansion. Windows: ● Install x86 V5 server drivers. ● Install Cloudbase-Init. ● Install bms-network-config. ● (Optional) Install the SDI driver. ● Set the Windows time zone. ● Set the Windows virtual memory. ● (Optional) Configure automatic windows update. ● Configure the SID.
Stopping the VM and obtaining the image	Stop the VM and obtain the image file. If the generated image file is too large, you can compress it.
Converting the image format	For BMS, the image format can only be ZVHD2. After obtaining an image file, convert its format to ZVHD2.

Supported OSs

BMS images support the following OSs:

Table 1-2 x86 OSs

OS Type	OS Version	Kernel Version
RedHat	Red Hat Linux Enterprise 6.5 64bit	2.6.32-431.el6.x86_64

OS Type	OS Version	Kernel Version
	Red Hat Linux Enterprise 6.7 64bit	2.6.32-573.el6.x86_64
	Red Hat Linux Enterprise 6.8 64bit	2.6.32-642.el6.x86_64
	Red Hat Linux Enterprise 6.9 64bit	2.6.32-696.e16.x86_64
	Red Hat Linux Enterprise 7.2 64bit	3.10.0-327.e17.x86_64
	Red Hat Linux Enterprise 7.3 64bit	3.10.0-514.el7.x86_64
	Red Hat Linux Enterprise 7.4 64bit	3.10.0-693.e17.x86_64
	Red Hat Linux Enterprise 7.5 64bit	3.10.0-862.el7.x86_64
SUSE	SUSE Linux Enterprise Server 11 SP4 64bit	3.0.101-63-default
	SUSE Linux Enterprise Server 12 SP1 64bit	3.12.49-11-default
	SUSE Linux Enterprise Server 12 SP2 64bit	4.4.21-69-default
	SUSE Linux Enterprise Server 12 SP3 64bit	4.4.73-5-default
Oracle Linux	Oracle Linux Server release 6.8 64bit	4.1.12-37.4.1.e16uek.x86_64
	Oracle Linux Server release 6.9 64bit	4.1.12-61.1.28.e16uek.x86_64
	Oracle Linux Server release 7.2 64bit	3.10.0-327.e17.x86_64
	Oracle Linux Server release 7.3 64bit	3.10.0-327.el7.x86_64 or 4.1.12-61.1.18.e17uek.x86_64
	Oracle Linux Server release 7.4 64bit	4.1.12-94.3.9.e17uek.x86_64
EulerOS	EulerOS 2.2 64bit	3.10.0-327.44.58.35.x86_64
	EulerOS 2.3 64bit	3.10.0-514.44.5.10.h142.x86_64
CentOS	CentOS 6.8 64bit	2.6.32-642.e16.x86_64
	CentOS 6.9 64bit	2.6.32-696.e16.x86_64
	CentOS 7.2 64bit	3.10.0-327.e17.x86_64

OS Type	OS Version	Kernel Version
	CentOS 7.3 64bit	3.10.0-514.el7.x86_64
	CentOS 7.4 64bit	3.10.0-693.e17.x86_64
	CentOS 7.5 64bit	3.10.0-862.e17.x86_64
Ubuntu	Ubuntu 16.04 LTS 64bit	4.4.0-21-generic x86_64
	Ubuntu 14.04 LTS 64bit	3.13.0-24-generic
Debian	Debian 8.6 64bit	3.16.0-4-amd64
Windows	Windows Server 2012 R2 Standard 64bit	-
	Windows Server 2016 Standard 64bit	-

Table 1-3 Arm OSs

OS Type	OS Version	Kernel Version
CentOS	CentOS 7.6 ARM	4.14.0-115.el7a.0.1.aarch64
EulerOS	EulerOS 2.8 ARM	4.19.36-vhulk1907.1.0.h475.eulerosv2r8.aarch64

NOTE

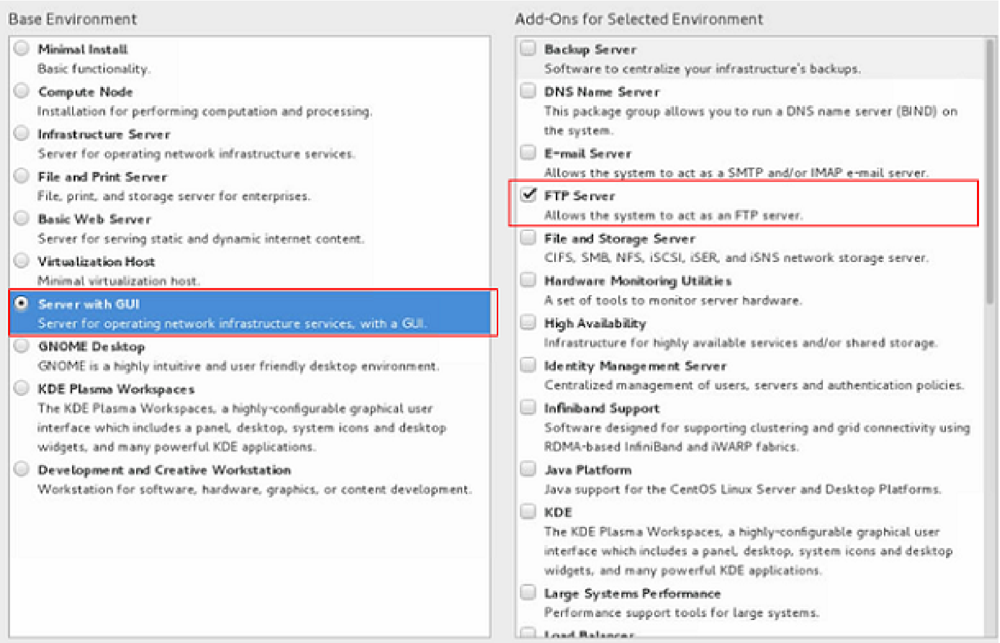
When you download an SDI driver, ensure that the driver matches your kernel version. You can run the **uname -r** command to query the OS kernel version.

2 Preparing the Environment

- Prepare a Linux physical server or VM as the host and install Linux on the host.

  For example, if you are installing CentOS 7.3 64bit on the host, you must select the GUI and virtualization environment.

  Select **Server with GUI** and then select **FTP Server**, **Virtualization Client**, **Virtualization Hypervisor**, and **Virtualization Tools**.



Base Environment

○ **Minimal Install**
Basic functionality.

○ **Compute Node**
Installation for performing computation and processing.

○ **Infrastructure Server**
Server for operating network infrastructure services.

○ **File and Print Server**
File, print, and storage server for enterprises.

○ **Basic Web Server**
Server for serving static and dynamic internet content.

○ **Virtualization Host**
Minimal virtualization host.

● **Server with GUI**
Server for operating network infrastructure services, with a GUI.

○ **GNOME Desktop**
GNOME is a highly intuitive and user friendly desktop environment.

○ **KDE Plasma Workspaces**
The KDE Plasma Workspaces, a highly-configurable graphical user interface which includes a panel, desktop, system icons and desktop widgets, and many powerful KDE applications.

○ **Development and Creative Workstation**
Workstation for software, hardware, graphics, or content development.

Add-Ons for Selected Environment

□ **Backup Server**
Software to centralize your infrastructure's backups.

□ **DNS Name Server**
This package group allows you to run a DNS name server (BIND) on the system.

□ **E-mail Server**
Allows the system to act as a SMTP and/or IMAP e-mail server.

☑ **FTP Server**
Allows the system to act as an FTP server.

□ **File and Storage Server**
CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server.

□ **Hardware Monitoring Utilities**
A set of tools to monitor server hardware.

□ **High Availability**
Infrastructure for highly available services and/or shared storage.

□ **Identity Management Server**
Centralized management of users, servers and authentication policies.

□ **Infiniband Support**
Software designed for supporting clustering and grid connectivity using RDMA-based InfiniBand and iWARP fabrics.

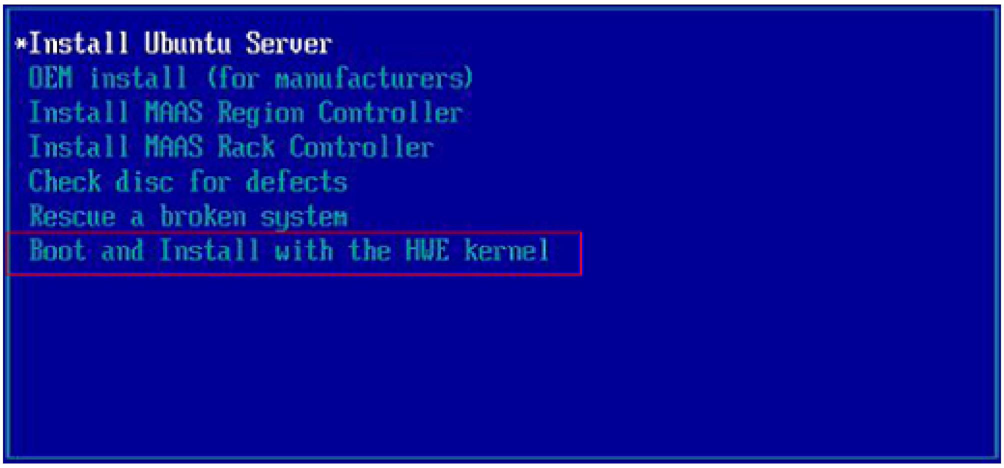
□ **Java Platform**
Java support for the CentOS Linux Server and Desktop Platforms.

□ **KDE**
The KDE Plasma Workspaces, a highly-configurable graphical user interface which includes a panel, desktop, system icons and desktop widgets, and many powerful KDE applications.

□ **Large Systems Performance**
Performance support tools for large systems.

□ **Load Balancer**

  For example, if you are creating an Arm64 image and installing Ubuntu 16.04 Server-ARM64 on the host. Select the option containing the HWE kernel.



```
*Install Ubuntu Server
 OEM install (for manufacturers)
 Install MAAS Region Controller
 Install MAAS Rack Controller
 Check disc for defects
 Rescue a broken system
 Boot and Install with the HWE kernel
```

After the OS is installed on the host, run the following commands to install the Ubuntu desktop and virtualization software and then restart the host.

sudo apt-get update

sudo apt-get dist-upgrade

sudo apt-get install ubuntu-desktop

sudo apt-get install qemu

sudo apt-get install qemu-kvm

sudo apt-get install libvirt0

sudo apt-get install virt-manager

sudo apt-get install qemu-efi

- Configure the host network and remote connection to the host.
  a. Connect the host to the Internet so that you can install software on VMs online through the host.
  b. Remotely connect to the host. If you are connecting from a Windows local server, additional configurations are needed.
- Enable the vsftpd, SSHD, and VNC services and configure them.

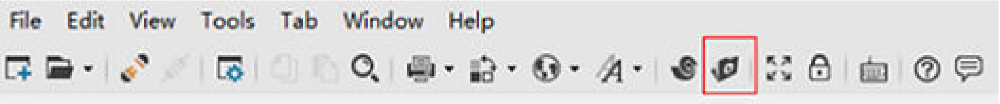
  These services allow you to remotely transmit software packages, ISO files, and scripts to the host, and remotely log in to the host. For details, see **Configuring the SSH Service**, **Configuring the vsftpd Service**, and **Configuring the VNC Service**.
- For CentOS 7.*x*, disable the firewall so that you can log in to the host using VNC Viewer. Run the following commands to disable the firewall:

  systemctl disable firewalld.service

  systemctl stop firewalld.service
- Transmit required files to the host.

  After the host configuration is complete, use vsftpd to upload the required files to the host. After the preceding operations are performed, the host environment configuration is complete.

  If you use Xftp to upload the files, click the icon shown in the red box in the following figure after you log in to the host through Xshell using SSH.


File
Edit
View
Tools
Tab
Window
Help

3 Linux

3.1 Software

Prepare the software listed in **Table 3-1**. Determine the drivers to be installed based on **Mapping Between BMS Specifications and Drivers**.

Table 3-1 Software

No.	Package	Description	How to Obtain	Provider
1	ISO file	ISO file used to create an image. **NOTE** Currently, only Windows Standard editions are supported.	You are advised to obtain the ISO file from the OS official websites.	OS official websites

No.	Package	Description	How to Obtain	Provider
2	SDI driver	With the SDI driver, EVS disks can be attached to BMSs. The EVS disks can be used as system disks from which the BMSs are booted. This facilitates quick BMS provisioning. **NOTE** This software package is only required by images with SDI cards installed (SDI 2.2 and SDI 3.0 excluded).	Linux: Visit **https://support.huawei.com/enterprise/en/intelligent-accelerator-components/sd100-pid-22040214/software/253495955?idAbsPath=fixnode01%7C23710424%7C251364409%7C21782478%7C22040214**, download **SD100-2.0.2.SPC15-DRIVER.zip**, and decompress it. Obtain the driver package based on the OS type. For example, the driver package for CentOS 7.6 is **kmod-scsi_ep_front-centos_7.6_1.0.18-3.10.0_957.el7.centos.x86_64.rpm**. Windows (Windows 2016 as an example): Visit **https://support.huawei.com/enterprise/en/intelligent-accelerator-components/sd100-pid-22040214/software/250607152?idAbsPath=fixnode01%7C23710424%7C251364409%7C21782478%7C22040214**, download **SD100-2.0.2.SPC11-DRIVER-V010.zip**, and decompress it. For example, the driver package for Windows Server 2016 is **sdidriver_win-2016-installpack.zip**.	Huawei
3	bms-network-config	It is used to automatically configure BMS networks.	Software: **https://bms-image-package.obs.cn-north-1.myhuaweicloud.com/bms-network-config-23.8.0.zip** SHA256 checksum: **https://bms-image-package.obs.cn-north-1.myhuaweicloud.com/bms-network-config-23.8.0.zip.sha256**	Huawei

No.	Package	Description	How to Obtain	Provider
4	Cloud-Init	Cloud-Init needs to be installed online. Ensure that the server on which Cloud-Init is to be installed can connect to the Internet.	Obtain the package from the official website.	Cloud-Init
5	Cloudbase-Init	Cloudbase-Init is used to initialize Windows instances (for example, initialize the instance login password). You are advised to download the version specified by HUAWEI CLOUD.	Software: **https://bms-image-package.obs.cn-north-1.myhuaweicloud.com/windows/cloudbase_init/CloudbaseInitSetup_x64.msi** SHA256 checksum: **https://bms-image-package.obs.cn-north-1.myhuaweicloud.com/CloudbaseInitSetup_x64.msi.sha256**	Cloudbase-Init
6	Hi1822 driver	This driver needs to be installed for centralized BMSs with Hi1822 NICs.	Visit **https://support.huawei.com/enterprise/en/management-software/fusionserver-idriver-pid-21588909/software/**. Click the recommended or latest version. Download **FusionServer iDriver-*xxx*-Driver-*xxx*.zip** based on the image OS type to obtain the Hi1822 driver packages. Example: Click **FusionServer iDriver 3.0.34**, select **CentOS**, and download **FusionServer iDriver-CentOS7.6-Driver-V116.zip**. Decompress the package to obtain **onboard_driver_CentOS7.6.iso** and then decompress the .iso package to obtain the **NIC-Hi1822-CentOS7.6-hinic-3.9.0.8-1-x86_64.rpm** and **NIC-Hi1822-CentOS7.6-hinicadm-3.9.0.8-1-x86_64.rpm** driver packages.	Huawei

No.	Package	Description	How to Obtain	Provider
		This driver needs to be installed for distributed BMSs with SDI 2.2 offload cards.	1. Visit **https://support.huawei.com**, search for **Hi1822_BM_X86_*xxx*.tar.gz** (*xxx* indicates the package version), download the package of the latest version, and decompress it. 2. In the decompressed folder, obtain the driver package based on the image OS type.	Huawei
		This driver needs to be installed for distributed BMSs with SDI 3.0 offload cards.	1. Visit **https://support.huawei.com**, search for **uNIC_GuestOS_Driver_BM_*xxx*.tar.gz** (*xxx* indicates the package version), download the package of the latest version, and decompress it. 2. In the decompressed folder, obtain the driver package based on the image OS type.	Huawei
7	IB driver	100G InfiniBand driver.	Visit **https://network.nvidia.com/products/infiniband-drivers/linux/mlnx_ofed/**, Scroll down and click **Download**.	Mellanox
8	FusionServer server driver	LAN On Motherboard (LOM), RAID, and disk drivers of FusionServer servers.	Visit **https://support.huawei.com/enterprise/en/servers/fusionserver-idriver-pid-21588909/software**. Click the recommended version. Download the driver package based on the image OS.	Huawei
9	TaiShan server driver	NIC and RAID drivers of TaiShan servers.	Visit **https://support.huawei.com/enterprise/en/management-software/taishanserver-idriver-pid-251215329/software**. Click the recommended version. Download the driver package based on the image OS.	Huawei
10	UltraPath	Multipath software required by HBA cards to mount FC storage.	Visit **https://support.huawei.com/enterprise/en/cloud-storage/ultrapath-pid-8576127/software** to obtain the software and documents of the required version.	Huawei

NOTE

Install only necessary software because too much software may result in a large image file.

The image file must be at least 150 MB smaller than the memory of the BMS to be created from the image.

3.2 Tools

Table 3-2 lists the required tools.

NOTE

VNC tools and qemu-img-hw are required only when virt-manager is used to create an image.

Table 3-2 Tools

Tool	Description	How to Obtain
Cross-platform remote access tool	Used to access the host, such as Xshell	Obtain it from the official website.
File transfer tool	Used to transfer files to the VM, such as Xftp	Obtain it from the official website.
qemu-img-hw	Used to convert image formats	Software: **https://bms-image-package.obs.cn-north-1.myhuaweicloud.com/qemu-img-hw.zip** SHA256 checksum: **https://bms-image-package.obs.cn-north-1.myhuaweicloud.com/qemu-img-hw.zip.sha256**
VNC tool	Used to log in to the VM, such as VNC Viewer **NOTE** If the VNC Viewer version is 5.3.2, choose **Options** > **Expert** > **ColorLevel** on the login page and set **ColorLevel** to **rgb222**. Otherwise, you may fail to log in to the VM.	Obtain it from the official website.

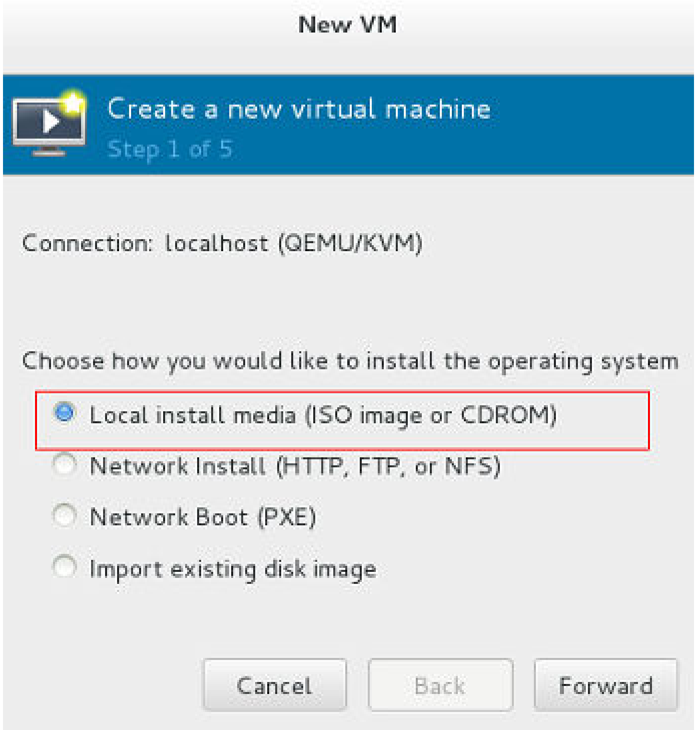
3.3 Creating a Linux VM

3.3.1 Creating a VM using virt-manager

3.3.1.1 Creating a Linux VM

This section uses Oracle Linux 6.8 as an example to describe how to create a Linux VM. The procedure is also applicable to other Linux OSs. The screenshots in the following steps are for reference only.

1. Download the required ISO image to the host. Alternatively, you can also download the image to your local PC, use Xshell to remotely connect to the host, and upload the image to the host.
2. Log in to the host and run the **virt-manager** command to start virt-manager.
3. Click **Create a new virtual machine**. In the **New VM** dialog box, select **Local install media (ISO image or CDROM)**. Click **Forward**.



New VM

Create a new virtual machine

Step 1 of 5

Connection: localhost (QEMU/KVM)

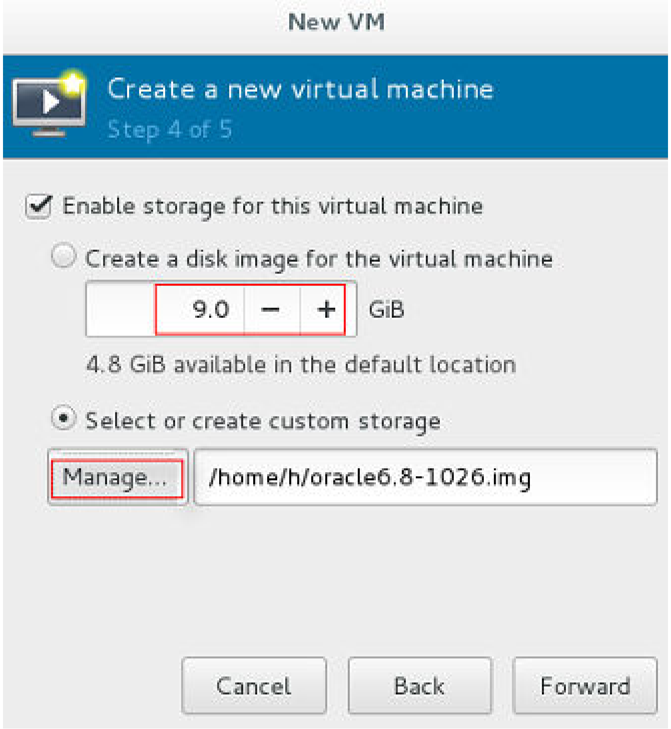
Choose how you would like to install the operating system

- ● Local install media (ISO image or CDROM)
- ○ Network Install (HTTP, FTP, or NFS)
- ○ Network Boot (PXE)
- ○ Import existing disk image

4. Select an ISO image, its OS type, and version. Click **Forward**.
5. Configure the VM memory and CPU. Click **Forward**.
   - Memory (RAM): 4096 MiB
   - CPUs: 4
6. Configure the VM storage by specifying the disk image size.

   NOTE

   - The image cannot be too large. For Oracle Linux 7.3/Red Hat 7.3 Linux, you are advised to set the image size to a value no greater than 6 GB. For Ubuntu 16.04 ARM, you are advised to select **Select managed or other existing storage** and then select a 150 GB QCOW2 image.
   - The total size of the disk image and memory (150 MB) cannot exceed the memory size of the BMS to be created. Otherwise, the BMS will fail to be created.



New VM

Create a new virtual machine
Step 4 of 5

☑ Enable storage for this virtual machine

○ Create a disk image for the virtual machine

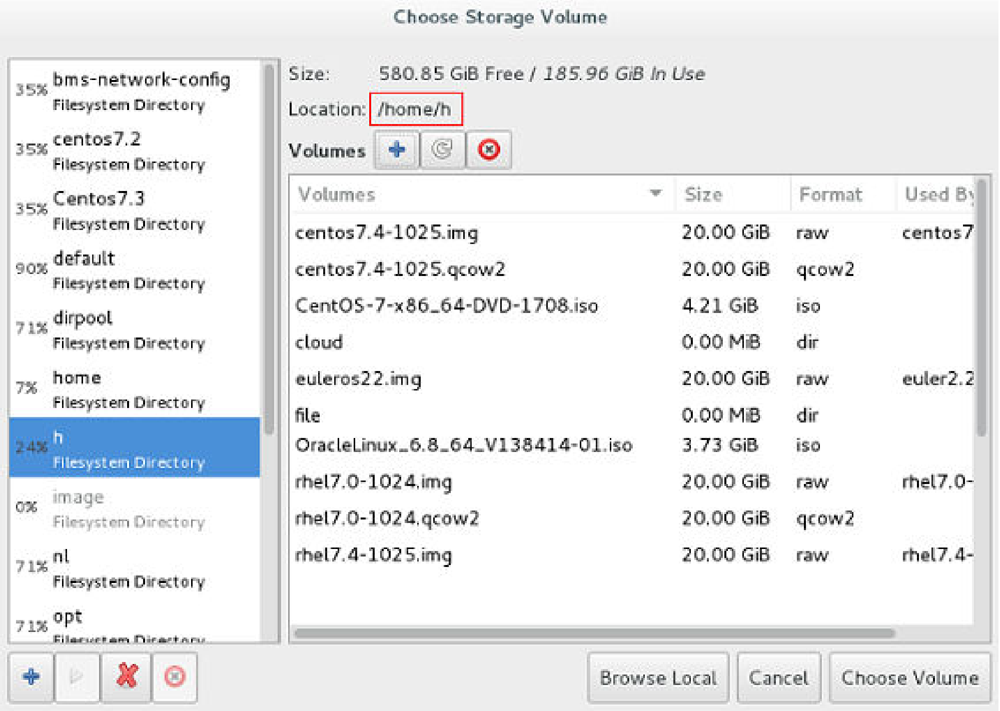
9.0 GiB

4.8 GiB available in the default location

● Select or create custom storage

Manage... /home/h/oracle6.8-1026.img

7. Click **Manage** and select a storage path, for example, **/home/h**.



Choose Storage Volume

35%	bms-network-config Filesystem Directory
35%	centos7.2 Filesystem Directory
35%	Centos7.3 Filesystem Directory
90%	default Filesystem Directory
71%	dirpool Filesystem Directory
7%	home Filesystem Directory
24%	h Filesystem Directory
0%	image Filesystem Directory
71%	nl Filesystem Directory
71%	opt Filesystem Directory

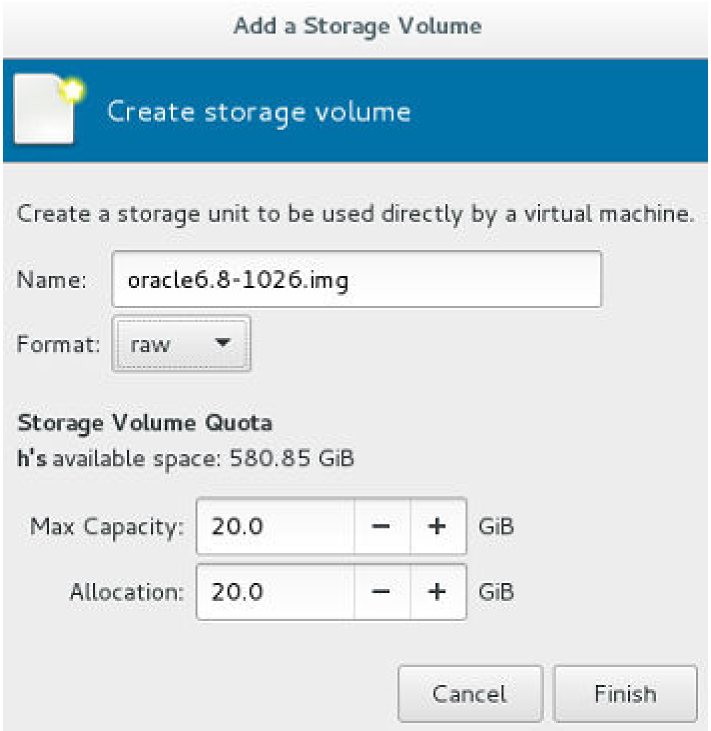
Size: 580.85 GiB Free / *185.96 GiB In Use*

Location: /home/h

Volumes

Volumes	Size	Format	Used By
centos7.4-1025.img	20.00 GiB	raw	centos7
centos7.4-1025.qcow2	20.00 GiB	qcow2	
CentOS-7-x86_64-DVD-1708.iso	4.21 GiB	iso	
cloud	0.00 MiB	dir	
euleros22.img	20.00 GiB	raw	euler2.2
file	0.00 MiB	dir	
OracleLinux_6.8_64_V138414-01.iso	3.73 GiB	iso	
rhel7.0-1024.img	20.00 GiB	raw	rhel7.0-
rhel7.0-1024.qcow2	20.00 GiB	qcow2	
rhel7.4-1025.img	20.00 GiB	raw	rhel7.4-

Click + to create a storage volume. Set **Name** (suffix **.img** is recommended so that the image can be compressed if it is large) and select **raw** (recommended) for **Format**.



Create a storage unit to be used directly by a virtual machine.

Name: oracle6.8-1026.img

Format: raw

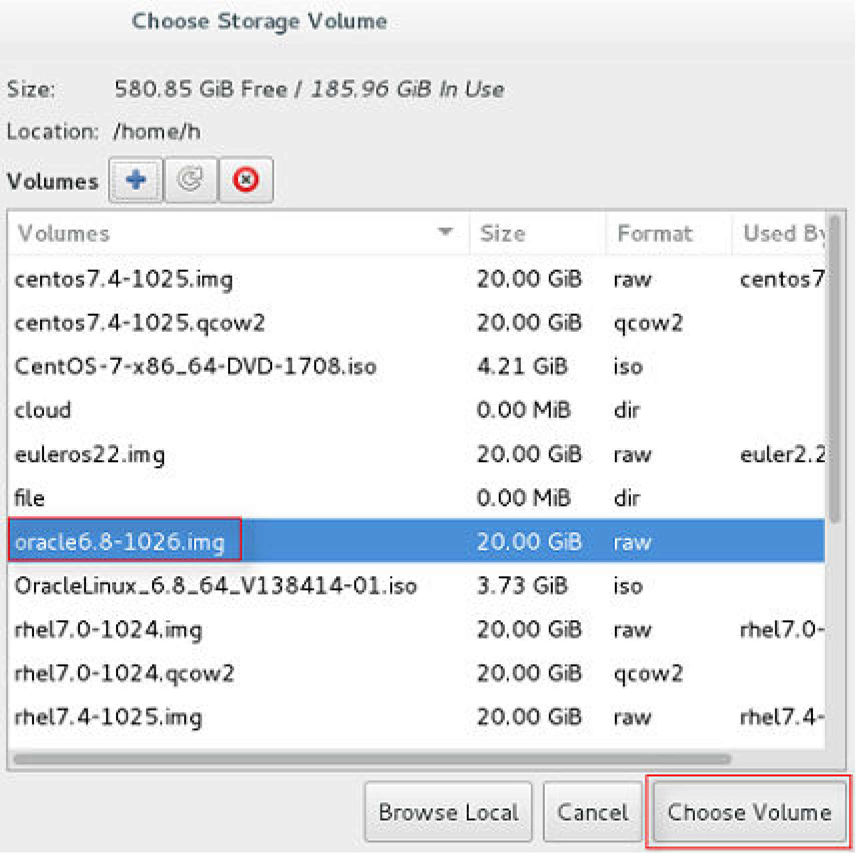
Storage Volume Quota

h's available space: 580.85 GiB

Max Capacity: 20.0 GiB

Allocation: 20.0 GiB

Click **Finish**. In the displayed storage volume list, select the created storage volume and click **Choose Volume**.

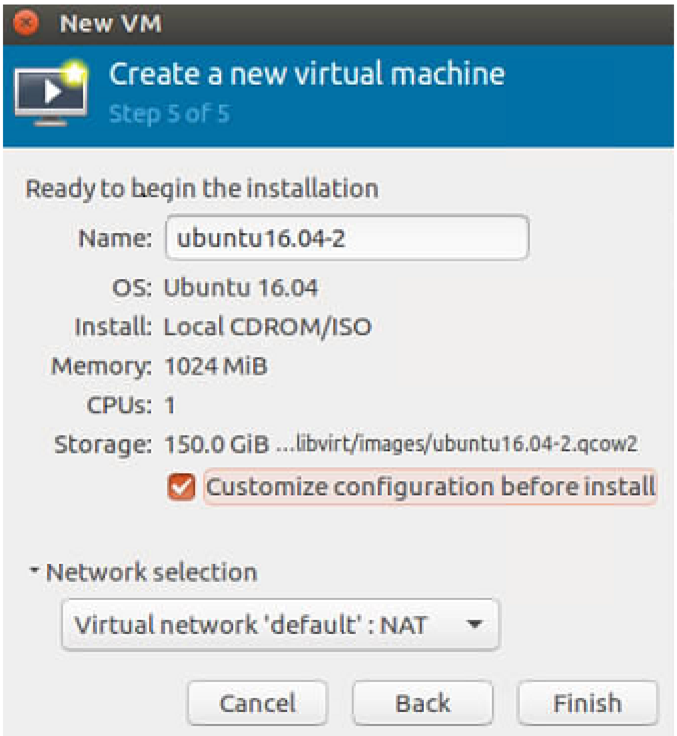


Size: 580.85 GiB Free / *185.96 GiB In Use*

Location: /home/h

Volumes	Size	Format	Used By
centos7.4-1025.img	20.00 GiB	raw	centos7
centos7.4-1025.qcow2	20.00 GiB	qcow2	
CentOS-7-x86_64-DVD-1708.iso	4.21 GiB	iso	
cloud	0.00 MiB	dir	
euleros22.img	20.00 GiB	raw	euler2.2
file	0.00 MiB	dir	
oracle6.8-1026.img	20.00 GiB	raw	
OracleLinux_6.8_64_V138414-01.iso	3.73 GiB	iso	
rhel7.0-1024.img	20.00 GiB	raw	rhel7.0-
rhel7.0-1024.qcow2	20.00 GiB	qcow2	
rhel7.4-1025.img	20.00 GiB	raw	rhel7.4-

8. Enter a name for the VM, for example, **oracle6.8** and select **Customize configuration before install**. For Ubuntu 16.04 ARM, you are advised to select NAT in **Advanced options**. Click **Finish**.



New VM

Create a new virtual machine
Step 5 of 5

Ready to begin the installation

Name: ubuntu16.04-2

OS: Ubuntu 16.04

Install: Local CDROM/ISO

Memory: 1024 MiB

CPUs: 1

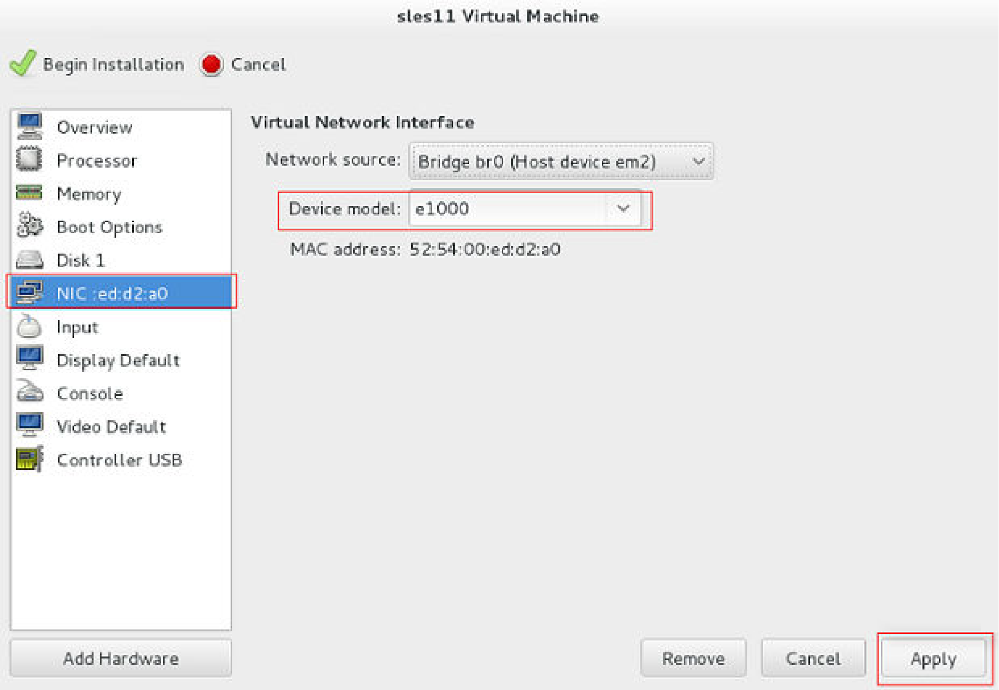
Storage: 150.0 GiB ...libvirt/images/ubuntu16.04-2.qcow2

☑ Customize configuration before install

Network selection

Virtual network 'default' : NAT

9. (Optional) For Ubuntu 16.04 ARM, skip this step. In the navigation pane on the left, choose **NIC**. In the right pane, select **e1000** (Gigabit network adapter) for **Device model**, and click **Apply**.



sles11 Virtual Machine

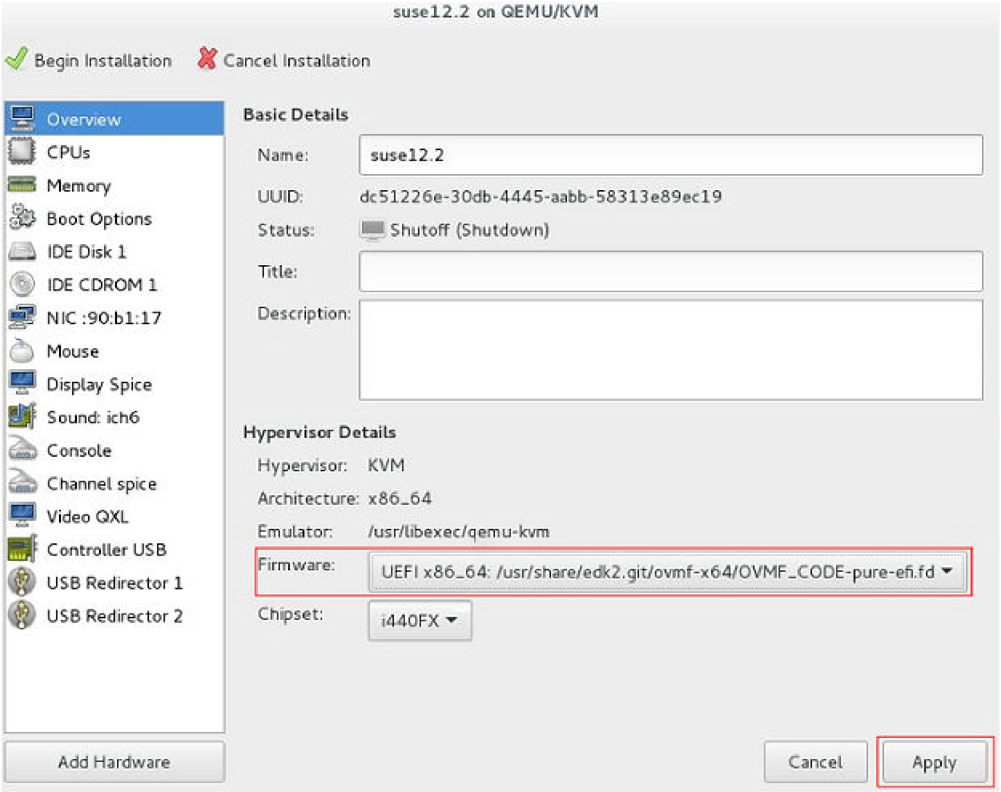
Virtual Network Interface

Network source: Bridge br0 (Host device em2)

Device model: e1000

MAC address: 52:54:00:ed:d2:a0

10. (Optional) This step is used to set the UEFI boot mode and is only necessary for SUSE 12 and KunLun servers for the HANA solution. In the navigation pane on the left, choose **Overview**. In the right pane, select a UEFI option for **Firmware**.



Basic Details

Name: suse12.2

UUID: dc51226e-30db-4445-aabb-58313e89ec19

Status: Shutoff (Shutdown)

Title:

Description:

Hypervisor Details

Hypervisor: KVM

Architecture: x86_64

Emulator: /usr/libexec/qemu-kvm

Firmware: UEFI x86_64: /usr/share/edk2.git/ovmf-x64/OVMF_CODE-pure-efi.fd

Chipset: i440FX

11. Click **Begin Installation**. virt-manager creates the VM as you configured.
12. Wait for the VM to start and install the OS. You need to configure the language, time zone, and other settings.

3.3.2 Creating a VM from an ISO Image

3.3.2.1 Registering an ISO File (Linux)

Scenarios

This section describes how to register an external ISO file as a private image (ISO image) on the cloud platform. Before registering an image, upload the ISO file to an OBS bucket.

Constraints

- To create a Kunpeng server image, set **Architecture** to **ARM** and ensure that Kunpeng ECSs can be created in the current region.
- To create an x86 server image that supports V6 CPUs, set **Boot Mode** to **UEFI**.

Prerequisite

- The file to be registered must be in ISO format.
- The ISO image file has been uploaded to an OBS bucket.

  NOTE

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

Procedure

1. In the **Image Type and Source** area, select **ISO image** for **Type**.
2. In the image file list, select the bucket and then the image file.
3. In the **Image Information** area, set the following parameters.
   - **Boot Mode**: Select **BIOS** or **UEFI**. Ensure that the selected boot mode is the same as that in the image file, or the BMSs created from this image will not be able to boot up.
   - **OS**: Select the OS specified in the ISO file. To ensure that the image can be created and used properly, select an OS consistent with that in the image file.
   - **System Disk**: Set the system disk capacity, which must be no less than the size of the system disk in the image file.
   - **Name**: Enter a name for the image to be created.
   - **Description**: (Optional) Enter image description as needed.
4. Switch back to the **Image Management Service** page to monitor the image status.

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

3.3.2.2 Creating a Linux ECS from an ISO Image

Scenarios

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

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

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

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

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

----End

Follow-up Procedure

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

3.4 Installing a Linux OS on the VM

3.4.1 Overview

Install a Linux OS based on the OS type of the BMS image to be created. This section describes how to install SUSE 11 SP4, Ubuntu 18.04, Ubuntu 16.04, Ubuntu 14.04, Debian 8.6, and SUSE 12 because installing these types of OSs requires some special configuration.

The installation procedure varies depending on the image file. Configure the time zone, KMS address, patch server, repo source update address, input method, and language based on service requirements.

NOTICE

- Creating a BMS image with the BIOS boot mode requires MBR partitioning, and a primary partition needs to be reserved for provisioning the BMS. After the BMS is provisioned, a 64 MB config drive partition is automatically generated. MBR supports a maximum of four partitions, including both the primary and extended ones. Therefore, a maximum of three image primary partitions are allowed. Otherwise, the BMS provisioning will fail.
- If automatic partition extension is required, the root partition must be the last and primary partition.
- If your services require a large number of partitions, you need to configure LVM partitions based on extended partitions.
- For a VM with the UEFI boot mode, do not restart it immediately after its OS is installed. You need to perform the operations in **Modifying the Boot File (UEFI Boot Mode)** to modify the boot file before restarting the VM.

3.4.2 OS Partitioning Recommendations

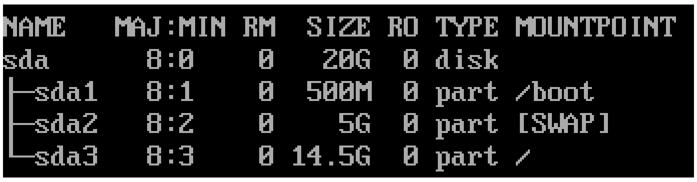
Scenario 1: BIOS Boot

If a BMS is booted in BIOS mode, BIOS needs to be configured for the image used to create the BMS and MBR partitioning is also required.

- **If the primary partition meets your requirements:**

  A: If the boot and swap partitions are independent, use the following partitioning:

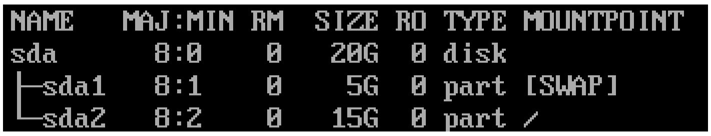
  boot-swap-root partition



```
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda       8:0    0   20G  0 disk
├─sda1    8:1    0  500M  0 part /boot
├─sda2    8:2    0    5G  0 part [SWAP]
└─sda3    8:3    0 14.5G  0 part /
```

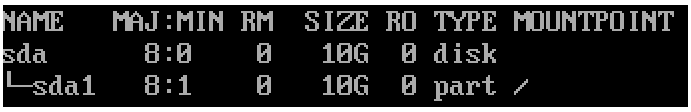
  B: If the boot and swap partitions are not independent, use the following partitioning:

swap-root partition



```
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   20G  0 disk
├─sda1   8:1    0    5G  0 part [SWAP]
└─sda2   8:2    0   15G  0 part /
```

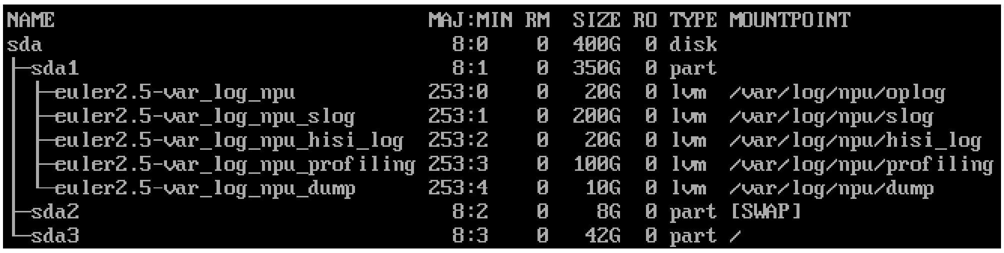
root partition



```
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   10G  0 disk
└─sda1   8:1    0   10G  0 part /
```

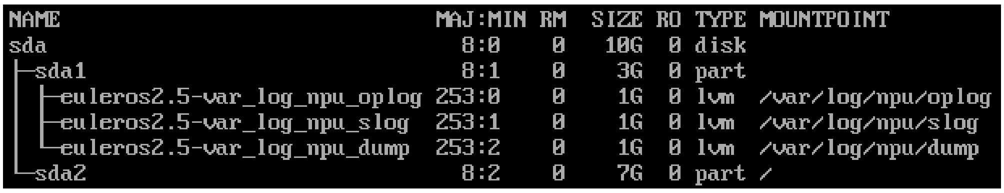
- **If an extended partition (for example, lvm) is required, use the following partitioning:**

  Extended partition (lvm)-swap-root partition



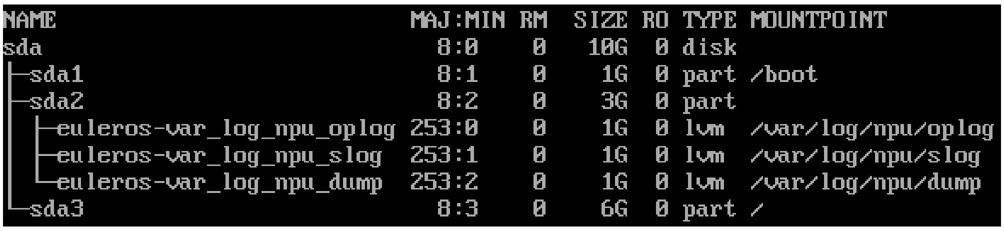
```
NAME                               MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                                  8:0    0  400G  0 disk
├─sda1                               8:1    0  350G  0 part
│ ├─euler2.5-var_log_npu           253:0    0   20G  0 lvm  /var/log/npu/oplog
│ ├─euler2.5-var_log_npu_slog      253:1    0  200G  0 lvm  /var/log/npu/slog
│ ├─euler2.5-var_log_npu_hisi_log  253:2    0   20G  0 lvm  /var/log/npu/hisi_log
│ ├─euler2.5-var_log_npu_profiling 253:3    0  100G  0 lvm  /var/log/npu/profiling
│ └─euler2.5-var_log_npu_dump      253:4    0   10G  0 lvm  /var/log/npu/dump
├─sda2                               8:2    0    8G  0 part [SWAP]
└─sda3                               8:3    0   42G  0 part /
```

  Extended partition (lvm)-root partition



```
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                                   8:0    0   10G  0 disk
├─sda1                                8:1    0    3G  0 part
│ ├─euleros2.5-var_log_npu_oplog    253:0    0    1G  0 lvm  /var/log/npu/oplog
│ ├─euleros2.5-var_log_npu_slog     253:1    0    1G  0 lvm  /var/log/npu/slog
│ └─euleros2.5-var_log_npu_dump     253:2    0    1G  0 lvm  /var/log/npu/dump
└─sda2                                8:2    0    7G  0 part /
```

  boot-extended partition (lvm)-root partition



```
NAME                             MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                                8:0    0   10G  0 disk
├─sda1                             8:1    0    1G  0 part /boot
├─sda2                             8:2    0    3G  0 part
│ ├─euleros-var_log_npu_oplog    253:0    0    1G  0 lvm  /var/log/npu/oplog
│ ├─euleros-var_log_npu_slog     253:1    0    1G  0 lvm  /var/log/npu/slog
│ └─euleros-var_log_npu_dump     253:2    0    1G  0 lvm  /var/log/npu/dump
└─sda3                             8:3    0    6G  0 part /
```

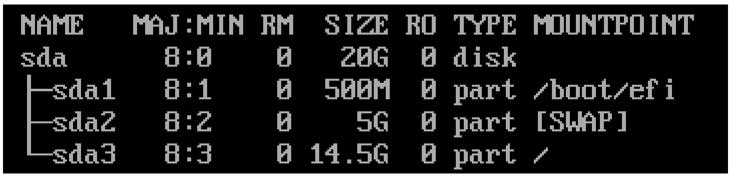
Scenario 2: UEFI Boot

If a BMS is booted in UEFI mode, UEFI needs to be configured for the image used to create the BMS. For an x86 BMS with the UEFI boot mode, MBR partitioning is required and the boot_efi partition is mandatory.

- **If the primary partition meets your requirements:**

  A: If the swap partition is independent, use the following partitioning:

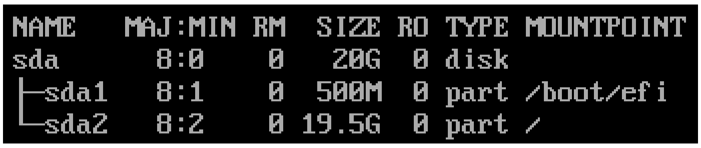
  boot_efi-swap-root partition



```
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   20G  0 disk
├─sda1   8:1    0  500M  0 part /boot/efi
├─sda2   8:2    0    5G  0 part [SWAP]
└─sda3   8:3    0 14.5G  0 part /
```

B: If the swap partition is not independent, use the following partitioning:

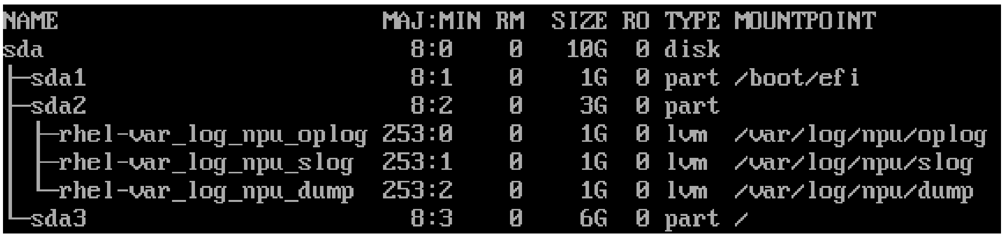
boot_efi-root partition



```
NAME    MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda       8:0    0    20G  0 disk
├─sda1    8:1    0   500M  0 part /boot/efi
└─sda2    8:2    0 19.5G  0 part /
```

- **If an extended partition is required, use the following partitioning:**

  boot_efi-extended partition (lvm)-root partition



```
NAME                          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                             8:0    0   10G  0 disk
├─sda1                          8:1    0    1G  0 part /boot/efi
├─sda2                          8:2    0    3G  0 part
│ ├─rhel-var_log_npu_oplog    253:0    0    1G  0 lvm  /var/log/npu/oplog
│ ├─rhel-var_log_npu_slog     253:1    0    1G  0 lvm  /var/log/npu/slog
│ └─rhel-var_log_npu_dump     253:2    0    1G  0 lvm  /var/log/npu/dump
└─sda3                          8:3    0    6G  0 part /
```

3.4.3 SUSE 11 SP4

1. In the **Installation Settings** phase, switch to the **Expert** tab and choose **Change** > **Partitioning**.

   Creating a swap partition

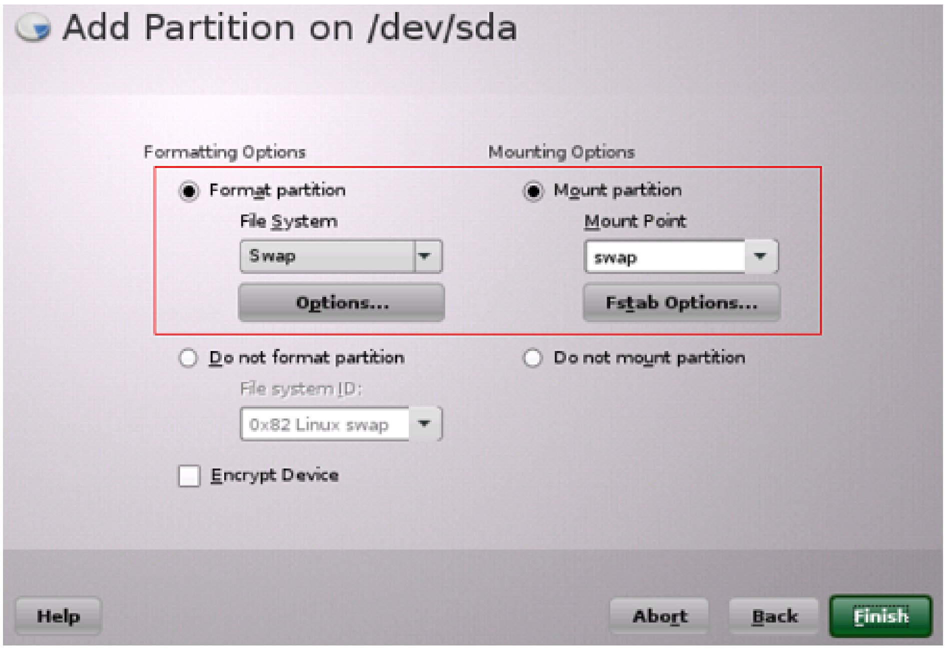
   a. On the **Preparing Hard Disk** page, select **Custom Partitioning (for experts)** and click **Next**.

   b. In the navigation pane on the left, choose **Hard Disks** and click **Add Partition**.

   c. On the **Add Partition on /dev/sda** page, select **Primary Partition** and click **Next**.

   d. Select **Custom Size**, set **Size** to **10GB**, and click **Next**.

   e. Configure **Formatting Options** and **Mounting Options**, and click **Finish**.



Add Partition on /dev/sda

Formatting Options

● Format partition

File System: Swap

○ Do not format partition

File system ID: 0x82 Linux swap

□ Encrypt Device

Mounting Options

● Mount partition

Mount Point: swap

○ Do not mount partition

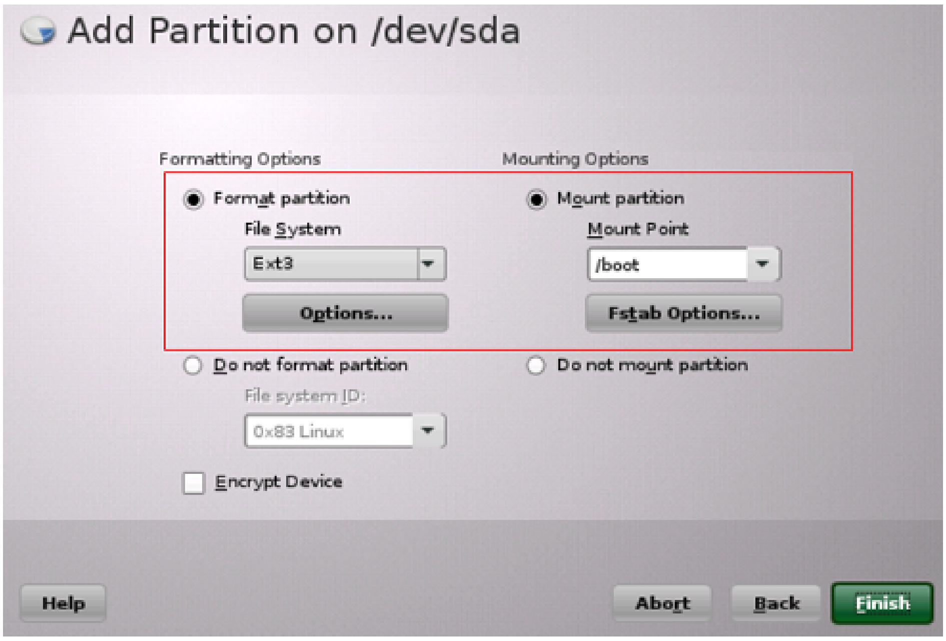
Creating a boot partition

a. In the navigation pane on the left, choose **Hard Disks** and click **Add Partition**.

b. On the **Add Partition on /dev/sda** page, select **Primary Partition** and click **Next**.

c. Select **Custom Size**, set **Size** to **5.00GB**, and click **Next**.

d. Configure **Formatting Options** and **Mounting Options**, and click **Finish**.



Add Partition on /dev/sda

Formatting Options

● Format partition

File System: Ext3

○ Do not format partition

File system ID: 0x83 Linux

□ Encrypt Device

Mounting Options

● Mount partition

Mount Point: /boot

○ Do not mount partition

The swap and boot partitions are created.

2. (Optional) Create volumes.

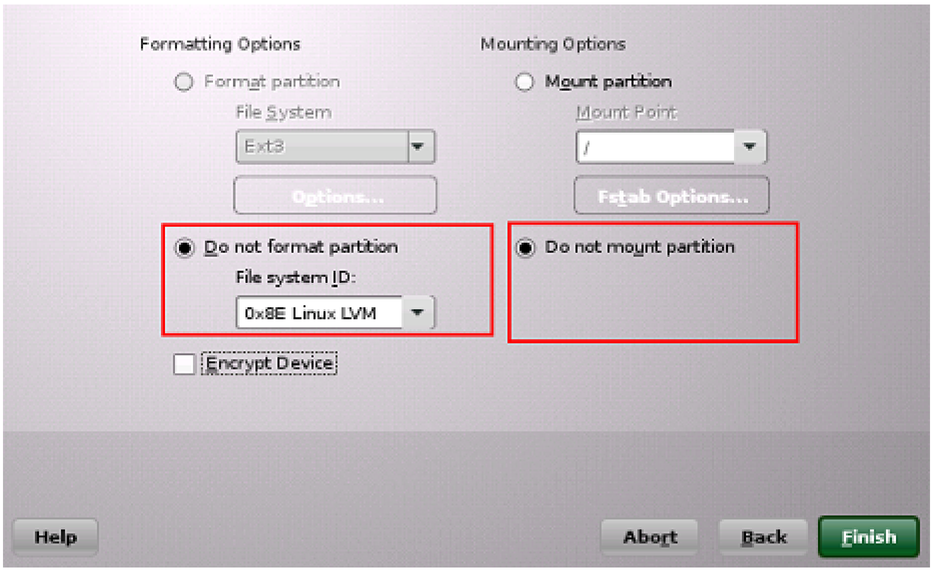
If both the swap and root volumes use LVM, perform the following operations to create volumes:

a. In the navigation pane on the left, choose **Hard Disks** and click **Add Partition**.

b. On the **Add Partition on /dev/sda** page, select **Primary Partition** and click **Next**.

c. Select **Custom Size**, set **Size** to **14.99GB**, and click **Next**.

d. Configure **Formatting Options** and **Mounting Options**, and click **Finish**.



Formatting Options

○ Format partition

File System: Ext3

● Do not format partition

File system ID: 0x8E Linux LVM

□ Encrypt Device

Mounting Options

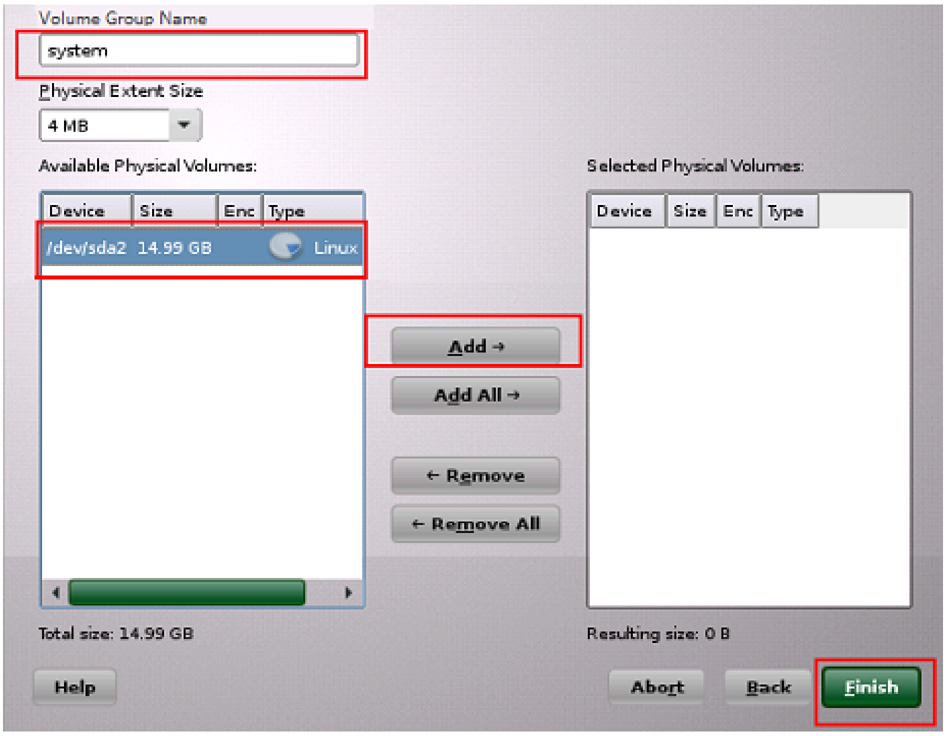
○ Mount partition

Mount Point: /

● Do not mount partition

e. In the navigation pane on the left, choose **Volume Management**. Click **Add** and then select **Volume Group**.

f. Configure required parameters and click **Finish**.



Volume Group Name: system

Physical Extent Size: 4 MB

Available Physical Volumes:

Device	Size	Enc	Type
/dev/sda2	14.99 GB		Linux

Selected Physical Volumes:

Device	Size	Enc	Type

Total size: 14.99 GB

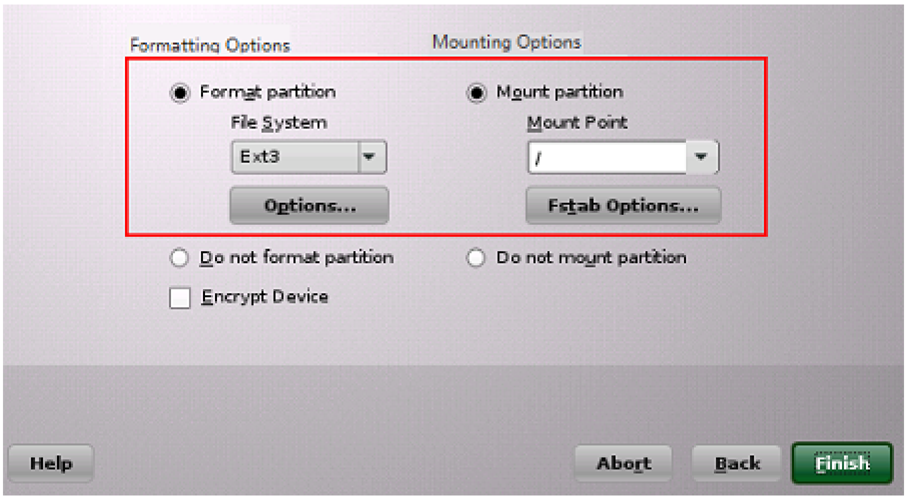
Resulting size: 0 B

g. In the navigation pane on the left, choose **Volume Management**. Click **Add** and then select **Logical Volume**.

h. Set **Name** to **root** and **Type** to **Normal Volume**, and click **Next**.

i. Set **Custom Size** to **10.00 GB** and click **Next**.

j. Configure **Formatting Options** and **Mounting Options**, and click **Finish**.



Formatting Options

● Format partition

File System: Ext3

○ Do not format partition

□ Encrypt Device

Mounting Options

● Mount partition

Mount Point: /

○ Do not mount partition

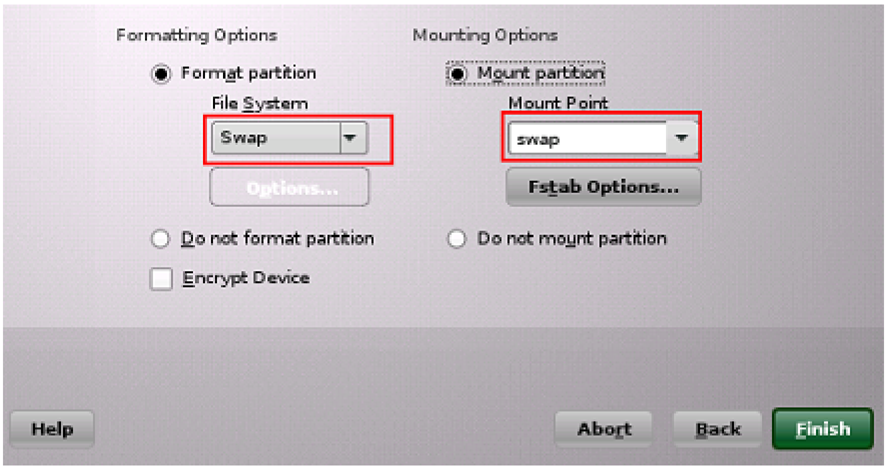
The root volume is created. The following steps describe how to create the swap volume.

k. In the navigation pane on the left, choose **Volume Management**. Click **Add** and then select **Logical Volume**.

l. Set **Name** to **swap** and **Type** to **Normal Volume**, and click **Next**.

m. Set **Size** to **Maximum Size (4.99 GB)** and click **Next**.

n. Configure **Formatting Options** and **Mounting Options**, and click **Finish**.



Formatting Options

● Format partition

File System: Swap

○ Do not format partition

□ Encrypt Device

Mounting Options

● Mount partition

Mount Point: swap

○ Do not mount partition

Click **Accept**.

The root and swap volumes are created.

3. Return to the **Installation Settings** page and check the current **Partitioning** and **Booting** configurations. Confirm the configurations and click **Install**.
4. Click **I Agree** and then **Install**.
5. Set the password of user **root**. Click **Next**.
6. Configure **Hostname** and **Domain Name**, and click **Next**.
7. On the **Network Configuration** page, select **Use Following Configuration** and click **Next**.

   On the **Test Internet Connection** page, select **No, Skip This Test** to skip the network connectivity test.
8. On the **Network Services Configuration** page, select **Use Following Configuration** and click **Next**.

9. Retain the default settings on the **User Authentication Method** page and click **Next**.
10. Create a local user, for example, **suse**. Click **Next**.

    NOTE

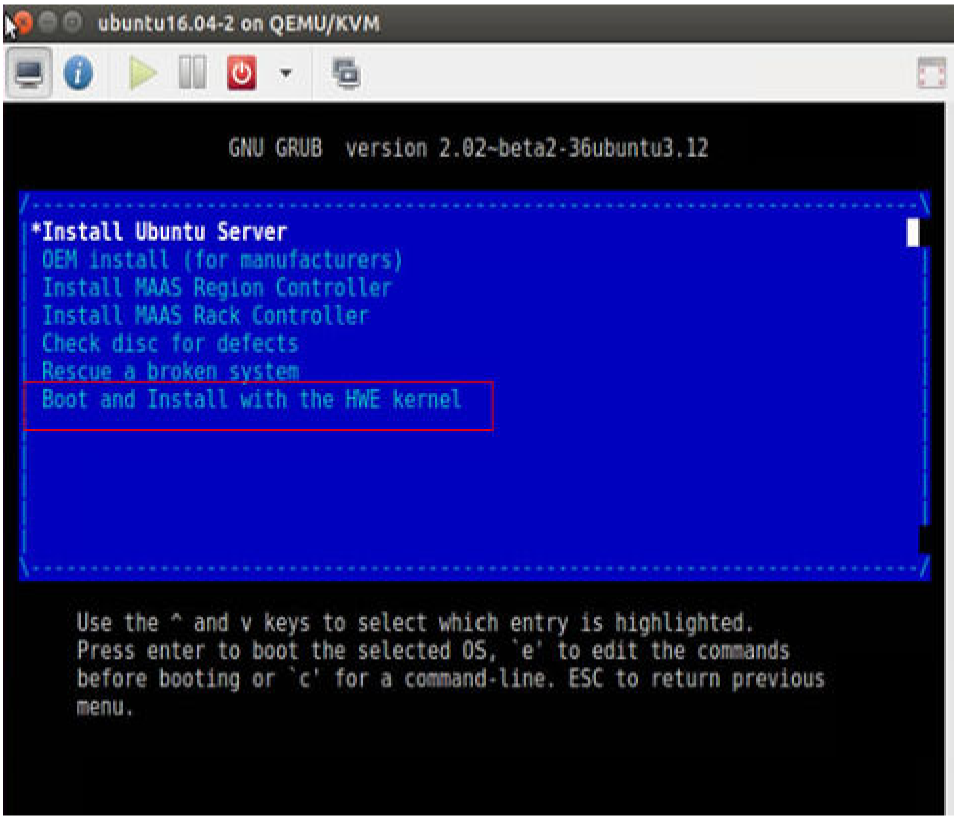
    When installing SUSE 11 SP4, you must create a local user. After the installation is complete, you can delete it if you do not need it. For details about how to delete it, see Configuring the VM Environment.
11. On the **Hardware Configuration** page, select **Use Following Configuration** and click **Next**.
12. Click **Finish**.

3.4.4 Ubuntu 18.04, Ubuntu 16.04, Ubuntu 14.04, and Debian 8.6

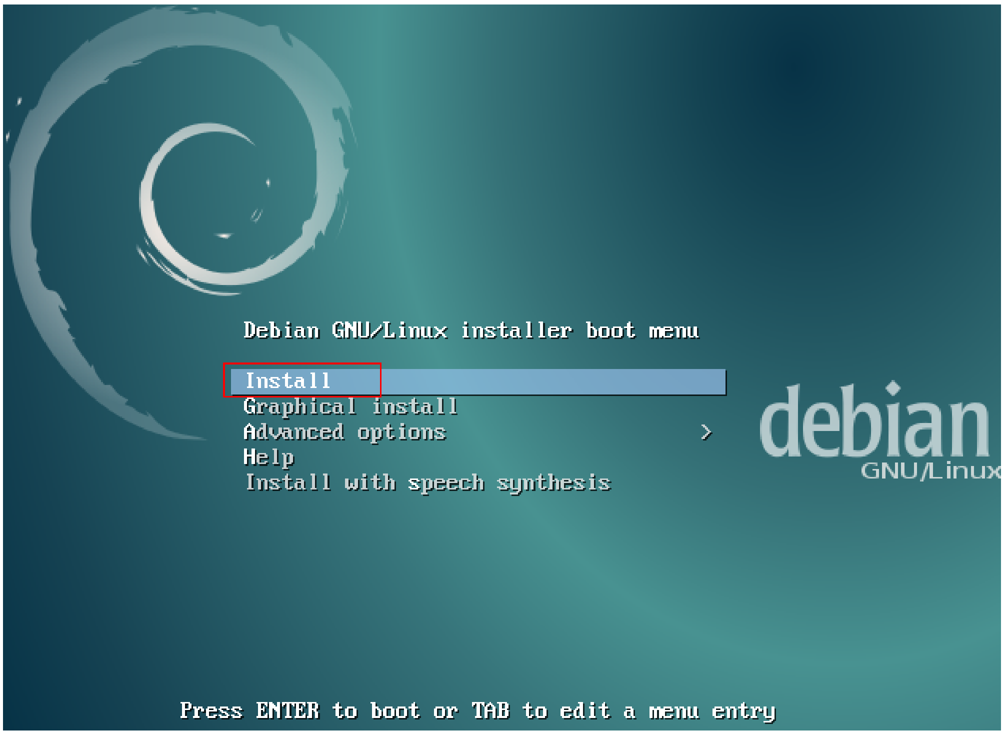
CAUTION

Use **ubuntu-***xx.xx.x***-server-amd64.iso** instead of **ubuntu-***xx.xx.x***-live-server-amd64.iso**.

1. When you install Ubuntu 18.04 or Ubuntu 16.04 ARM, select **Boot and Install with the HWE kernel** and then **Install Ubuntu Server**. (When you create an Ubuntu 18.04, Ubuntu 16.04, Ubuntu 14.04, or Debian 8.6 image, you only need to select **Install**.)

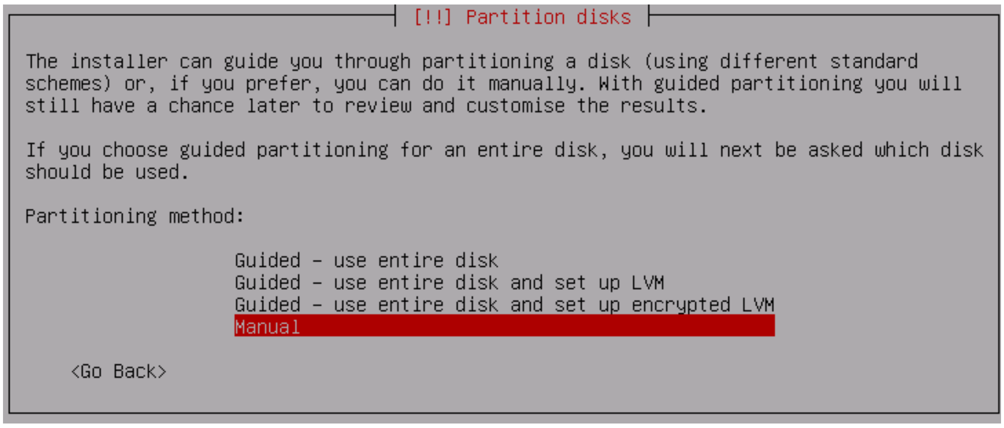


```
GNU GRUB  version 2.02~beta2-36ubuntu3.12

*Install Ubuntu Server
 OEM install (for manufacturers)
 Install MAAS Region Controller
 Install MAAS Rack Controller
 Check disc for defects
 Rescue a broken system
 Boot and Install with the HWE kernel

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line. ESC to return previous
menu.
```

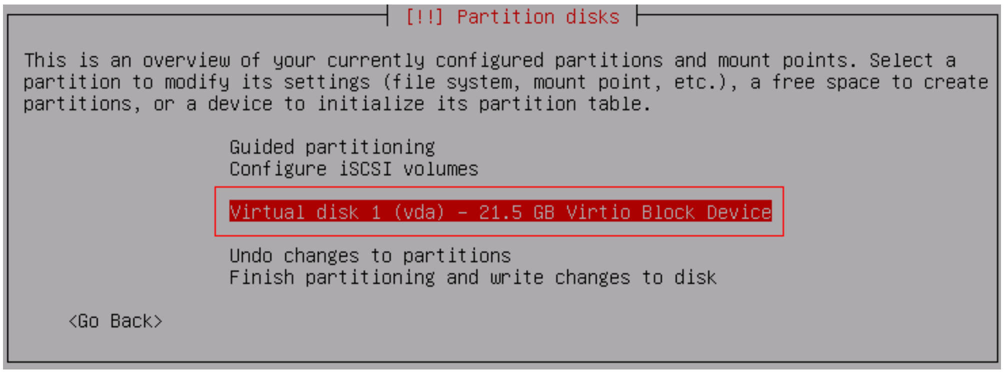


```
Debian GNU/Linux installer boot menu

 Install
 Graphical install
 Advanced options                     >
 Help
 Install with speech synthesis

Press ENTER to boot or TAB to edit a menu entry
```

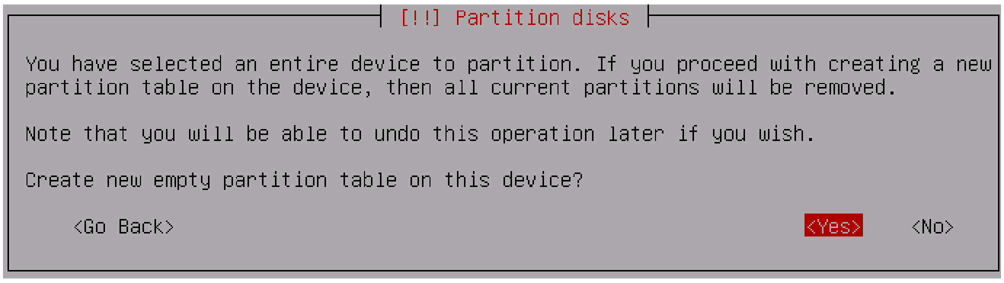
2. For Ubuntu 16.04 ARM image, select automatic partitioning. For16.04, Ubuntu 14.04, or Debian 8.6, perform the following steps for manual partitioning:



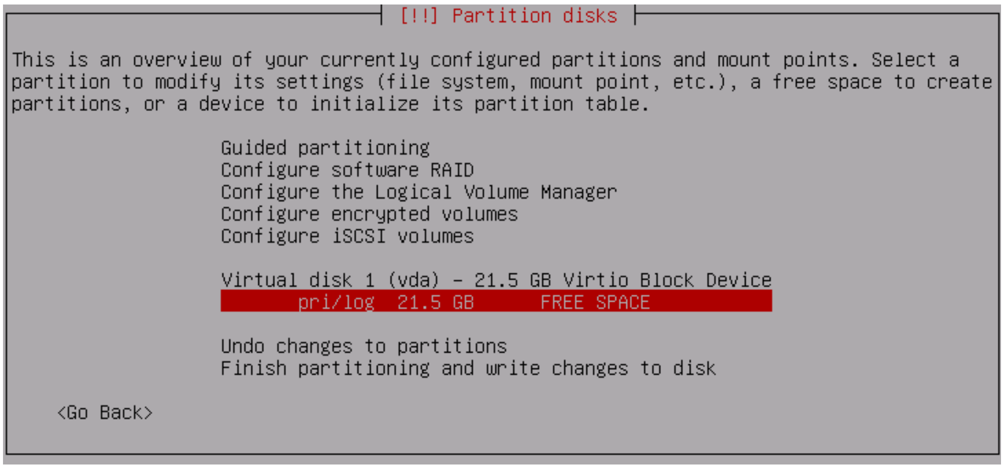
```
                          [!!] Partition disks

The installer can guide you through partitioning a disk (using different standard
schemes) or, if you prefer, you can do it manually. With guided partitioning you will
still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk
should be used.

Partitioning method:

                  Guided - use entire disk
                  Guided - use entire disk and set up LVM
                  Guided - use entire disk and set up encrypted LVM
                  Manual

    <Go Back>
```



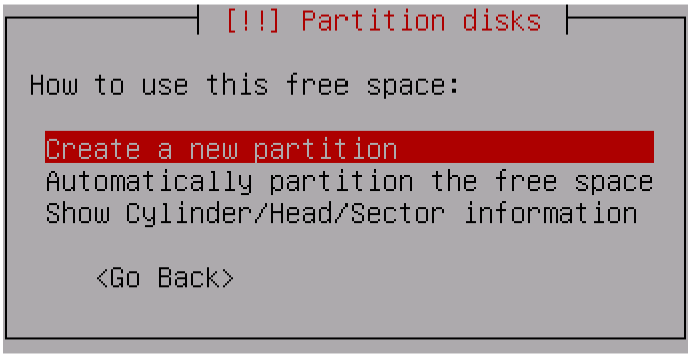
```
                          [!!] Partition disks

This is an overview of your currently configured partitions and mount points. Select a
partition to modify its settings (file system, mount point, etc.), a free space to create
partitions, or a device to initialize its partition table.

                  Guided partitioning
                  Configure iSCSI volumes

                  Virtual disk 1 (vda) - 21.5 GB Virtio Block Device

                  Undo changes to partitions
                  Finish partitioning and write changes to disk

    <Go Back>
```



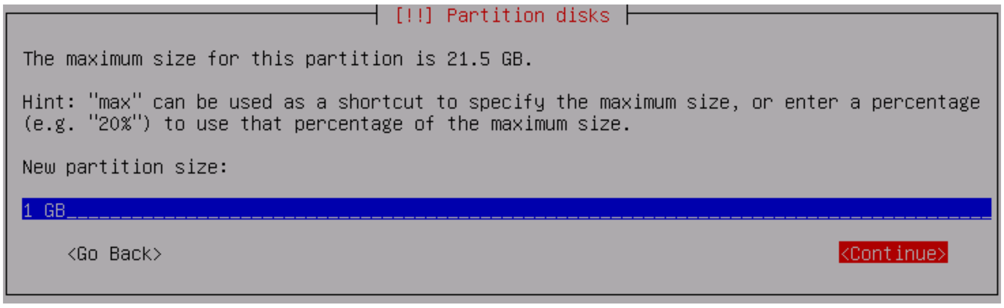
```
[!!] Partition disks

You have selected an entire device to partition. If you proceed with creating a new
partition table on the device, then all current partitions will be removed.

Note that you will be able to undo this operation later if you wish.

Create new empty partition table on this device?

    <Go Back>                                                      <Yes>    <No>
```



```
[!!] Partition disks

This is an overview of your currently configured partitions and mount points. Select a
partition to modify its settings (file system, mount point, etc.), a free space to create
partitions, or a device to initialize its partition table.

                   Guided partitioning
                   Configure software RAID
                   Configure the Logical Volume Manager
                   Configure encrypted volumes
                   Configure iSCSI volumes

                   Virtual disk 1 (vda) - 21.5 GB Virtio Block Device
                          pri/log  21.5 GB        FREE SPACE

                   Undo changes to partitions
                   Finish partitioning and write changes to disk

    <Go Back>
```

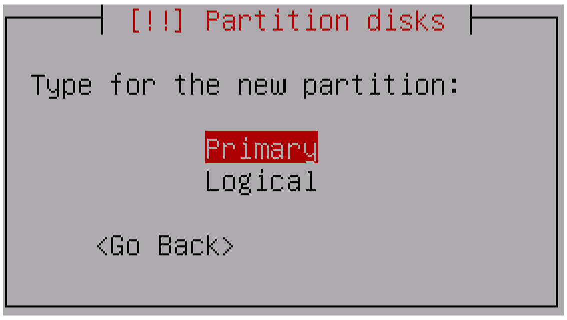


```
[!!] Partition disks

How to use this free space:

 Create a new partition
 Automatically partition the free space
 Show Cylinder/Head/Sector information

    <Go Back>
```

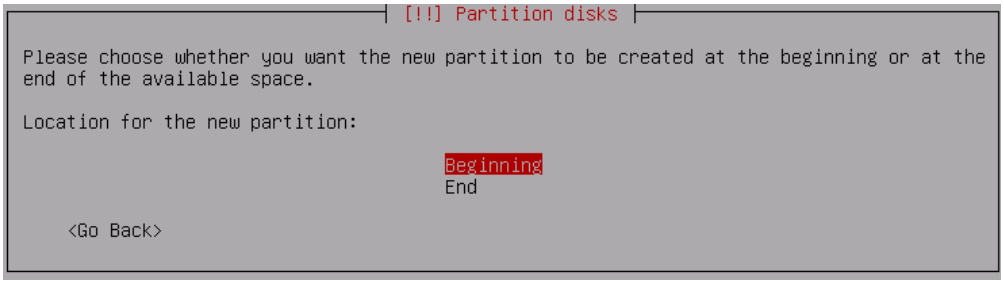


```
[!!] Partition disks

The maximum size for this partition is 21.5 GB.

Hint: "max" can be used as a shortcut to specify the maximum size, or enter a percentage
(e.g. "20%") to use that percentage of the maximum size.

New partition size:

1 GB

    <Go Back>                                                            <Continue>
```

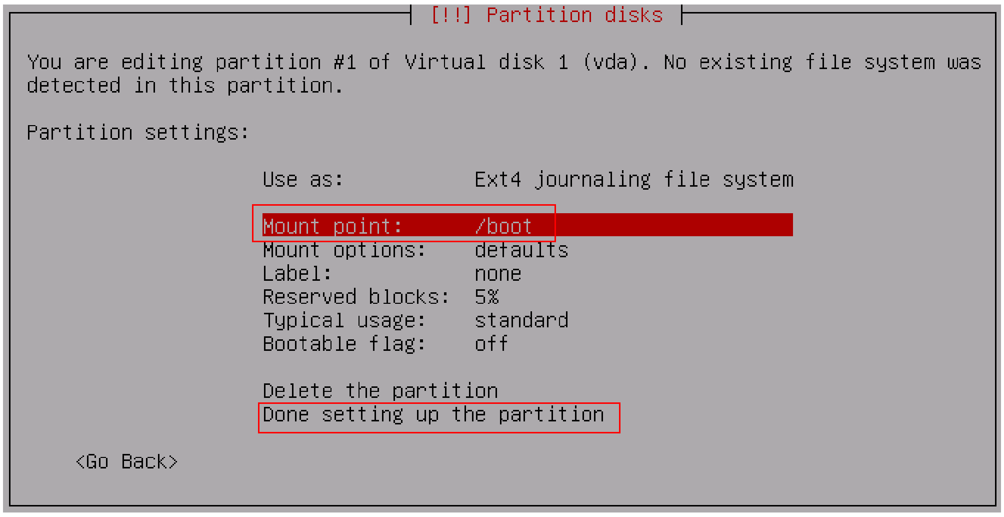
Select **Primary** rather than **Logical**, as shown in the following figure.



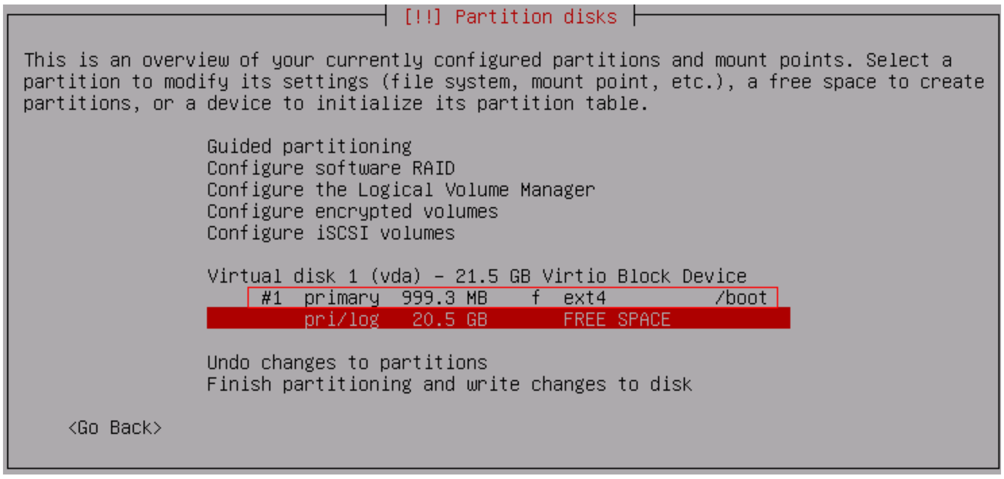
```
[!!] Partition disks

Type for the new partition:

          Primary
          Logical

    <Go Back>
```



```
[!!] Partition disks

Please choose whether you want the new partition to be created at the beginning or at the
end of the available space.

Location for the new partition:

                                  Beginning
                                  End

    <Go Back>
```

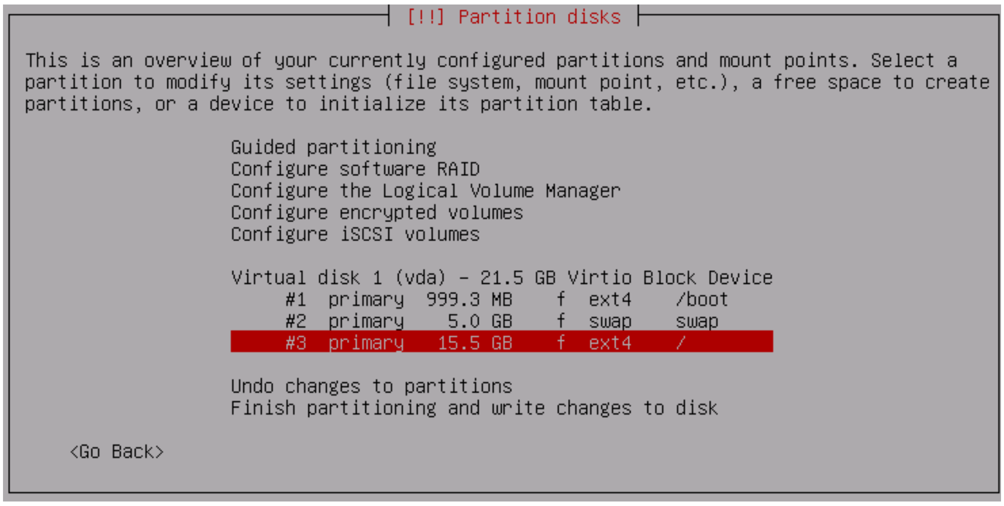


```
[!!] Partition disks

You are editing partition #1 of Virtual disk 1 (vda). No existing file system was
detected in this partition.

Partition settings:

                    Use as:           Ext4 journaling file system

                    Mount point:      /boot
                    Mount options:    defaults
                    Label:            none
                    Reserved blocks:  5%
                    Typical usage:    standard
                    Bootable flag:    off

                    Delete the partition
                    Done setting up the partition

    <Go Back>
```



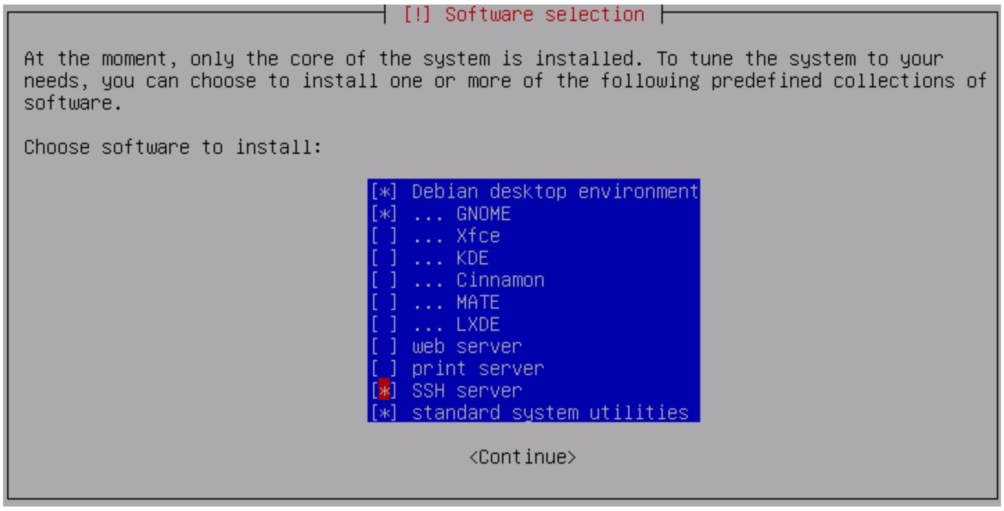
```
[!!] Partition disks

This is an overview of your currently configured partitions and mount points. Select a
partition to modify its settings (file system, mount point, etc.), a free space to create
partitions, or a device to initialize its partition table.

                 Guided partitioning
                 Configure software RAID
                 Configure the Logical Volume Manager
                 Configure encrypted volumes
                 Configure iSCSI volumes

                 Virtual disk 1 (vda) - 21.5 GB Virtio Block Device
                      #1  primary  999.3 MB     f  ext4             /boot
                          pri/log   20.5 GB        FREE SPACE

                 Undo changes to partitions
                 Finish partitioning and write changes to disk

    <Go Back>
```

The preceding figures show how to create the boot partition and are also applicable to swap and / partitions. The following figures show the partitioning results (root partition is the last partition).



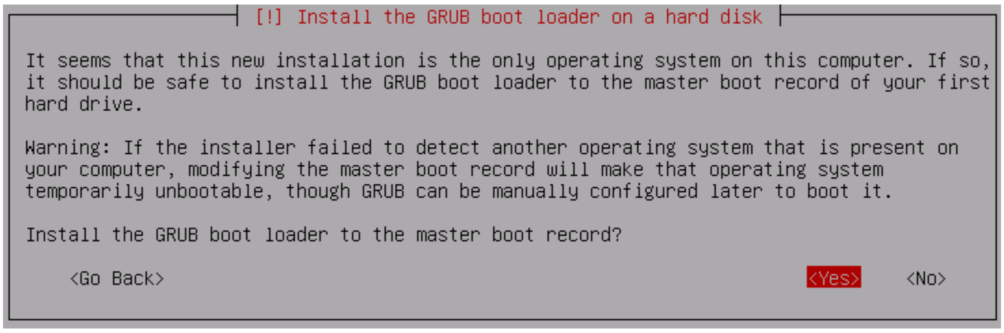
```
[!!] Partition disks

This is an overview of your currently configured partitions and mount points. Select a
partition to modify its settings (file system, mount point, etc.), a free space to create
partitions, or a device to initialize its partition table.

                   Guided partitioning
                   Configure software RAID
                   Configure the Logical Volume Manager
                   Configure encrypted volumes
                   Configure iSCSI volumes

                   Virtual disk 1 (vda) - 21.5 GB Virtio Block Device
                        #1  primary  999.3 MB    f  ext4    /boot
                        #2  primary    5.0 GB    f  swap    swap
                        #3  primary   15.5 GB    f  ext4    /

                   Undo changes to partitions
                   Finish partitioning and write changes to disk

    <Go Back>
```

Install predefined software.

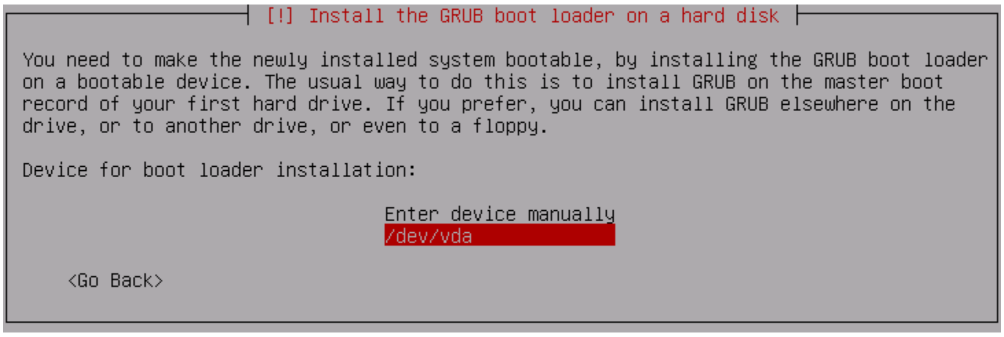


```
[!] Software selection

At the moment, only the core of the system is installed. To tune the system to your
needs, you can choose to install one or more of the following predefined collections of
software.

Choose software to install:

                                [*] Debian desktop environment
                                [*] ... GNOME
                                [ ] ... Xfce
                                [ ] ... KDE
                                [ ] ... Cinnamon
                                [ ] ... MATE
                                [ ] ... LXDE
                                [ ] web server
                                [ ] print server
                                [*] SSH server
                                [*] standard system utilities

                                         <Continue>
```

Install GRUB on your hard disk.



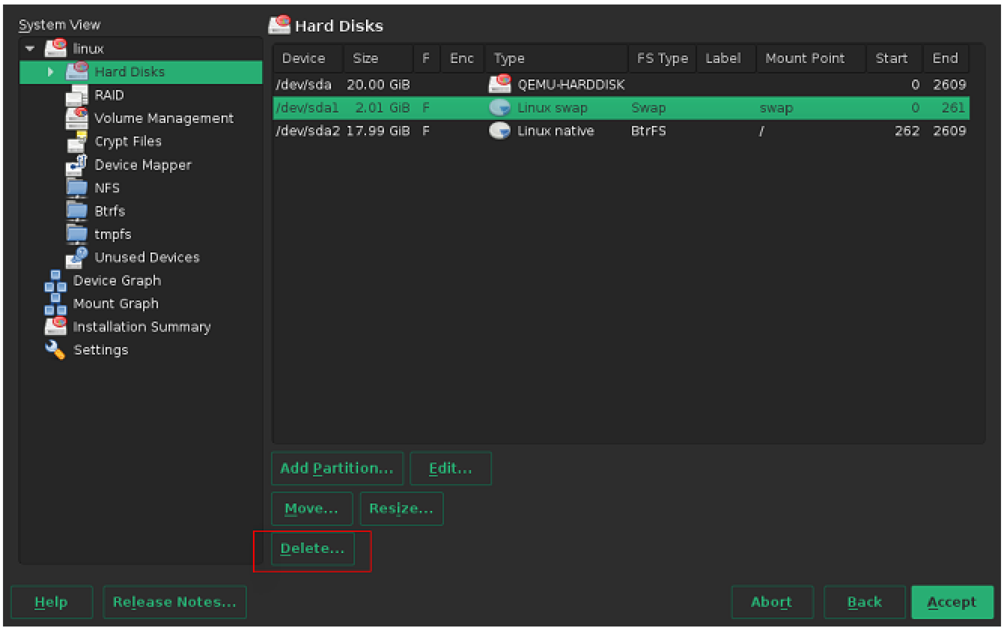
```
[!] Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so,
it should be safe to install the GRUB boot loader to the master boot record of your first
hard drive.

Warning: If the installer failed to detect another operating system that is present on
your computer, modifying the master boot record will make that operating system
temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

    <Go Back>                                                           <Yes>    <No>
```



```
[!] Install the GRUB boot loader on a hard disk

You need to make the newly installed system bootable, by installing the GRUB boot loader
on a bootable device. The usual way to do this is to install GRUB on the master boot
record of your first hard drive. If you prefer, you can install GRUB elsewhere on the
drive, or to another drive, or even to a floppy.

Device for boot loader installation:

                                 Enter device manually
                                 /dev/vda

    <Go Back>
```

3.4.5 SUSE 12

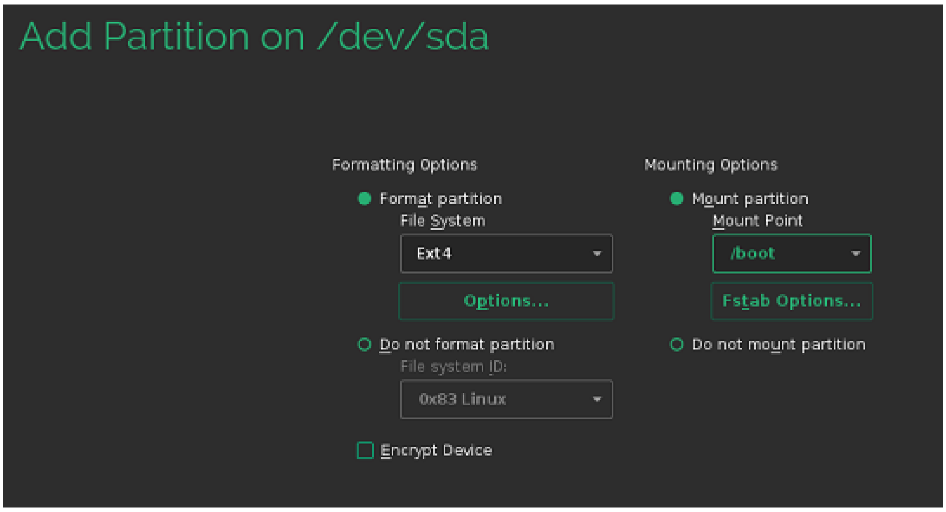
1. Click **Expert Partitioner** before you install the OS.
2. Right-click the default partition and choose **Delete** from the shortcut menu.



Hard Disks

Device	Size	F	Enc	Type	FS Type	Label	Mount Point	Start	End
/dev/sda	20.00 GiB			QEMU-HARDDISK				0	2609
/dev/sda1	2.01 GiB	F		Linux swap	Swap		swap	0	261
/dev/sda2	17.99 GiB	F		Linux native	BtrFS		/	262	2609

3. Partition the disk based on service requirements. The following is for reference only.
   a. In the navigation pane on the left, choose **Hard Disks** and click **Add Partition**.
   b. Select **Primary Partition** and click **Next**.
   c. Set the value of **Size** to **500 MiB** (for example) or based on service requirements.
   d. Select **Operating System** for **Role** and click **Next**.
   e. Select **File System** and **Mount Point**, and click **Finish**.



Add Partition on /dev/sda

Formatting Options

● Format partition

File System: Ext4

○ Do not format partition

File system ID: 0x83 Linux

□ Encrypt Device

Mounting Options

● Mount partition

Mount Point: /boot

○ Do not mount partition

The boot partition is created.

4. If both the swap and root volumes use LVM, perform the following operations to create volumes:

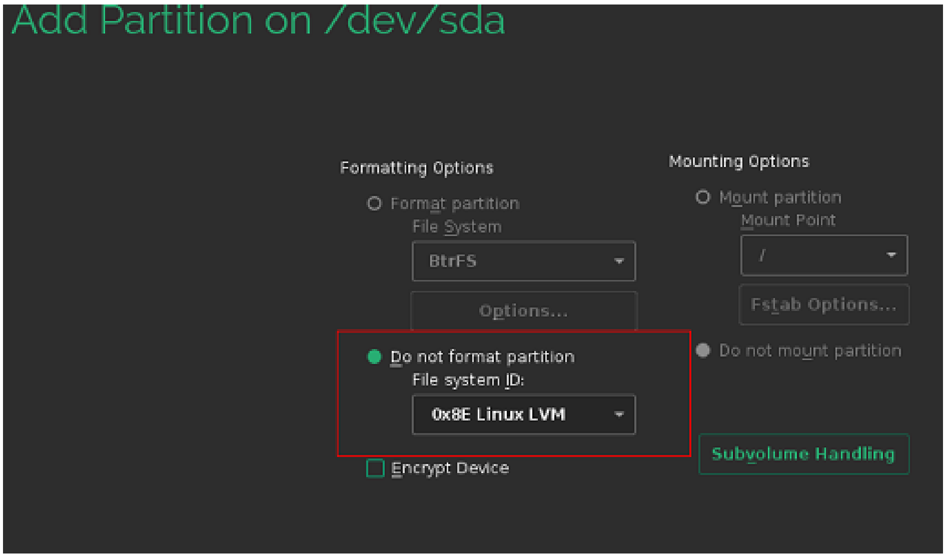
a. In the navigation pane on the left, choose **Hard Disks** and click **Add Partition**.

b. Select **Primary Partition** and click **Next**.

c. Select **Custom Size**, set **Size** to **19.50 GB**, and click **Next**.

d. Select **Operating System** for **Role** and click **Next**.

e. Configure **Formatting Options** and click **Finish**.



Add Partition on /dev/sda

Formatting Options

○ Format partition

File System: BtrFS

● Do not format partition

File system ID: 0x8E Linux LVM

□ Encrypt Device

Mounting Options

○ Mount partition

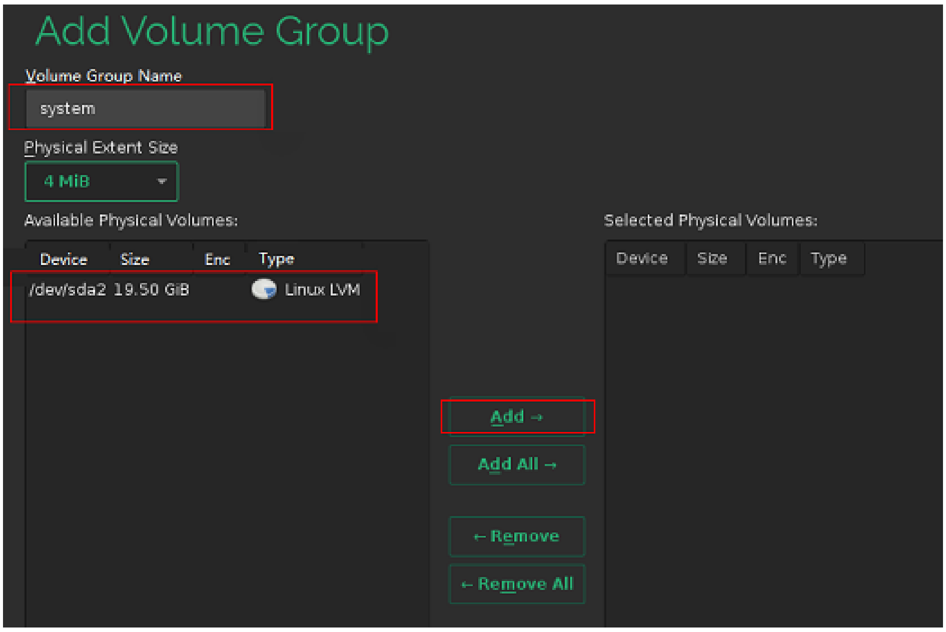
Mount Point: /

● Do not mount partition

f. In the navigation pane on the left, choose **Volume Management**. Click **Add** and then select **Volume Group**.

g. Configure parameters shown in the following figure and click **Add** to add available physical volumes to the **Selected Physical Volumes** area.

Click **Finish**.



Add Volume Group

Volume Group Name: system

Physical Extent Size: 4 MiB

Available Physical Volumes:

Device	Size	Enc	Type
/dev/sda2	19.50 GiB		Linux LVM

Selected Physical Volumes:

Device	Size	Enc	Type

h. In the navigation pane on the left, choose **Volume Management**. Click **Add** and then select **Logical Volume**.

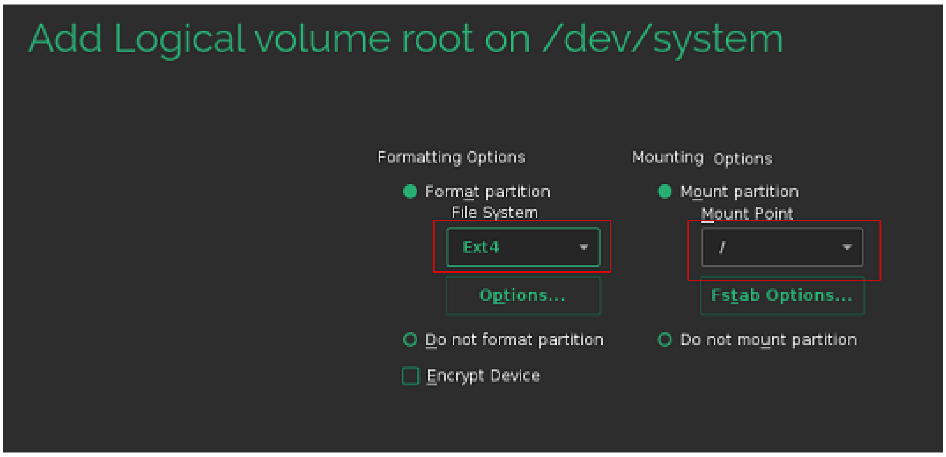
i. Set the logical volume name to **swap** and size to **5 GiB**.

j. Select **Operating System** for **Role**.

k. Configure **Formatting Options** and **Mounting Options**, and click **Finish**.

l. Create the root volume in the similar way as the swap volume. Set the logical volume name to **root** and size to **14.50 GiB**.

Configure **Formatting Options** and **Mounting Options** and click **Finish**.



Add Logical volume root on /dev/system

Formatting Options

● Format partition

File System: Ext4

○ Do not format partition

□ Encrypt Device

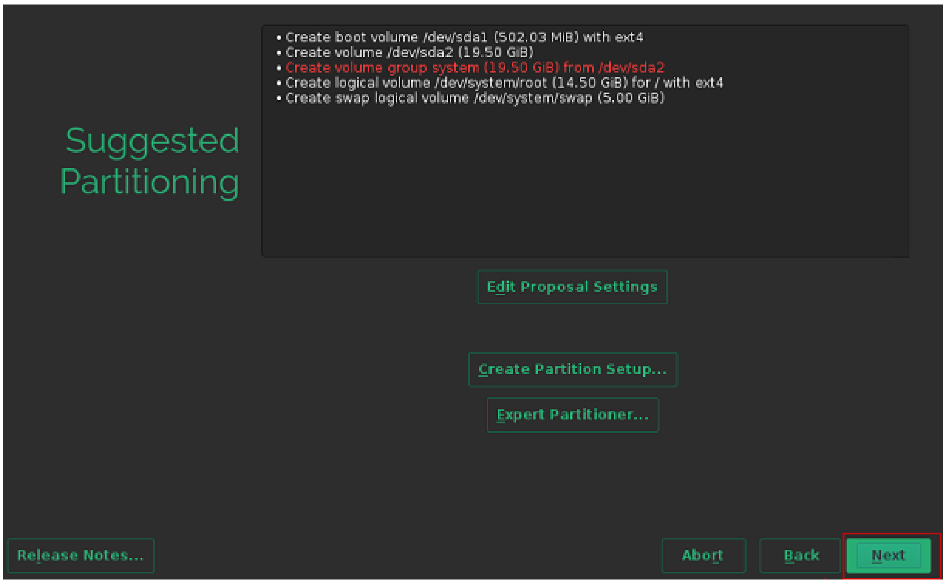
Mounting Options

● Mount partition

Mount Point: /

○ Do not mount partition

Check the partitions and volumes.



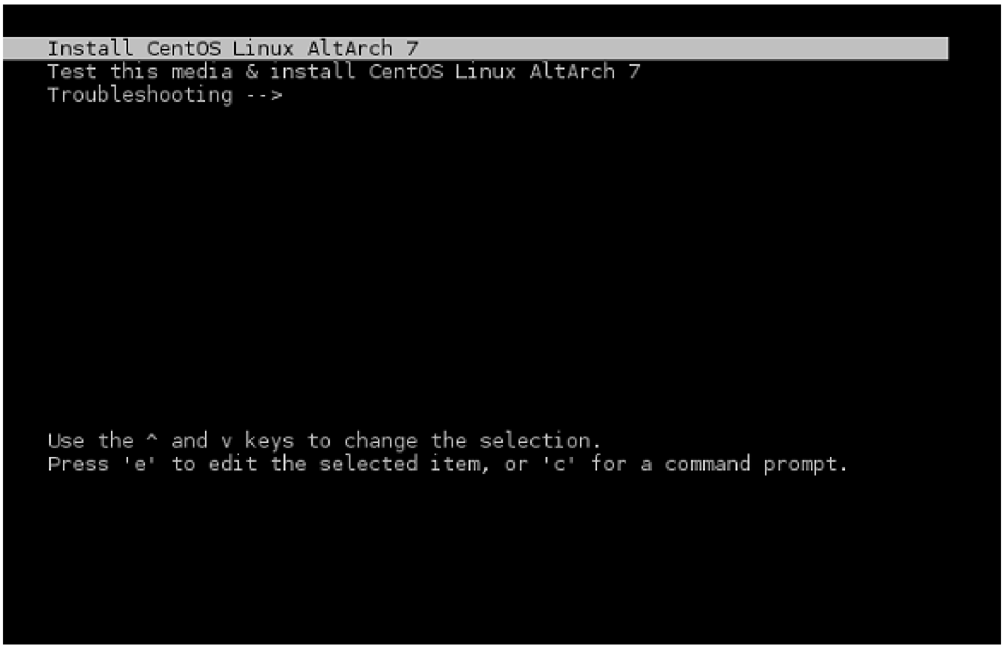
Suggested Partitioning

```
• Create boot volume /dev/sda1 (502.03 MiB) with ext4
• Create volume /dev/sda2 (19.50 GiB)
• Create volume group system (19.50 GiB) from /dev/sda2
• Create logical volume /dev/system/root (14.50 GiB) for / with ext4
• Create swap logical volume /dev/system/swap (5.00 GiB)
```

The partitions and volumes are created successfully. Click **Next** and continue the OS installation as prompted.

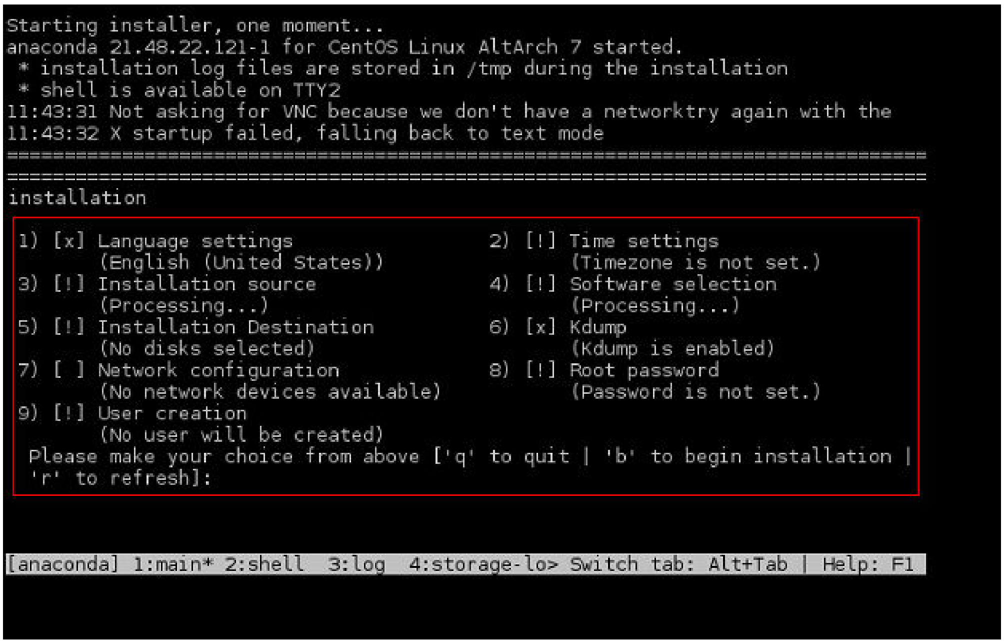
3.4.6 CentOS 7.4 ARM

1. Select **Install CentOS Linux AltArch 7**.



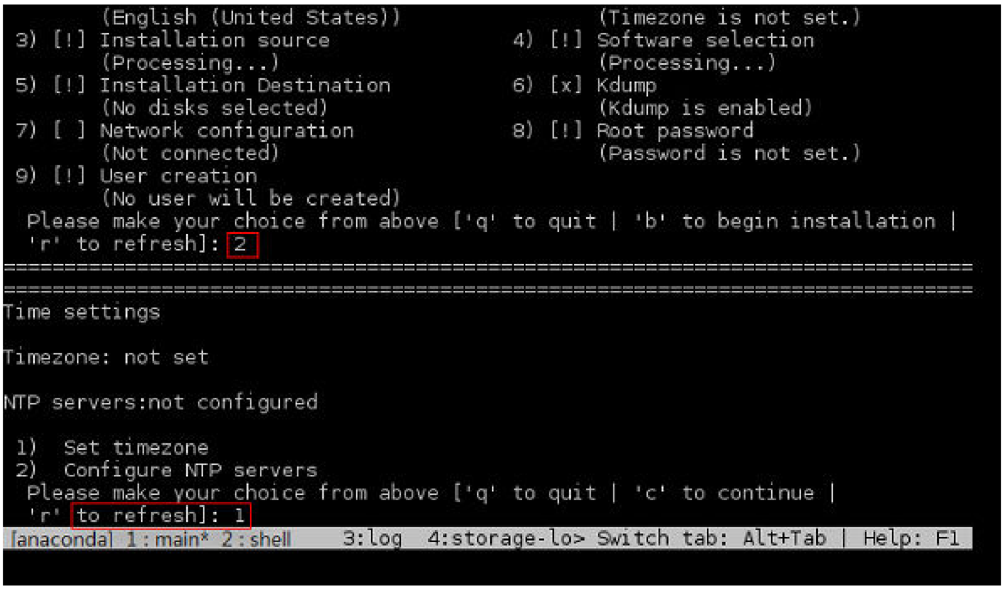
```
    Install CentOS Linux AltArch 7
    Test this media & install CentOS Linux AltArch 7
    Troubleshooting -->




    Use the ^ and v keys to change the selection.
    Press 'e' to edit the selected item, or 'c' for a command prompt.
```

2. View the installation configuration items.

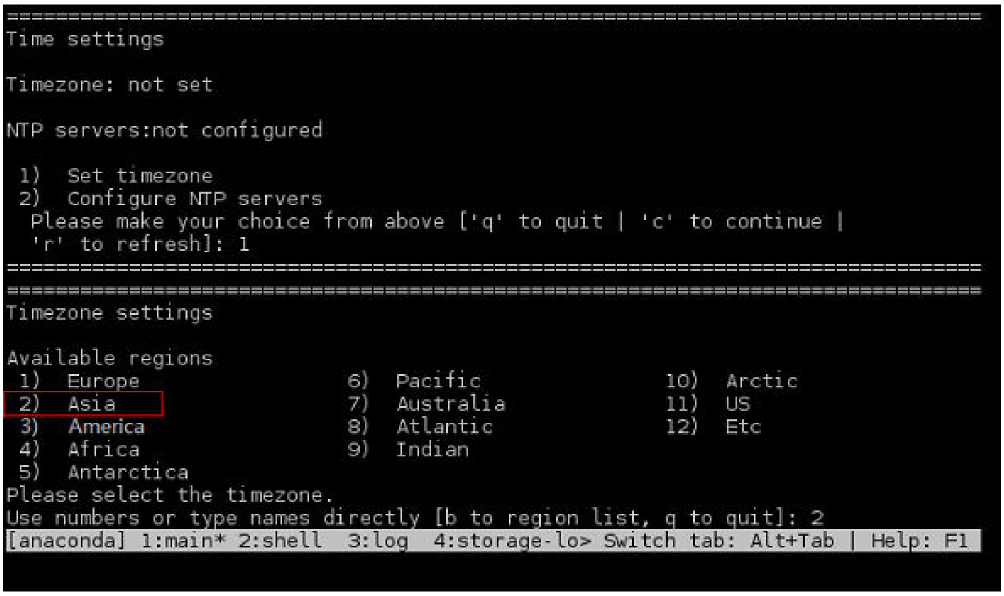


```
Starting installer, one moment...
anaconda 21.48.22.121-1 for CentOS Linux AltArch 7 started.
 * installation log files are stored in /tmp during the installation
 * shell is available on TTY2
11:43:31 Not asking for VNC because we don't have a networktry again with the
11:43:32 X startup failed, falling back to text mode
================================================================================
================================================================================
installation

 1) [x] Language settings                 2) [!] Time settings
        (English (United States))                (Timezone is not set.)
 3) [!] Installation source               4) [!] Software selection
        (Processing...)                          (Processing...)
 5) [!] Installation Destination          6) [x] Kdump
        (No disks selected)                      (Kdump is enabled)
 7) [ ] Network configuration             8) [!] Root password
        (No network devices available)           (Password is not set.)
 9) [!] User creation
        (No user will be created)
  Please make your choice from above ['q' to quit | 'b' to begin installation |
  'r' to refresh]:


[anaconda] 1:main* 2:shell  3:log  4:storage-lo> Switch tab: Alt+Tab | Help: F1
```

3. Configure the time zone.

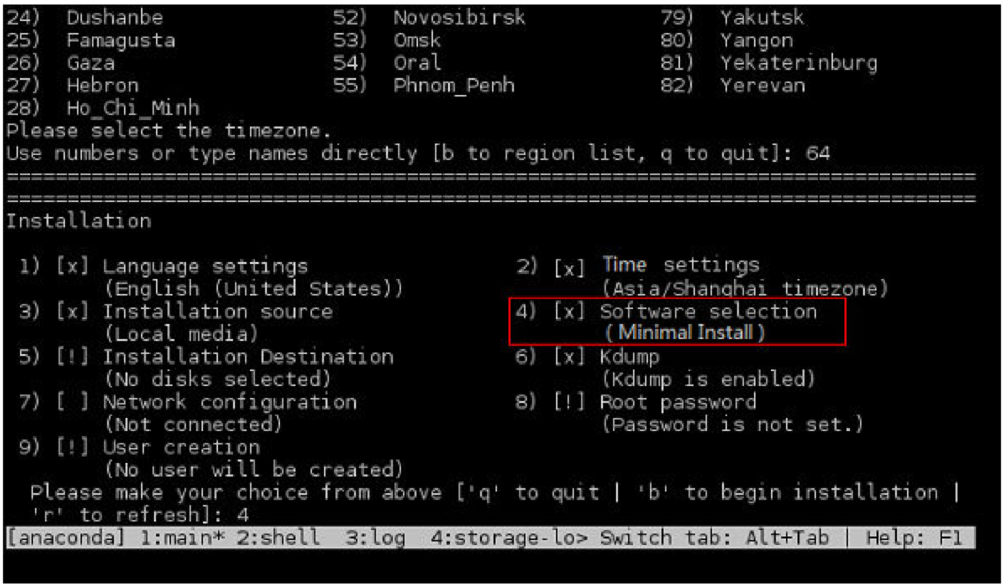


```
        (English (United States))                (Timezone is not set.)
 3) [!] Installation source                4) [!] Software selection
        (Processing...)                          (Processing...)
 5) [!] Installation Destination           6) [x] Kdump
        (No disks selected)                      (Kdump is enabled)
 7) [ ] Network configuration              8) [!] Root password
        (Not connected)                          (Password is not set.)
 9) [!] User creation
        (No user will be created)
  Please make your choice from above ['q' to quit | 'b' to begin installation |
  'r' to refresh]: 2
================================================================================
================================================================================
Time settings

Timezone: not set

NTP servers:not configured

 1)  Set timezone
 2)  Configure NTP servers
  Please make your choice from above ['q' to quit | 'c' to continue |
  'r' to refresh]: 1
[anaconda] 1:main* 2:shell   3:log  4:storage-lo> Switch tab: Alt+Tab | Help: F1
```

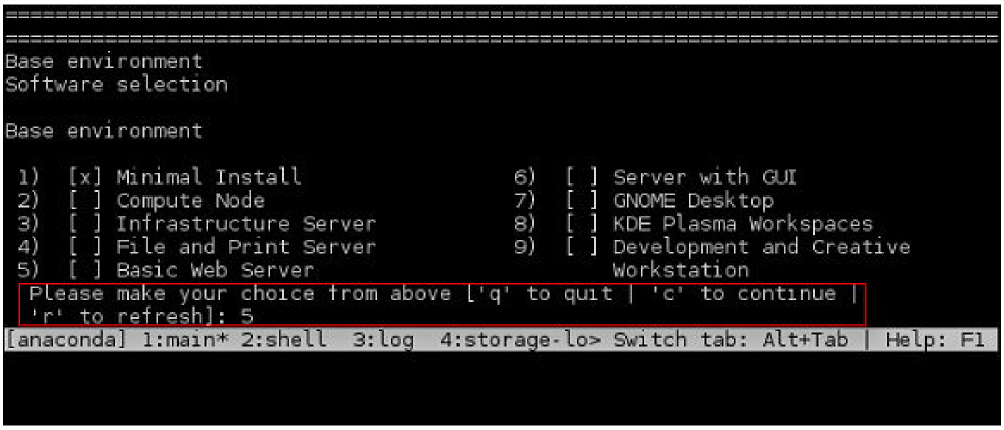


```
================================================================================
Time settings

Timezone: not set

NTP servers:not configured

 1)  Set timezone
 2)  Configure NTP servers
  Please make your choice from above ['q' to quit | 'c' to continue |
  'r' to refresh]: 1
================================================================================
================================================================================
Timezone settings

Available regions
 1)  Europe                  6)  Pacific             10)  Arctic
 2)  Asia                    7)  Australia           11)  US
 3)  America                 8)  Atlantic            12)  Etc
 4)  Africa                  9)  Indian
 5)  Antarctica
Please select the timezone.
Use numbers or type names directly [b to region list, q to quit]: 2
[anaconda] 1:main* 2:shell  3:log  4:storage-lo> Switch tab: Alt+Tab | Help: F1
```

4. Select the software to be installed.

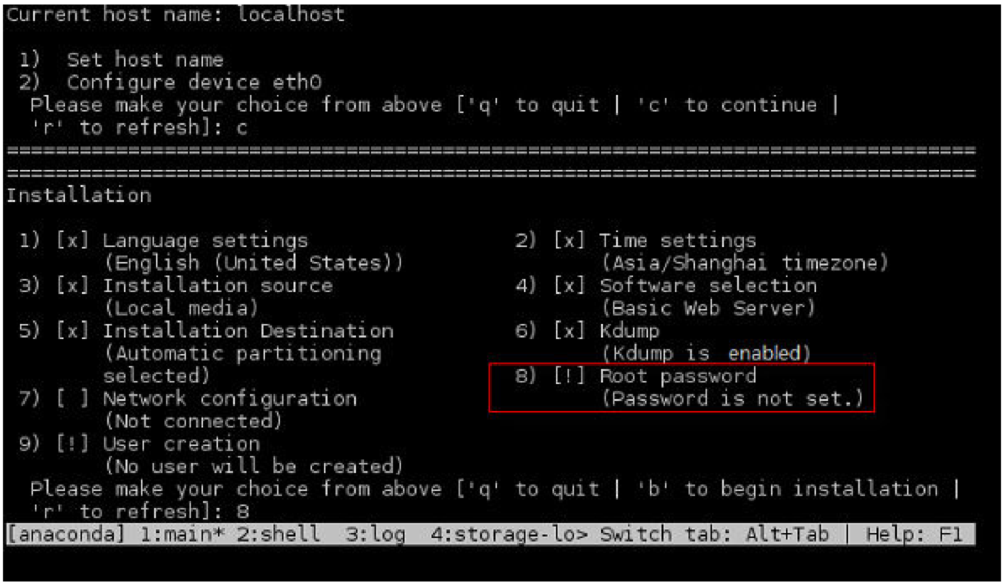


```
24)  Dushanbe              52)  Novosibirsk           79)  Yakutsk
25)  Famagusta             53)  Omsk                  80)  Yangon
26)  Gaza                  54)  Oral                  81)  Yekaterinburg
27)  Hebron                55)  Phnom_Penh            82)  Yerevan
28)  Ho_Chi_Minh
Please select the timezone.
Use numbers or type names directly [b to region list, q to quit]: 64
================================================================================
================================================================================
Installation

 1) [x] Language settings                 2) [x] Time settings
        (English (United States))                (Asia/Shanghai timezone)
 3) [x] Installation source               4) [x] Software selection
        (Local media)                            ( Minimal Install )
 5) [!] Installation Destination          6) [x] Kdump
        (No disks selected)                      (Kdump is enabled)
 7) [ ] Network configuration             8) [!] Root password
        (Not connected)                          (Password is not set.)
 9) [!] User creation
        (No user will be created)
  Please make your choice from above ['q' to quit | 'b' to begin installation |
  'r' to refresh]: 4
[anaconda] 1:main* 2:shell  3:log  4:storage-lo> Switch tab: Alt+Tab | Help: F1
```



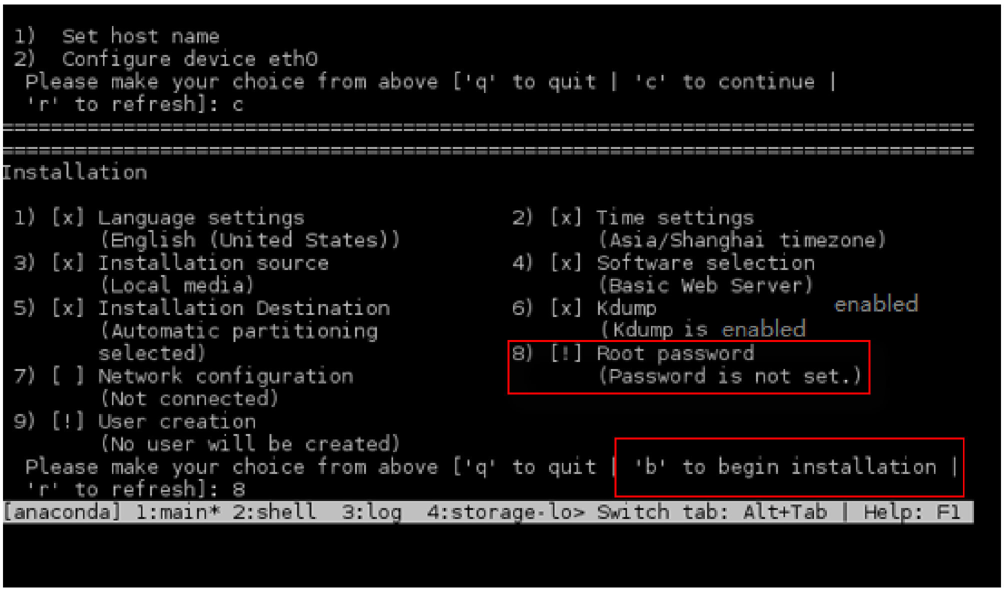
```
================================================================================
================================================================================
Base environment
Software selection

Base environment

 1)  [x] Minimal Install                 6)  [ ] Server with GUI
 2)  [ ] Compute Node                    7)  [ ] GNOME Desktop
 3)  [ ] Infrastructure Server           8)  [ ] KDE Plasma Workspaces
 4)  [ ] File and Print Server           9)  [ ] Development and Creative
 5)  [ ] Basic Web Server                        Workstation
  Please make your choice from above ['q' to quit | 'c' to continue |
  'r' to refresh]: 5
[anaconda] 1:main* 2:shell  3:log  4:storage-lo> Switch tab: Alt+Tab | Help: F1
```

5. Configure the system password.



```
Current host name: localhost

 1)  Set host name
 2)  Configure device eth0
  Please make your choice from above ['q' to quit | 'c' to continue |
  'r' to refresh]: c
================================================================================
================================================================================
Installation

 1) [x] Language settings                 2) [x] Time settings
        (English (United States))                (Asia/Shanghai timezone)
 3) [x] Installation source               4) [x] Software selection
        (Local media)                            (Basic Web Server)
 5) [x] Installation Destination          6) [x] Kdump
        (Automatic partitioning                  (Kdump is  enabled)
        selected)                         8) [!] Root password
 7) [ ] Network configuration                    (Password is not set.)
        (Not connected)
 9) [!] User creation
        (No user will be created)
  Please make your choice from above ['q' to quit | 'b' to begin installation |
  'r' to refresh]: 8
[anaconda] 1:main* 2:shell  3:log  4:storage-lo> Switch tab: Alt+Tab | Help: F1
```

6. Enter **b** and press **Enter** to start the installation.



```
 1)  Set host name
 2)  Configure device eth0
  Please make your choice from above ['q' to quit | 'c' to continue |
  'r' to refresh]: c
================================================================================
================================================================================
Installation

 1) [x] Language settings                    2) [x] Time settings
        (English (United States))                   (Asia/Shanghai timezone)
 3) [x] Installation source                  4) [x] Software selection
        (Local media)                               (Basic Web Server)
 5) [x] Installation Destination             6) [x] Kdump                  enabled
        (Automatic partitioning                     (Kdump is enabled
        selected)                            8) [!] Root password
 7) [ ] Network configuration                       (Password is not set.)
        (Not connected)
 9) [!] User creation
        (No user will be created)
  Please make your choice from above ['q' to quit | 'b' to begin installation |
  'r' to refresh]: 8
[anaconda] 1:main* 2:shell  3:log  4:storage-lo> Switch tab: Alt+Tab | Help: F1
```

3.5 Modifying the Boot File (UEFI Boot Mode)

In the UEFI boot mode, you must modify the boot file. Otherwise, BMSs provisioned using the VM image may fail to start after they are forcibly restarted.

After the OS is installed, do not restart the VM immediately. Press **Ctrl + Alt + F2** to enter the CLI and perform the operations in this section to modify the boot file.

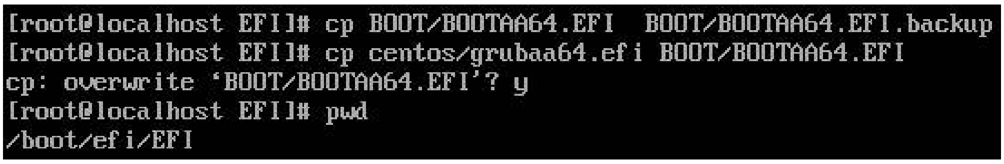
NOTE

- Startup failure cause and solution: When an image is created from a VM, the boot file in the image may encounter an error due to file format inconsistency. As a result, the BMS created from the image will fail to be forcibly restarted. You need to optimize the GRUB file to rectify this issue.
- Relevant to OS or not: The startup failure is irrelevant to the OS. You are advised to optimize the GRUB file for the VMs booted in UEFI mode.
- Impact: If no action is taken, it is possible that the BMS startup will fail. As a result, services cannot run on the BMS properly.

Arm

Run the **find / -name "boot/efi/EFI"** command to locate the boot file. Replace **boot/efi/EFI/BOOT/BOOTAA64.EFI** with **boot/efi/EFI/***$os_version***/grubaa64.efi**.

For example, *$os_version* for CentOS 7.4 is **centos**. Replace **boot/efi/EFI/BOOT/BOOTAA64.EFI** with **boot/efi/EFI/centos/grubaa64.efi**.



```
[root@localhost EFI]# cp BOOT/BOOTAA64.EFI  BOOT/BOOTAA64.EFI.backup
[root@localhost EFI]# cp centos/grubaa64.efi BOOT/BOOTAA64.EFI
cp: overwrite 'BOOT/BOOTAA64.EFI'? y
[root@localhost EFI]# pwd
/boot/efi/EFI
```

The location of **grubaa64.efi** varies depending on the OS. For details, see Table 3-3.

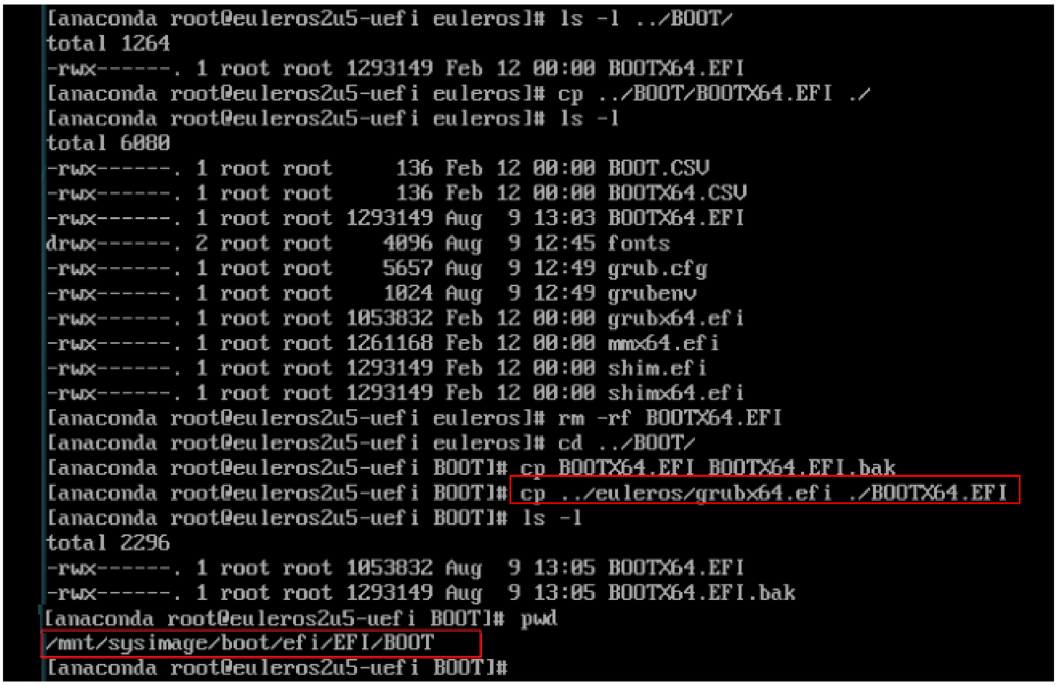
Table 3-3 Location of **grubaa64.efi**

OS	grubaa64.efi Location
CentOS	/boot/efi/EFI/centos/grubaa64.efi
EulerOS	/boot/efi/EFI/euleros/grubaa64.efi
SUSE	/boot/efi/EFI/sles/grubaa64.efi
Ubuntu	/boot/efi/EFI/ubuntu/grubaa64.efi
Red Hat	/boot/efi/EFI/redhat/grubaa64.efi

x86

Run the **find / -name "boot/efi/EFI"** command to locate the boot file. For example, the boot file of EulerOS 2.5 is located in **/boot/efi/EFI**. Replace **/boot/efi/EFI/BOOT/BOOTX64.EFI** with **/boot/efi/EFI/***$os_version***/grubx64.efi**.

For example, *$os_version* for EulerOS 2.5 is **euleros**. Replace **/boot/efi/EFI/BOOT/BOOTX64.EFI** with **/boot/efi/EFI/euleros/grubx64.efi**.



```
[anaconda root@euleros2u5-uefi euleros]# ls -l ../BOOT/
total 1264
-rwx------. 1 root root 1293149 Feb 12 00:00 BOOTX64.EFI
[anaconda root@euleros2u5-uefi euleros]# cp ../BOOT/BOOTX64.EFI ./
[anaconda root@euleros2u5-uefi euleros]# ls -l
total 6080
-rwx------. 1 root root     136 Feb 12 00:00 BOOT.CSV
-rwx------. 1 root root     136 Feb 12 00:00 BOOTX64.CSV
-rwx------. 1 root root 1293149 Aug  9 13:03 BOOTX64.EFI
drwx------. 2 root root    4096 Aug  9 12:45 fonts
-rwx------. 1 root root    5657 Aug  9 12:49 grub.cfg
-rwx------. 1 root root    1024 Aug  9 12:49 grubenv
-rwx------. 1 root root 1053832 Feb 12 00:00 grubx64.efi
-rwx------. 1 root root 1261168 Feb 12 00:00 mmx64.efi
-rwx------. 1 root root 1293149 Feb 12 00:00 shim.efi
-rwx------. 1 root root 1293149 Feb 12 00:00 shimx64.efi
[anaconda root@euleros2u5-uefi euleros]# rm -rf BOOTX64.EFI
[anaconda root@euleros2u5-uefi euleros]# cd ../BOOT/
[anaconda root@euleros2u5-uefi BOOT]# cp BOOTX64.EFI BOOTX64.EFI.bak
[anaconda root@euleros2u5-uefi BOOT]# cp ../euleros/grubx64.efi ./BOOTX64.EFI
[anaconda root@euleros2u5-uefi BOOT]# ls -l
total 2296
-rwx------. 1 root root 1053832 Aug  9 13:05 BOOTX64.EFI
-rwx------. 1 root root 1293149 Aug  9 13:05 BOOTX64.EFI.bak
[anaconda root@euleros2u5-uefi BOOT]# pwd
/mnt/sysimage/boot/efi/EFI/BOOT
[anaconda root@euleros2u5-uefi BOOT]#
```

The location of **grubx64.efi** varies depending on the OS. For details, see **Table 3-4**.

Table 3-4 Location of **grubx64.efi**

OS	grubx64.efi Location
CentOS	/boot/efi/EFI/centos/grubx64.efi
EulerOS	/boot/efi/EFI/euleros/grubx64.efi

OS	grubx64.efi Location
SUSE	/boot/efi/EFI/sles/grubx64.efi
Ubuntu	/boot/efi/EFI/ubuntu/grubx64.efi
Red Hat	/boot/efi/EFI/redhat/grubx64.efi

3.6 Configuring the VM Environment

3.6.1 Overview

This section describes how to configure the VM environment.

Prerequisites

- The host can connect to the Internet.
- You have logged in to the host using a remote desktop tool, such as VNC Viewer.
- The required installation packages have been uploaded to the host.

3.6.2 (Optional) Installing Basic Components

Scenario

This section is only necessary for Debian. For other OSs, skip this section. The basic components include vim, dkms, linux--headers-*xxx*-common, and linux-headers-*xxx*-amd64.

Procedure

1. Install vim.
   a. Configure the apt source.

      Run the **vi /etc/apt/sources.list** command to add the apt sources. The content to be added varies depending on the Debian OS version. The following uses Debian 8.6 as an example.

      ```
      deb http://mirrors.ustc.edu.cn/debian jessie main contrib non-free
      deb-src http://mirrors.ustc.edu.cn/debian jessie main contrib non-free
      deb http://mirrors.ustc.edu.cn/debian jessie-proposed-updates main contrib non-free
      deb-src http://mirrors.ustc.edu.cn/debian jessie-proposed-updates main contrib non-free
      deb http://mirrors.ustc.edu.cn/debian jessie-updates main contrib non-free
      deb-src http://mirrors.ustc.edu.cn/debian jessie-updates main contrib non-free
      ```

      Enter **:wq!** to save the file. Then, run the **apt update** command.

   b. Run the **apt-get install vim** command to install vim.
2. Run the **apt-get install dkms** command to install dkms.
3. Run the **apt-get install linux--headers-*xxx*-common** command to install **linux--headers-*xxx*-common**.

xxx indicates the kernel version number. For example, if the kernel version of Debain 8.6 is 3.16.0-4, run the **apt-get install linux--headers-3.16.0-4-common** command.

4. Run the **apt-get install linux-headers-*xxx*-amd64** command to install **linux-headers-*xxx*-amd64**.

   xxx indicates the kernel version number. For example, if the kernel version of Debain 8.6 is 3.16.0-4, run the **apt-get install linux-headers-3.16.0-4-amd64** command.

5. Delete configuration items from the **/etc/network/interfaces** file.

   Run the **vi /etc/network/interfaces** command. If the configuration of eth0 exists, delete the last two lines.

   ```
   ...
   # The loopback network interface
   auto lo
   iface lo inet loopback

   # The primary network interface
   # The following configuration items need to be deleted:
   allow-hotplug eth0
   iface eth0 inet dhcp
   ```

   Enter **:wq!** to save the file.

3.6.3 Configuring the Network

Scenario

Configure an available IP address for the VM to enable it to communicate with the host.

If the **ifconfig** and **route** are unavailable for SUSE 15, use the **zypper install net-tools-deprecated** to install the tools.

Procedure

1. On the VM, run the following command to query the NIC name:

   ifconfig -a

2. Run the following command to check whether the NIC has obtained an IP address:

   ifconfig

   If the following information is displayed, the NIC has obtained an IP address (*xxx* indicates the obtained IP address, and *XX* indicates the MAC address):

   ```
   eth0     Link encap:Ethernet  HWaddr XX:XX:XX:XX:XX:XX
   inet addr:xxx.xxx.xxx.xxx  Bcast:xxx.xxx.x.xxx Mask:xxx.xxx.xxx.xxx
   ```

3. If the NIC has not obtained an IP address, run the following command to enable the NIC to dynamically obtain an IP address:

   ifup *NIC name*

   Example:

   ifup eth0

   The following information is displayed:

   ```
   Determining IP information for eth0... done
   ```

If a message is displayed indicating that the **ifup** command failed, run the following commands:

ip link set *NIC name* **up**

dhclient *NIC name*

You can also run the following command:

ifconfig eth0 up

Generally, no information is displayed.

3.6.4 Configuring systemd Timeout Parameters

Scenario

Configure time parameters to prevent BMS provisioning timeout.

Procedure

For Red Hat 7, EulerOS, CentOS 7, CentOS 8, Oracle Linux 7, Ubuntu 16.04, Ubuntu 18.04, SUSE 12 SP2, SUSE 12 SP3, SUSE 15, and Debian, run the following command:

vi /etc/systemd/system.conf

Delete the comment tags (#) before **DefaultTimeoutStartSec** and **DefaultTimeoutStopSec**, and change their values to **300s**.

```
#TimeSlackNSec=
#DefaultTimerAccuracySec=1min
#DefaultStandardOutput=journal
#DefaultStandardError=inherit
DefaultTimeoutStartSec=300s
DefaultTimeoutStopSec=300s
#DefaultRestartSec=100ms
#DefaultStartLimitInterval=10s
#DefaultStartLimitBurst=5
#DefaultEnvironment=
#DefaultCPUAccounting=no
#DefaultBlockIOAccounting=no
```

3.6.5 Disabling the Firewall

Scenario

Disable the firewall on the VM. The firewall prevents the remote login in SSH mode.

Procedure

- For Red Hat 7.0, Red Hat 7.2, Red Hat 7.3, Red Hat 7.4, Oracle Linux 7, EulerOS, CentOS 7, CentOS 8, or SUSE15, run the following commands:

  systemctl disable firewalld.service

  systemctl stop firewalld.service

  Run the **systemctl status firewalld.service** command to check the firewall status.

- For Red Hat 6.7, Red Hat 6.8, Red Hat 6.9, CentOS 6.8, CentOS 6.9, Oracle Linux 6.8, or Oracle Linux 6.9, run the following commands:

  chkconfig iptables off

  service iptables stop

  Run the **service iptables status** command to check the firewall status.

  ```
  [root@localhost ~]# service iptables status
  iptables: Firewall is not running.
  ```

- For SUSE 12, run the following commands:

  systemctl disable SuSEfirewall2.service

  systemctl stop SuSEfirewall2.service

  Run the **service SuSEfirewall2 status** command to check the firewall status.

- For SUSE 11, run the following command:

  rcSuSEfirewall2 stop

  Then, run the following command:

  a. **yast**

  b. Choose **Security and Users** > **Firewall** > **Disable Firewall Automatic Starting**.

  c. Check whether automatic firewall starting is disabled.

     ▪ If yes, click **Cancel** and then **Quit**.

     ▪ If no, click **Next**, **Finish**, and then **Quit**.

- For Ubuntu 18.04, Ubuntu 16.04, Ubuntu 14.04, or Debian, run the following command:

  ufw disable

  If **ufw** is unavailable, download it from the official website (for example, **https://packages.ubuntu.com/**) and install it.

  The .deb installation package is as follows (the version number is for reference only):

  ufw_0.35-0ubuntu2_all.deb

  Alternatively, after configuring apt sources in **SUSE/Red Hat/CentOS/Oracle Linux/Ubuntu/Debian**, run the **apt-get install ufw** command to install it and then run the **ufw disable** command to disable the firewall.

3.6.6 (Optional) Upgrading Wicked Components

Scenario

For SUSE 12 SP1, you need to upgrade wicked components. For other OSs, skip this section.

Procedure

1. Run the **rpm -ivh --nodeps --force *rpm** command to forcibly install wicked.
2. Run the following command to query all the installed wicked components:

   ```
   linux-locc:/home/fsp/Desktop # rpm -qa | grep wick
   wicked-service-0.6.28-1.1.x86_64
   libwicked-0-6-0.6.28-1.1.x86_64
   ```

```
libwicked-0-6-0.6.40-28.6.1.x86_64
wicked-0.6.28-1.1.x86_64
wicked-service-0.6.40-28.6.1.x86_64
wicked-0.6.40-28.6.1.x86_64
```

3. Uninstall the old wicked.

```
linux-locc:/home/fsp/Desktop # rpm -e wicked-service-0.6.28-1.1.x86_64
linux-locc:/home/fsp/Desktop # rpm -e libwicked-0-6-0.6.28-1.1.x86_64
linux-locc:/home/fsp/Desktop # rpm -e wicked-0.6.28-1.1.x86_64
```

3.6.7 (Optional) Disabling NetworkManager

Scenario

A centralized BMS uses NetworkManager for network management. This tool needs to be disabled because it may conflict with the **network-config** configuration. For a distributed BMS, skip this section.

NOTE

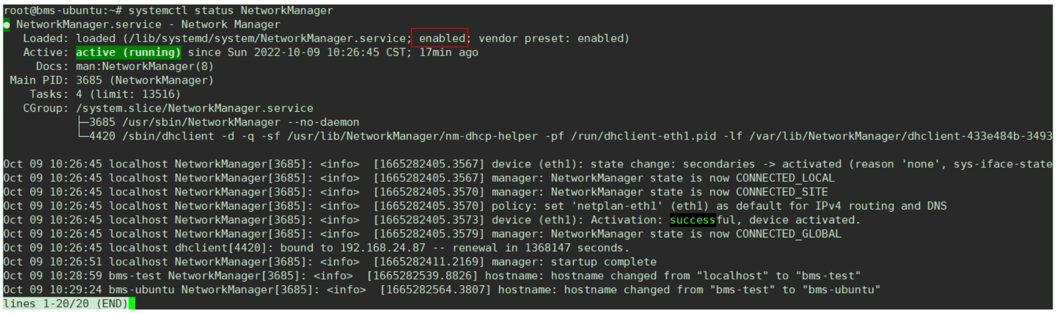
For SUSE 11 SP4, Ubuntu 16.04, and Ubuntu 14.04, skip this section. For BMSs with SDI 3.0 or 2.2 NIC cards, skip this section because NetworkManager is used for network management.

Note:

If NetworkManager is used for network management, you need to perform the following operations (only for Ubuntu):

Take Ubuntu 1804.2 as an example.

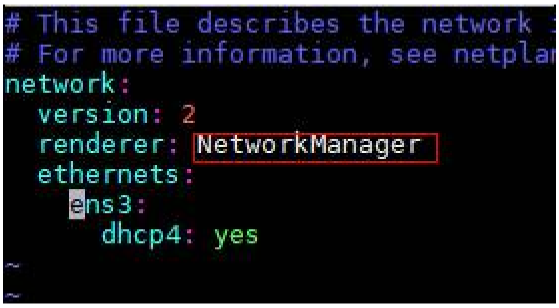
1. Run the **systemctl status NetworkManager** command to check whether the service is set to automatically start upon system startup.



```
root@bms-ubuntu:~# systemctl status NetworkManager
● NetworkManager.service - Network Manager
   Loaded: loaded (/lib/systemd/system/NetworkManager.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2022-10-09 10:26:45 CST; 17min ago
     Docs: man:NetworkManager(8)
 Main PID: 3685 (NetworkManager)
    Tasks: 4 (limit: 13516)
   CGroup: /system.slice/NetworkManager.service
           ├─3685 /usr/sbin/NetworkManager --no-daemon
           └─4420 /sbin/dhclient -d -q -sf /usr/lib/NetworkManager/nm-dhcp-helper -pf /run/dhclient-eth1.pid -lf /var/lib/NetworkManager/dhclient-433e484b-3493

Oct 09 10:26:45 localhost NetworkManager[3685]: <info>  [1665282405.3567] device (eth1): state change: secondaries -> activated (reason 'none', sys-iface-state
Oct 09 10:26:45 localhost NetworkManager[3685]: <info>  [1665282405.3567] manager: NetworkManager state is now CONNECTED_LOCAL
Oct 09 10:26:45 localhost NetworkManager[3685]: <info>  [1665282405.3570] manager: NetworkManager state is now CONNECTED_SITE
Oct 09 10:26:45 localhost NetworkManager[3685]: <info>  [1665282405.3570] policy: set 'netplan-eth1' (eth1) as default for IPv4 routing and DNS
Oct 09 10:26:45 localhost NetworkManager[3685]: <info>  [1665282405.3573] device (eth1): Activation: successful, device activated.
Oct 09 10:26:45 localhost NetworkManager[3685]: <info>  [1665282405.3579] manager: NetworkManager state is now CONNECTED_GLOBAL
Oct 09 10:26:45 localhost dhclient[4420]: bound to 192.168.24.87 -- renewal in 1368147 seconds.
Oct 09 10:26:51 localhost NetworkManager[3685]: <info>  [1665282411.2169] manager: startup complete
Oct 09 10:28:59 bms-test NetworkManager[3685]: <info>  [1665282539.8826] hostname: hostname changed from "localhost" to "bms-test"
Oct 09 10:29:24 bms-ubuntu NetworkManager[3685]: <info>  [1665282564.3807] hostname: hostname changed from "bms-test" to "bms-ubuntu"
lines 1-20/20 (END)
```

If the service does not exist, run the **apt-get install network-manager command** to install it.

2. Add the network management service and NIC information to the **/etc/netplan/01*yaml** file.



```
# This file describes the network
# For more information, see netpla
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      dhcp4: yes
~
~
```

Enter **:wq!**. Then, run the **netplan try** command to update the network configuration.

Procedure

- For Red Hat 7, Oracle Linux 7, Debian, EulerOS, CentOS 7, or CentOS 8, run the following commands:

  systemctl disable NetworkManager.service

  systemctl stop NetworkManager.service

  Run the **service NetworkManager.service status** command to check the NetworkManager status.

  ```
  [root@localhost ~]# service NetworkManager.service status
  edirecting to /bin/systemctl status NetworkManager.service
   NetworkManager.service - Network Manager
    Loaded: loaded (/usr/lib/systemd/system/NetworkManager.service disabled; vendor preset: enabled)
    Active: inactive (dead) since Mon 2017-11-13 19:06:18 CST; 1 min 17s ago
  ```

  For EulerOS, you also need to disable the following services:

  systemctl disable euleros-security

  systemctl disable NetworkManager-wait-online

- For Red Hat 6.7/Red Hat 6.8/Red Hat 6.9/CentOS 6.8/CentOS 6.9/Oracle Linux 6.8/Oracle Linux 6.9, run the following commands:

  NOTE

  For Red Hat 6.7/Red Hat 6.8/Red Hat 6.9/CentOS 6.8/CentOS 6.9/Oracle Linux 6.8/Oracle Linux 6.9, if you choose **Server with GUI** when creating a VM, you need to disable NetworkManager; if you choose **Minimal Install**, you do not need to disable NetworkManager.

  service NetworkManager stop

  chkconfig NetworkManager off

- For SUSE 12, run the following commands:

  systemctl disable wicked

  systemctl stop wicked

- For Ubuntu18.04, run the following commands:

  apt-get install ifupdown --> Install ifupdown.

  apt-get install ifenslave --> Install ifenslave for bond management.

  apt-get --assume-yes purge nplan netplan.io --> Uninstall Netplan.

3.6.8 (Optional) Deleting the Network Management Tool Plug-in

NOTE

A distributed BMS image uses the NetworkManager provided by the OS, you need to delete the **NetworkManager-config-server** plug-in from the VM. Otherwise, the NIC cannot automatically obtain an IP address. For a centralized BMS, skip this section because it does not use NetworkManager.

Run the **rpm -qa | grep NetworkManager-config-server** command to query whether the plug-in exists. If yes, run the **rpm -e NetworkManager-config-server** command to delete it.

3.6.9 (Optional) Deleting the Local User

Scenario

A local user is created during the VM creation. If you do not need it any longer, delete it.

Procedure

Run the **userdel -rf** *xxx* command.

xxx indicates the name of the local user. If no folder of this user exists in the **/home** directory, the user is deleted successfully.

NOTE

If the local user fails to be deleted, restart the VM, log in to the VM as user **root**, and run the **userdel -rf** *xxx* command again.

3.6.10 (Optional) Modifying DHCP Configuration Items

Scenario

This section is only necessary for SUSE. For other OSs, skip it.

Procedure

1. In the VM OS, enter the (CLI) mode and run the **su root** command to switch to user **root**.
2. Run the **vi /etc/sysconfig/network/dhcp** command to open the configuration file.
3. Enter **?DHCLIENT_PRIMARY_DEVICE** to locate the configuration item to be modified.

   Press **i** to enter the editing mode, and set the value of the configuration item to **yes** so that the system obtains the default gateway using DHCP.

   Press **Esc** to exit the editing mode.

   NOTE

   If **DHCLIENT_PRIMARY_DEVICE** does not exist in the configuration file, skip this step.
4. Enter **?DHCLIENT_SET_HOSTNAME** to locate the configuration item to be modified.

   Press **i** to enter the editing mode, and set the value of the configuration item to **no** so that the host name will not be changed when DHCP is used.

   Press **Esc** to exit the editing mode.
5. Enter **?DHCLIENT_USE_LAST_LEASE** to locate the configuration item to be modified.

   Press **i** to enter the editing mode, and set the value of the configuration item to **no** so that the fallback to the last lease is disabled.

   Press **Esc** to exit the editing mode.

6. Enter **?DHCLIENT6_MODE** to locate the configuration item to be modified.

   Press **i** to enter the editing mode and set the value of the configuration item to **managed**.

   Press **Esc** to exit the editing mode.

7. Enter **:wq** to save your settings and exit.

3.6.11 (Optional) Configuring the GRUB Timeout

Scenario

For Ubuntu 14.04 or Debian, you need to set the GRUB timeout to prevent system login failures caused by unexpected power-off. For other OSs, skip this section.

Procedure

1. Use the vi editor to open the **/etc/default/grub** file and appendix **GRUB_RECORDFAIL_TIMEOUT=10** to the **GRUB_CMDLINE_LINUX** field.

```
GRUB_DEFAULT=0
#GRUB_HIDDEN_TIMEOUT=0
GRUB_HIDDEN_TIMEOUT_QUIET=true
GRUB_TIMEOUT=2
GRUB_DISTRIBUTOR='lsb_release -i -s 2> /dev/null || echo Debian'
GRUB_CMDLINE_LINUX_DEFAULT=""
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0"
GRUB_RECORDFAIL_TIMEOUT=10
```

2. Run the following commands to update the configuration:

   grub-mkconfig -o /boot/grub/grub.cfg

3.6.12 Setting the Maximum Number of Handles to 65535.

- Generally, the default upper limit of handles on a Linux server is 1024. To check it, run the following command:

[root@platservice6~]# ulimit -n

1024

- For BMSs, you need to change the value to **65535**.

Run the **vim** command to edit the **/etc/systemd/system.conf** file as follows:

DefaultLimitNOFILE=65535

DefaultLimitNPROC=65535

NOTE

After the preceding operations are complete, you need to restart the VM. Otherwise, the number of handles does not take effect. After the restart, log in to the VM and check the maximum number of handles again.

3.6.13 Upload Required Software Packages

Scenario

Three methods are available for uploading required software packages.

Procedure

- Method 1: If the VM can communicate with the host, run the **scp** command to upload software packages to the VM. (This method is recommended. You can learn how to use the **scp** command by running **scp -help**.)

  For example, you can run the following command (the file name is an example only):

  scp fsp@*xxx.xxx.xxx.xxx***:/home/fsp/network-config-1.0-1.x86_64.rpm /home**

  The command indicates **scp** *Username***@***Host IP address*/*User-defined directory*/*File name*/*VM directory*.

- Method 2: If the VM can communicate with the host and you can log in to the VM using Xshell, use Xftp to transfer software packages to the VM.
- Method 3: If the VM cannot communicate with the host, use the virtual CD-ROM drive to mount software packages.

  Step 1: Create an ISO file on the host.

  Perform the following operations in the Linux terminal.

  – Run the **mkdir /root/software** command to create a directory.

  – Put **network-config** and the SDI driver package to the **software** directory.

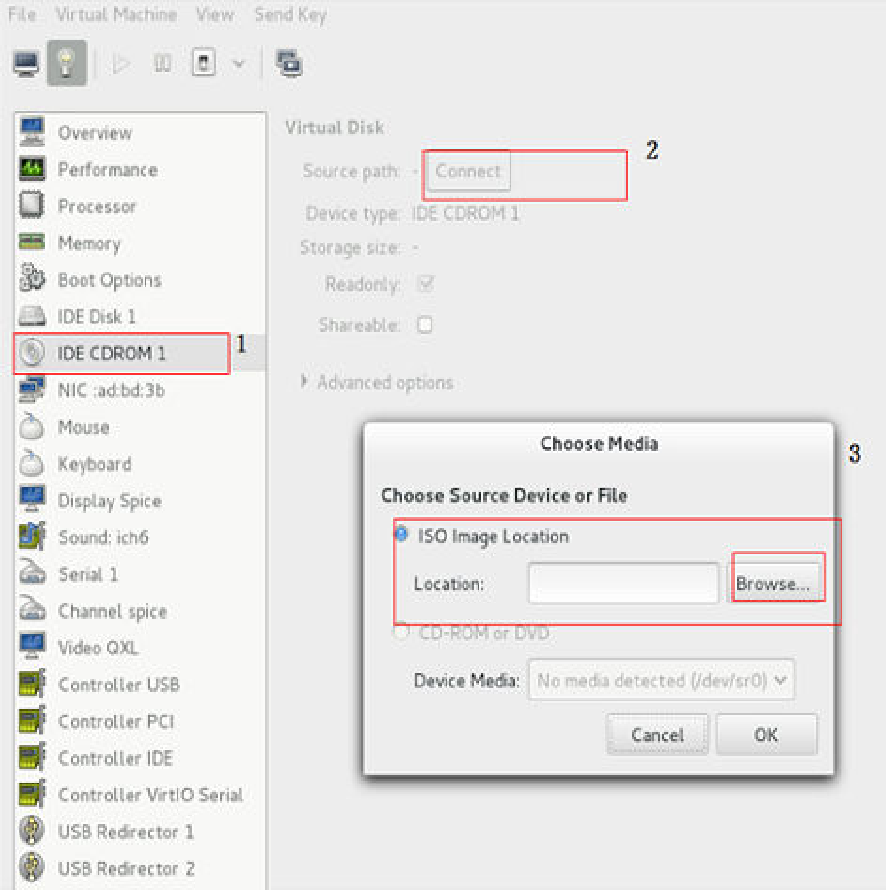
  – Run the **cd /root** command, and then run the **mkisofs -L -R -J -T -V system-sp2 -o defindsoftware.iso /root/software** command to create an ISO file.

  – Run the **ll** command. The **defindsoftware.iso** displayed in the command output is the created ISO file.

  Step 2: Use virt-manager to mount the ISO file.

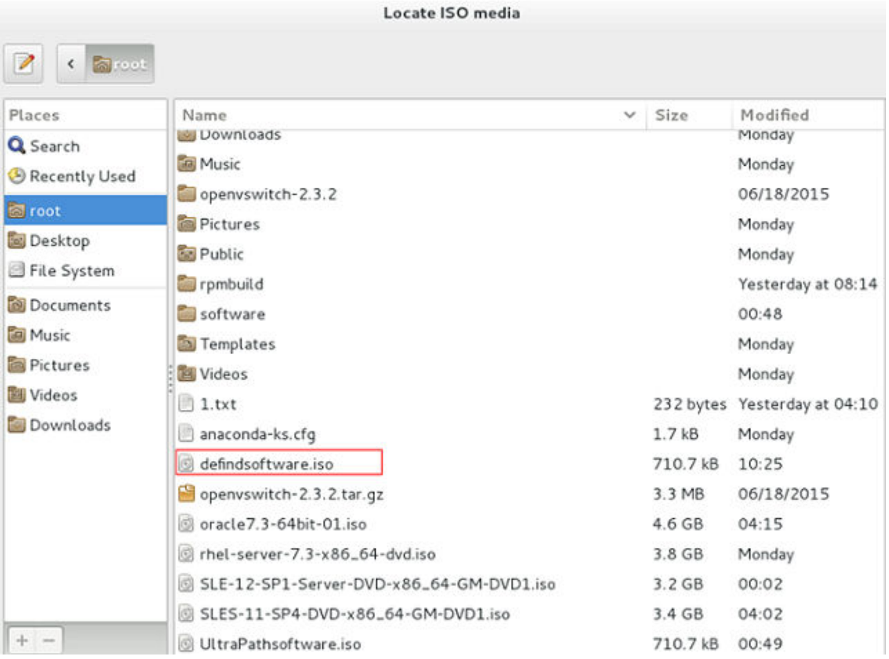
  a. On virt-manager, choose **View** > **Details**.

  b. In the navigation pane on the left, choose **IDE CDROM 1**. In the right pane, perform the operations specified in the following figure.



c. Click **Browse Local** and select the **/root** directory.

d. Locate and double-click the **defindsoftware.iso** file. In the displayed dialog box, click **OK**.



Name	Size	Modified
Downloads		Monday
Music		Monday
openvswitch-2.3.2		06/18/2015
Pictures		Monday
Public		Monday
rpmbuild		Yesterday at 08:14
software		00:48
Templates		Monday
Videos		Monday
1.txt	232 bytes	Yesterday at 04:10
anaconda-ks.cfg	1.7 kB	Monday
defindsoftware.iso	710.7 kB	10:25
openvswitch-2.3.2.tar.gz	3.3 MB	06/18/2015
oracle7.3-64bit-01.iso	4.6 GB	04:15
rhel-server-7.3-x86_64-dvd.iso	3.8 GB	Monday
SLE-12-SP1-Server-DVD-x86_64-GM-DVD1.iso	3.2 GB	00:02
SLES-11-SP4-DVD-x86_64-GM-DVD1.iso	3.4 GB	04:02
UltraPathsoftware.iso	710.7 kB	00:49

e. Choose **View** > **Console**, and select the VM.

f. After logging in to the VM, open the terminal and run **lsblk** to check whether the ISO file is mounted. For example, the ISO file can be mounted in the **/run/media/suse/system-sp2** directory.

g. Run the **cd /run/media/suse/system-sp2** command to copy the ISO file to a directory, for example, **/home**. If the ISO is not mounted, run the **mount /dev/sr0** */home* command to manually mount the ISO file to the **/home** directory. */home* is an example only.

3.7 Installing Cloud-Init

3.7.1 Overview

Scenario

Cloud-Init is a tool developed to initiate VMs or BMSs in the cloud environment. It is used to customize the network configuration, host name, hosts configuration file, username, and password when a user uses images to create VMs or BMSs. Cloud-Init is also required if the password of a VM created by using images is to be generated by the system at random.

In other case, Cloud-Init is not required. The Cloud-Init installation file has requirements on Linux versions and can only be installed from the Internet. Therefore, ensure that the VM can access the Internet.

Prerequisites

- You have logged in to the VM.
- The host can connect to the Internet.
- You have logged in to the host using VNC Viewer and installed an OS on the host using virt-manager.

Description

1. The Cloud-Init installation procedures in the following sections are for reference only. You are advised to download the Cloud-Init from the official website. The Cloud-init version is updated on the official website in real time. Install the latest version.
2. When you modify the **/etc/cloud/cloud.cfg** file, ensure that the file format (such as alignment and spaces) is consistent with the provided example that conforms to the yaml syntax.

3.7.2 SUSE/Red Hat/CentOS/Oracle Linux/Ubuntu/Debian

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 Compiled Source Code**.

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

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

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

- SUSE Linux

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

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

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

  NOTE

  Select the required repo installation package in the provided paths.

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

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

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

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

     zypper refresh

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

     zypper install cloud-init

  d. 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

NOTICE

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

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

   vi etc/sysconfig/network/dhcp

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

- CentOS

  Table 3-5 lists the Cloud-Init installation paths for CentOS. Select an address from the following table and download the EPEL release package.

Table 3-5 Cloud-Init installation package addresses

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

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

yum install https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/Packages/e/epel-release-*xx-xx***.noarch.rpm**

yum install cloud-init

NOTE

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

- Debian

  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 official website.

  Run the following commands to install Cloud-Init:

  apt-get update

  apt-get install cloud-init

  After Cloud-Init is installed in the Debian OS, run the following commands to install the vlan and ifenslave services:

  apt-get install vlan

  apt-get install ifenslave

- 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 Ubuntu official website.

  Run the following commands to install Cloud-Init:

  apt-get update

  apt-get install cloud-init

  After Cloud-Init is installed in the Ubuntu OS, perform the following operations to install tools and services:

  a. Install the SSH service.

     For x86, run the following commands:

     apt-get install openssh-client

     apt-get install openssh-server

     For ARM64, run the following commands:

     apt install openssh-client

     apt install openssh-server

  b. Install dkms.

     To ensure that SDI drivers can run properly, you need to install dkms for Ubuntu.

     Run the following command to install the tool:

     apt-get install dkms

     Then, run the following command:

     vi /usr/sbin/dkms

     Go to line 283 (press **shift** and **:** to enter the CLI mode. Then, type **283** and press **Enter**) and modify this line as follows:

     ```
     invoke_command "$mkinitrd -f $initrd_dir/$initrd $1" "$mkinitrd" background
     ```

  c. Install the vlan and ifenslave services.

     apt-get install vlan

     apt-get install ifenslave

  d. Install the ifupdown service.

     apt-get install ifupdown

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

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

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

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

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

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

   NOTE

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

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

   NOTE

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

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

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

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

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

   ```
   cloud-init 0.7.9
   ```

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

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

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

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

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

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

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

NOTICE

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 Compiled Source Code

The Cloud-Init configuration has been compiled in the source code. Therefore, you do not need to configure Cloud-Init after the installation. 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 Cloud-Init 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

   wget https://github.com/canonical/cloud-init/archive/refs/tags/0.7.9.zip

   mkdir /tmp/CLOUD-INIT

   cp cloud-init-0.7.9.zip /tmp/CLOUD-INIT

   cd /tmp/CLOUD-INIT

2. Run the following command to decompress the package:

   unzip cloud-init-0.7.9.zip

3. Run the following command to enter the **cloud-init-0.7.9** directory:

   cd cloud-init-0.7.9

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

     python setup.py build

     python setup.py install --init-system sysvinit

   - For CentOS 7.*x*, SUSE 12.*x*, or EulerOS 2.8 ARM, run the following commands:

     python setup.py build

     python setup.py install --init-system systemd

   NOTICE

   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

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

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

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

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

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

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

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

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

   cloud-init -v

   cloud-init init --local

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

```
cloud-init 0.7.9
```

3.7.3 EulerOS/OpenEuler

1. Use EulerOS2.2 as an example. Configure the yum source of EulerOS2.2 by editing the **/etc/yum.repos.d/EulerOS-base.repo** file. For example, the configuration is:

```
[EulerOS-base]
name=EulerOS-base
baseurl=https://repo.huaweicloud.com/euler/2.2/os/x86_64/
enabled=1
gpgcheck=1
gpgkey=https://repo.huaweicloud.com/euler/2.2/os/RPM-GPG-KEY-EulerOS
```

   Save the configuration.

2. Run the following command to update the yum source:

   yum repolist

   Run the following command to install Cloud-Init 0.7.6:

   yum install cloud-init

   Dependent packages of Cloud-Init 0.7.6 will be installed automatically.

```
Installed:
  cloud-init.x86_64 0:0.7.6-2

Dependency Installed:
  PyYAML.x86_64 0:3.10-11                                audit-libs-python.x86_64 0:2.4.1-5
  checkpolicy.x86_64 0:2.1.12-6                          libsemanage-python.x86_64 0:2.1.10-18
  libyaml.x86_64 0:0.1.4-11                              policycoreutils-python.x86_64 0:2.2.5-15.h1
  python-IPy.noarch 0:0.75-6                             python-backports.x86_64 0:1.0-8
  python-backports-ssl_match_hostname.noarch 0:3.4.0.2-4        python-jsonpatch.noarch 0:1.2-2
  python-jsonpointer.noarch 0:1.9-2                      python-prettytable.noarch 0:0.7.2-1
  python-requests.noarch 0:2.6.0-1                       python-six.noarch 0:1.9.0-2
  python-urllib3.noarch 0:1.10.2-2                       setools-libs.x86_64 0:3.3.7-46

Complete!
```

3. To inject the password of user **root**, run the following command to upgrade **selinux-policy** from h1 to h2.

   yum install selinux-policy

4. Run the **cloud-init -v** command. If the command output contains the Cloud-Init version number, the installation is complete.

3.8 Configuring Cloud-Init

After installing Cloud-Init, you need to configure it.

Use the vi editor to modify the **/etc/cloud/cloud.cfg** file. The following sections are for reference only. You can modify the file as you need.

3.8.1 Cloud-Init 0.7.5

1. Add the following key-value pair with an empty line above and below it:
```
no_ssh_fingerprints: true
```
2. Set **ssh_pwauth** to **false**. This parameter specifies whether to enable password login in SSH mode.
```
ssh_pwauth: false
```
3. Add **preserve_hostname: false**.
```
preserve_hostname: false
```
4. Use the number sign (#) to comment out the following statements:
```
mount_default_fields: [~, ~, 'auto', 'defaults,nofail', '0', '2']
resize_rootfs_tmp: /dev
ssh_deletekeys:   0
```
5. Modify **ssh_genkeytypes** as follows:
```
ssh_genkeytypes: ['rsa', 'dsa']
```
6. Modify **syslog_fix_perms** as follows:
```
syslog_fix_perms: root:root
```
7. Add the following statements:
```
network:
  config: disabled
datasource_list: [ OpenStack ]
```

NOTICE

For Ubuntu 14.04, the following line does not need to be added:
```
datasource_list: [ OpenStack ]
```

8. Add the following statement after **- final-message** in **cloud_final_modules**:
```
- power-state-change
```
9. Check and modify the information in **system info** to make it consistent with the following content:
```
system_info:
  default_user:
    name: linux  //Username for OS login
    lock_passwd: True   //True indicates that login using a password is disabled. Note that some OSs use value 1 to disable the password login.
   gecos: redhat
   groups: [audio, cdrom, dialout, floppy]   // (optional) Add the user to other groups that have been configured in etc/group.
    sudo: ["ALL=(ALL) NOPASSWD:ALL"]  //Current user has all the root rights.
    shell: /bin/bash   //Execute shell in bash mode.
  distro: sles
   paths:
    cloud_dir: /var/lib/cloud/
    templates_dir: /etc/cloud/templates/
    upstart_dir: /etc/init/
   ssh_svcname: sshd
```

In the preceding command, change the value of **distro** based on the OS, such as **distro: sles**, **distro: rhel**, **distro: ubuntu**, **distro: debian**, and **dustro: fedora**.

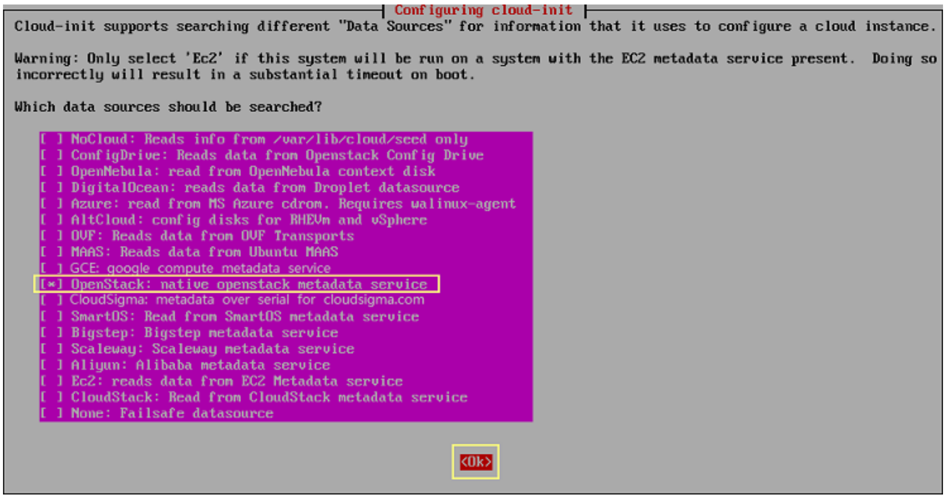
10. (Optional) For Ubuntu 14.04, perform the following operations:

    a. Use the vi editor to open the **/etc/init/cloud-init-local.conf** configuration file and modify the following configuration items:

    ```
    # cloud-init - the initial cloud-init job
    #   crawls metadata service, emits cloud-config
    start on mounted MOUNTPOINT=/ and mounted MOUNTPOINT=/run and stopped bms-network_config
    ```

    b. Run the following commands to configure the OpenStack source:

    dpkg-reconfigure cloud-init



```
                            ┤ Configuring cloud-init ├
Cloud-init supports searching different "Data Sources" for information that it uses to configure a cloud instance.

Warning: Only select 'Ec2' if this system will be run on a system with the EC2 metadata service present.  Doing so
incorrectly will result in a substantial timeout on boot.

Which data sources should be searched?

   [ ] NoCloud: Reads info from /var/lib/cloud/seed only
   [ ] ConfigDrive: Reads data from Openstack Config Drive
   [ ] OpenNebula: read from OpenNebula context disk
   [ ] DigitalOcean: reads data from Droplet datasource
   [ ] Azure: read from MS Azure cdrom. Requires walinux-agent
   [ ] AltCloud: config disks for RHEVm and vSphere
   [ ] OVF: Reads data from OVF Transports
   [ ] MAAS: Reads data from Ubuntu MAAS
   [ ] GCE: google compute metadata service
   [*] OpenStack: native openstack metadata service
   [ ] CloudSigma: metadata over serial for cloudsigma.com
   [ ] SmartOS: Read from SmartOS metadata service
   [ ] Bigstep: Bigstep metadata service
   [ ] Scaleway: Scaleway metadata service
   [ ] Aliyun: Alibaba metadata service
   [ ] Ec2: reads data from EC2 Metadata service
   [ ] CloudStack: Read from CloudStack metadata service
   [ ] None: Failsafe datasource

                                        <Ok>
```

Run the **vim /etc/cloud/cloud.cfg.d/90_dpkg.cfg** command to open the configuration file and check whether the items are correctly configured in the file.

```
# to update this file, run dpkg-reconfigure cloud-init
datasource_list: [ OpenStack ]
~
~
~
```

If the configuration file content is consistent with the preceding command output, the configuration is successful.

3.8.2 Cloud-Init 0.7.6

1. Add the following key-value pair with an empty line above and below it:

   ```
   no_ssh_fingerprints: true
   ```

2. set **users** to **default**.

   ```
   users:
       - default
   ```

3. Modify the following fields:

   ```
   disable_root: True
   preserve_hostname: false
   syslog_fix_perms: root:root
   ```

4. Configure **ssh_pwauth**. This parameter specifies whether to enable password login in SSH mode.

   ```
   ssh_pwauth: false
   ```

5. Use the number sign (#) to comment out the following statements:

```
mount_default_fields: [~, ~, 'auto', 'defaults', '0', '2']
manual_cache_clean: true
```

6. Add **network** statements.

```
network:
  config: disabled
datasource_list: [ OpenStack ]
```

For SUSE 11 SP4, you also need to add **growpart** statements.

```
growpart:
  mode: false
```

NOTICE

For Debian 8.6, the following line does not need to be added:

```
datasource_list: [ OpenStack ]
```

7. Add the following statement after **- final-message** in **cloud_final_modules**:

```
- power-state-change
```

8. Check and modify the information in **system info** to make it consistent with the following content:

```
system_info:
   distro: sles
   default_user:
      name: linux  //Username for OS login
      lock_passwd: True   //True indicates that login using a password is disabled. Note that some OSs
use value 1 to disable the password login.
     gecos: redhat
groups: [adm, audio, cdrom, dialout, dip, floppy, lxd, netdev, plugdev, sudo, video]   // (Optional) Add
the user to other groups that have been configured in etc/group.
      sudo: ["ALL=(ALL) NOPASSWD:ALL"]  //Current user has all the root rights.
      shell: /bin/bash   //Execute shell in bash mode.
    paths:
      cloud_dir: /var/lib/cloud/
      templates_dir: /etc/cloud/templates/
    ssh_svcname: sshd
```

In the preceding command, change the value of **distro** based on the OS, such as **distro: sles**, **distro: rhel**, **distro: ubuntu**, **distro: debian**, and **dustro: fedora**.

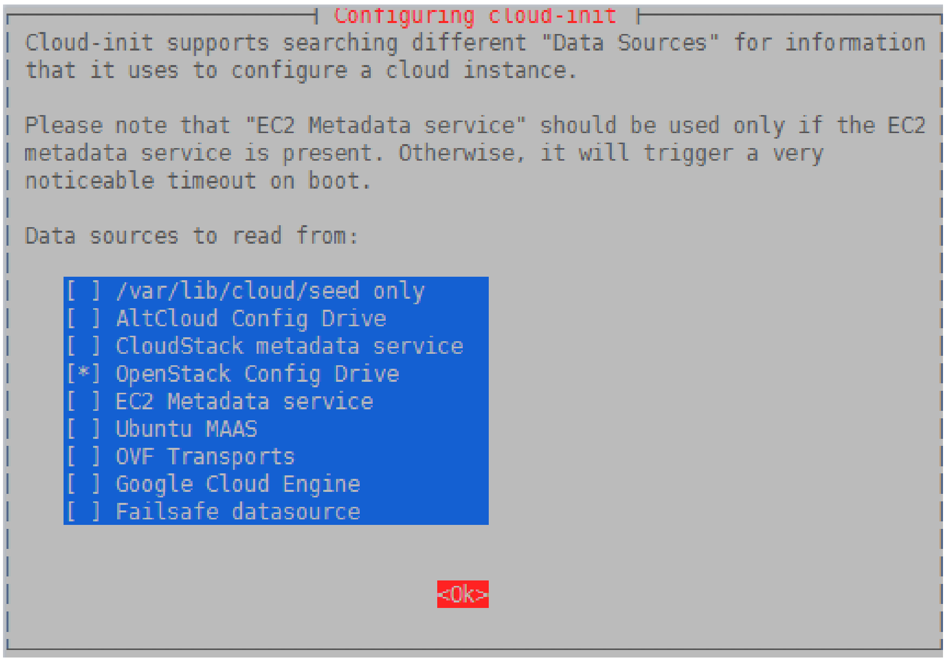
9. Use the number sign (#) to comment out the following statement:

```
ssh_genkeytypes: ['rsa', 'dsa']
```

10. (Optional) For Debian 8.6, perform the following operations:

    a. Run the following commands to configure the OpenStack source:

       dpkg-reconf igure cloud-init



```
Configuring cloud-init
Cloud-init supports searching different "Data Sources" for information
that it uses to configure a cloud instance.

Please note that "EC2 Metadata service" should be used only if the EC2
metadata service is present. Otherwise, it will trigger a very
noticeable timeout on boot.

Data sources to read from:

    [ ] /var/lib/cloud/seed only
    [ ] AltCloud Config Drive
    [ ] CloudStack metadata service
    [*] OpenStack Config Drive
    [ ] EC2 Metadata service
    [ ] Ubuntu MAAS
    [ ] OVF Transports
    [ ] Google Cloud Engine
    [ ] Failsafe datasource


                                   <Ok>
```

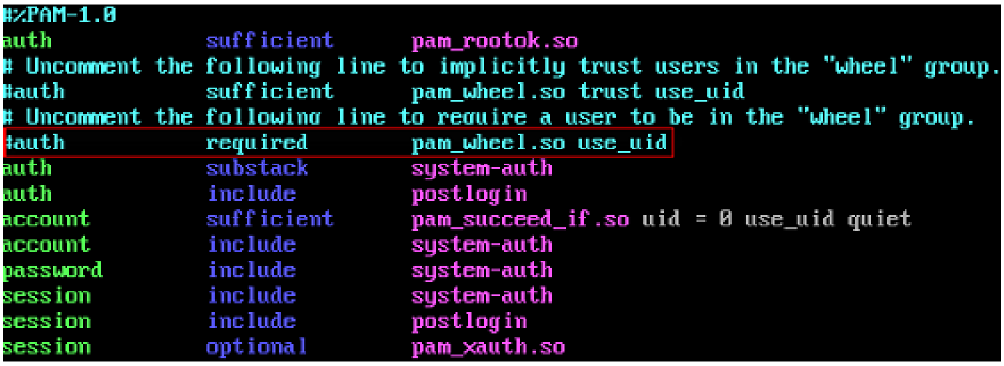
Run the **vim /etc/cloud/cloud.cfg.d/90_dpkg.cfg** command to open the configuration file and check whether the items are correctly configured in the file.

```
# to update this file, run dpkg-reconf igure cloud-init
datasource_list: [ OpenStack ]
~
~
~
```

If the configuration file content is consistent with the preceding command output, the configuration is successful.

11. (Optional) For EulerOS 2.2 and EulerOS 2.3, perform the following operations:

    Check whether the line shown in the following figure has been commented out using the number sign (#) in the **/etc/pam.d/su** configuration file. If the line has been commented out, skip this step.



```
#%PAM-1.0
auth            sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth           sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth           required        pam_wheel.so use_uid
auth            substack        system-auth
auth            include         postlogin
account         sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account         include         system-auth
password        include         system-auth
session         include         system-auth
session         include         postlogin
session         optional        pam_xauth.so
```

3.8.3 Cloud-Init 0.7.9 or later

1. Add the following key-value pair with an empty line above and below it:

```
no_ssh_fingerprints: true
```

2. Set **ssh_pwauth** to **false** or **0**, indicating that password login in SSH mode is disabled.

```
ssh_pwauth: false
```

3. Set **disable_root** to **false**. This parameter specifies whether to allow SSH login of user **root**.

```
disable_root: true
```

4. Add **preserve_hostname: false**.

```
preserve_hostname: false
```

5. (Optional) Use the number sign (#) to comment out the following statements (skip this step if the statements do not exist):

```
mount_default_fields: [~, ~, 'auto', 'defaults,nofail', '0', '2']
resize_rootfs_tmp: /dev
ssh_deletekeys:   0
```

6. Modify **ssh_genkeytypes** as follows (add it if it does not exist):

```
ssh_genkeytypes: ['rsa', 'dsa']
```

7. Modify **syslog_fix_perms** as follows (add it if it does not exist):

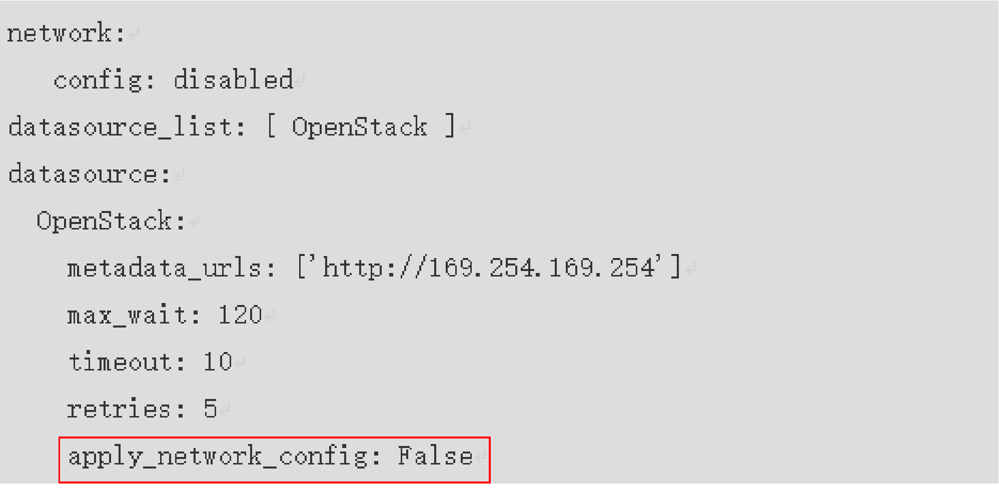
```
syslog_fix_perms: root:root
```

8. Add the following statements:

```
network:
   config: disabled
datasource_list: [ OpenStack ]
datasource:
  OpenStack:
    metadata_urls: ['http://169.254.169.254']
    max_wait: 120
    timeout: 10
    retries: 5
```

9. (Optional) In **/etc/cloud/cloud.cfg**, set **apply_network_config** to **False**.

   This step is only for Cloud-Init 18.3 or later.



```
network:
   config: disabled
datasource_list: [ OpenStack ]
datasource:
  OpenStack:
    metadata_urls: ['http://169.254.169.254']
    max_wait: 120
    timeout: 10
    retries: 5
    apply_network_config: False
```

10. Add the following content after **- final-message** in **cloud_final_modules**:

```
- power-state-change
```

11. Modify **system_info** as follows:

```
system_info:
   distro: rhel
   default_user:
      name: linux  //Username for OS login
      lock_passwd: True   //True indicates that login using a password is disabled. Note that some OSs
use value 1 to disable the password login.
```

   In the preceding command, change the value of **distro** based on the OS, such as **distro: sles**, **distro: rhel**, **distro: ubuntu**, **distro: debian**, and **dustro: fedora**.

12. (Optional) For SUSE 12 SP1 and SUSE 12 SP2, modify **[Unit]** in the **/usr/lib/systemd/system/cloud-init-local.service** file.

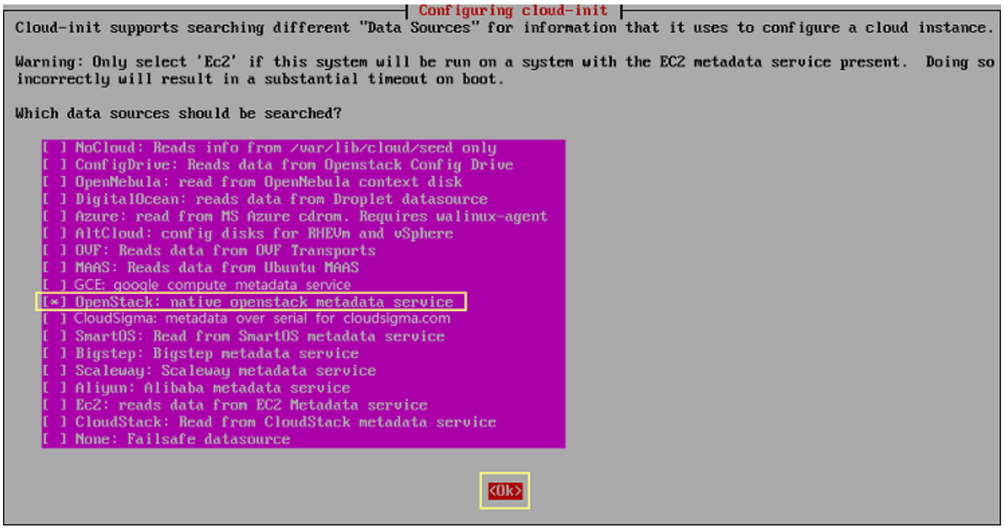
vi /usr/lib/systemd/system/cloud-init-local.service

Ensure that **[Unit]** is configured as follows:

```
[Unit]
Description=Initial cloud-init job (pre-networking)
DefaultDependencies=no
Wants=network-pre.target
Wants=local-fs.target
After=local-fs.target
Before=network-pre.target
Before=shutdown.target
Before=basic.target
Conflicts=shutdown.target
# Other distros use Before=sysinit.target. There is not a clearly identified
# reason for usage of basic.target instead.
```

13. (Optional) For Ubuntu 16.04, run the following command to configure the OpenStack source:

    dpkg-reconfigure cloud-init



```
Configuring cloud-init
Cloud-init supports searching different "Data Sources" for information that it uses to configure a cloud instance.

Warning: Only select 'Ec2' if this system will be run on a system with the EC2 metadata service present.  Doing so
incorrectly will result in a substantial timeout on boot.

Which data sources should be searched?

   [ ] NoCloud: Reads info from /var/lib/cloud/seed only
   [ ] ConfigDrive: Reads data from Openstack Config Drive
   [ ] OpenNebula: read from OpenNebula context disk
   [ ] DigitalOcean: reads data from Droplet datasource
   [ ] Azure: read from MS Azure cdrom. Requires walinux-agent
   [ ] AltCloud: config disks for RHEVm and vSphere
   [ ] OVF: Reads data from OVF Transports
   [ ] MAAS: Reads data from Ubuntu MAAS
   [ ] GCE: google compute metadata service
   [*] OpenStack: native openstack metadata service
   [ ] CloudSigma: metadata over serial for cloudsigma.com
   [ ] SmartOS: Read from SmartOS metadata service
   [ ] Bigstep: Bigstep metadata service
   [ ] Scaleway: Scaleway metadata service
   [ ] Aliyun: Alibaba metadata service
   [ ] Ec2: reads data from EC2 Metadata service
   [ ] CloudStack: Read from CloudStack metadata service
   [ ] None: Failsafe datasource

                                   <Ok>
```

Run the **vim /etc/cloud/cloud.cfg.d/90_dpkg.cfg** command to open the configuration file and check whether the items are correctly configured in the file.

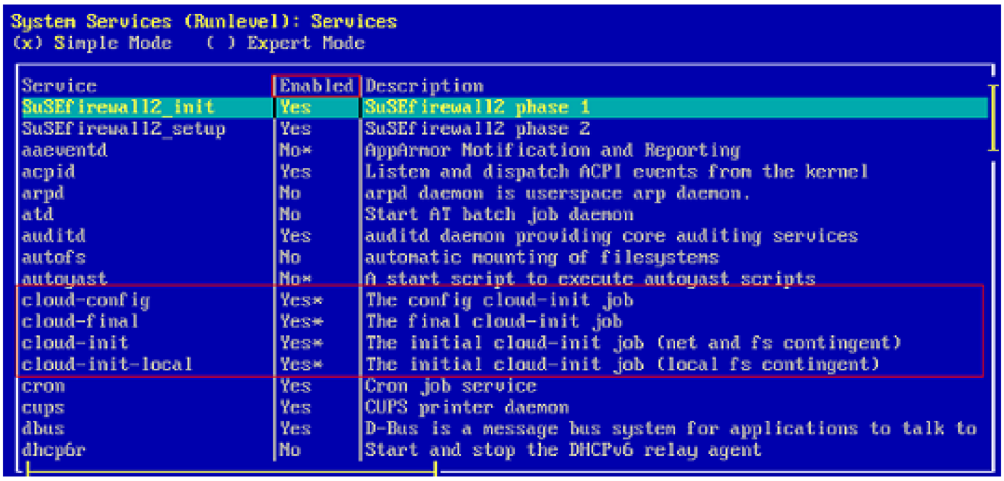
```
# to update this file, run dpkg-reconfigure cloud-init
datasource_list: [ OpenStack ]
~
~
~
```

If the configuration file content is consistent with the preceding command output, the configuration is successful.

3.9 Checking the Cloud-Init Status

3.9.1 SUSE 11 SP4

1. Run the **yast** command and select **System**.
2. Press **Tab** and select **Sytem Services (Runlevel)**.
3. Press **Enter**. The following figure indicates that automatic startup has been enabled for the four services of Cloud-Init. If it is not enabled for a service, enable it.

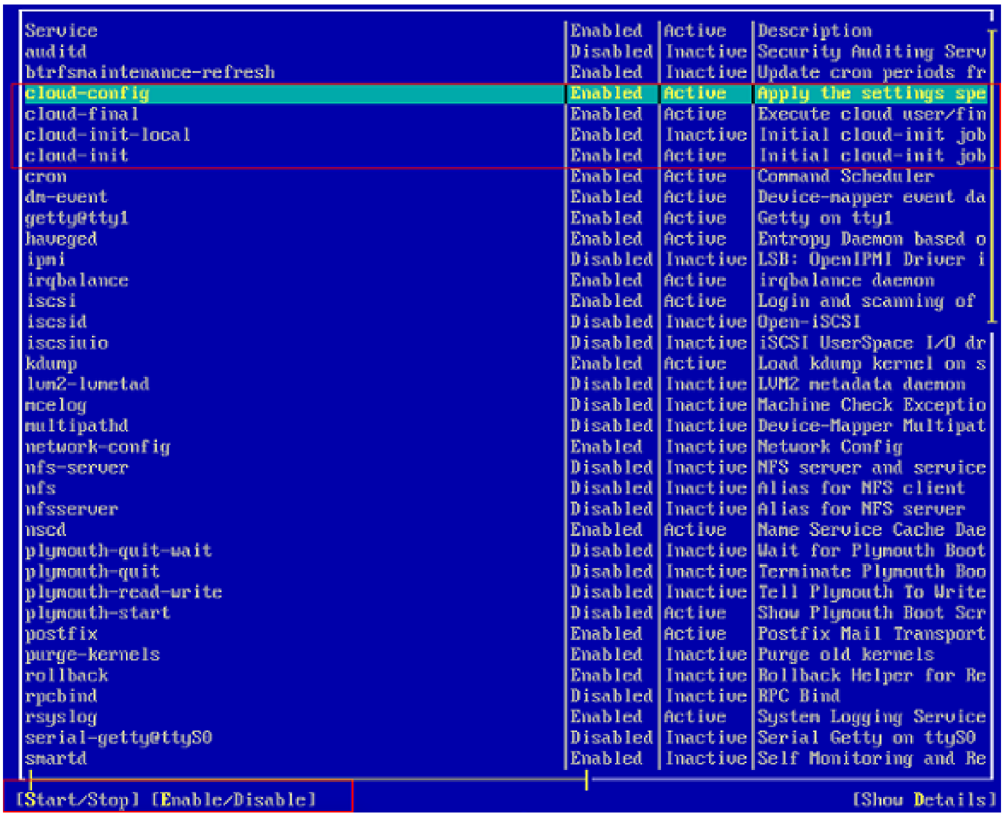


```
System Services (Runlevel): Services
(x) Simple Mode    ( ) Expert Mode

Service              Enabled Description
SuSEfirewall2_init   Yes     SuSEfirewall2 phase 1
SuSEfirewall2_setup  Yes     SuSEfirewall2 phase 2
aaeventd             No*     AppArmor Notification and Reporting
acpid                Yes     Listen and dispatch ACPI events from the kernel
arpd                 No      arpd daemon is userspace arp daemon.
atd                  No      Start AT batch job daemon
auditd               Yes     auditd daemon providing core auditing services
autofs               No      automatic mounting of filesystems
autoyast             No*     A start script to execute autoyast scripts
cloud-config         Yes*    The config cloud-init job
cloud-final          Yes*    The final cloud-init job
cloud-init           Yes*    The initial cloud-init job (net and fs contingent)
cloud-init-local     Yes*    The initial cloud-init job (local fs contingent)
cron                 Yes     Cron job service
cups                 Yes     CUPS printer daemon
dbus                 Yes     D-Bus is a message bus system for applications to talk to
dhcp6r               No      Start and stop the DHCPv6 relay agent
```

3.9.2 SUSE 12 SP1

1. Check whether the Cloud-init services will automatically start when the system starts.

   To query the Cloud-Init status, run the **yast** command and use up and down arrow keys to select **System**. Then, press **Tab** and use up and down arrow keys to select **System Manager**.



```
Service                    Enabled  Active   Description
auditd                     Disabled Inactive Security Auditing Serv
btrfsmaintenance-refresh   Enabled  Inactive Update cron periods fr
cloud-config               Enabled  Active   Apply the settings spe
cloud-final                Enabled  Active   Execute cloud user/fin
cloud-init-local           Enabled  Inactive Initial cloud-init job
cloud-init                 Enabled  Active   Initial cloud-init job
cron                       Enabled  Active   Command Scheduler
dm-event                   Enabled  Active   Device-mapper event da
getty@tty1                 Enabled  Active   Getty on tty1
haveged                    Enabled  Active   Entropy Daemon based o
ipmi                       Disabled Inactive LSB: OpenIPMI Driver i
irqbalance                 Enabled  Active   irqbalance daemon
iscsi                      Enabled  Active   Login and scanning of
iscsid                     Disabled Inactive Open-iSCSI
iscsiuio                   Disabled Inactive iSCSI UserSpace I/O dr
kdump                      Enabled  Active   Load kdump kernel on s
lvm2-lvmetad               Disabled Inactive LVM2 metadata daemon
mcelog                     Disabled Inactive Machine Check Exceptio
multipathd                 Disabled Inactive Device-Mapper Multipat
network-config             Enabled  Inactive Network Config
nfs-server                 Disabled Inactive NFS server and service
nfs                        Disabled Inactive Alias for NFS client
nfsserver                  Disabled Inactive Alias for NFS server
nscd                       Enabled  Active   Name Service Cache Dae
plymouth-quit-wait         Disabled Inactive Wait for Plymouth Boot
plymouth-quit              Disabled Inactive Terminate Plymouth Boo
plymouth-read-write        Disabled Inactive Tell Plymouth To Write
plymouth-start             Disabled Active   Show Plymouth Boot Scr
postfix                    Enabled  Active   Postfix Mail Transport
purge-kernels              Enabled  Inactive Purge old kernels
rollback                   Enabled  Inactive Rollback Helper for Re
rpcbind                    Disabled Inactive RPC Bind
rsyslog                    Enabled  Active   System Logging Service
serial-getty@ttyS0         Disabled Inactive Serial Getty on ttyS0
smartd                     Enabled  Inactive Self Monitoring and Re

[Start/Stop] [Enable/Disable]                          [Show Details]
```

2. As shown in the preceding figure, automatic startup has been enabled for the four services of Cloud-Init. **Active** indicates that the service has been started. If automatic startup is not enabled for a service, select the service using up and down arrow keys, press **Tab**, and use the **Enable/Disable** option to enable it.

3.9.3 SUSE 12 SP2/SUSE 12 SP3/SUSE 15/Oracle Linux 7/Red Hat 7/CentOS 7/CentOS 8

1. Check whether the Cloud-init services will automatically start when the system starts.

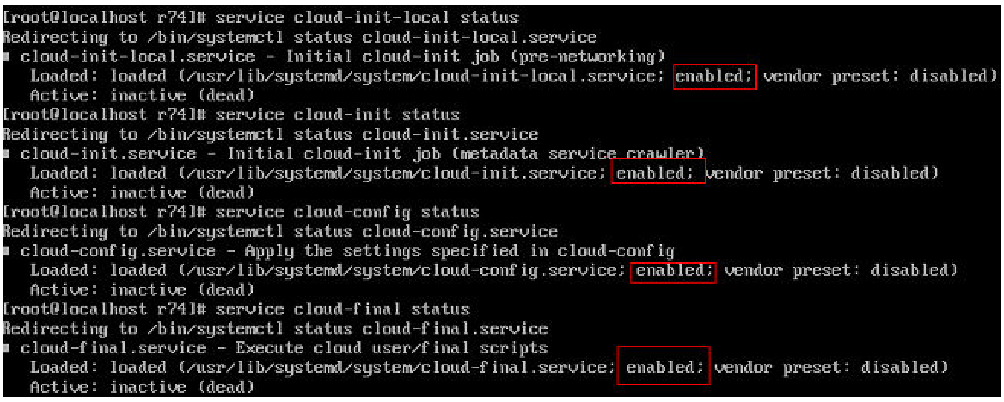
   systemctl status cloud-init-local

   systemctl status cloud-init

   systemctl status cloud-config

   systemctl status cloud-final

2. **enabled** indicates that the service will automatically start.

```
[root@localhost r74]# service cloud-init-local status
Redirecting to /bin/systemctl status cloud-init-local.service
● cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init-local.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost r74]# service cloud-init status
Redirecting to /bin/systemctl status cloud-init.service
● cloud-init.service - Initial cloud-init job (metadata service crawler)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost r74]# service cloud-config status
Redirecting to /bin/systemctl status cloud-config.service
● cloud-config.service - Apply the settings specified in cloud-config
   Loaded: loaded (/usr/lib/systemd/system/cloud-config.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost r74]# service cloud-final status
Redirecting to /bin/systemctl status cloud-final.service
● cloud-final.service - Execute cloud user/final scripts
   Loaded: loaded (/usr/lib/systemd/system/cloud-final.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
```

   Otherwise, run the following commands to enable automatic startup for them.

   systemctl enable cloud-init-local

   systemctl enable cloud-init

   systemctl enable cloud-config

   systemctl enable cloud-final

3. Run the following commands to start Cloud-Init:

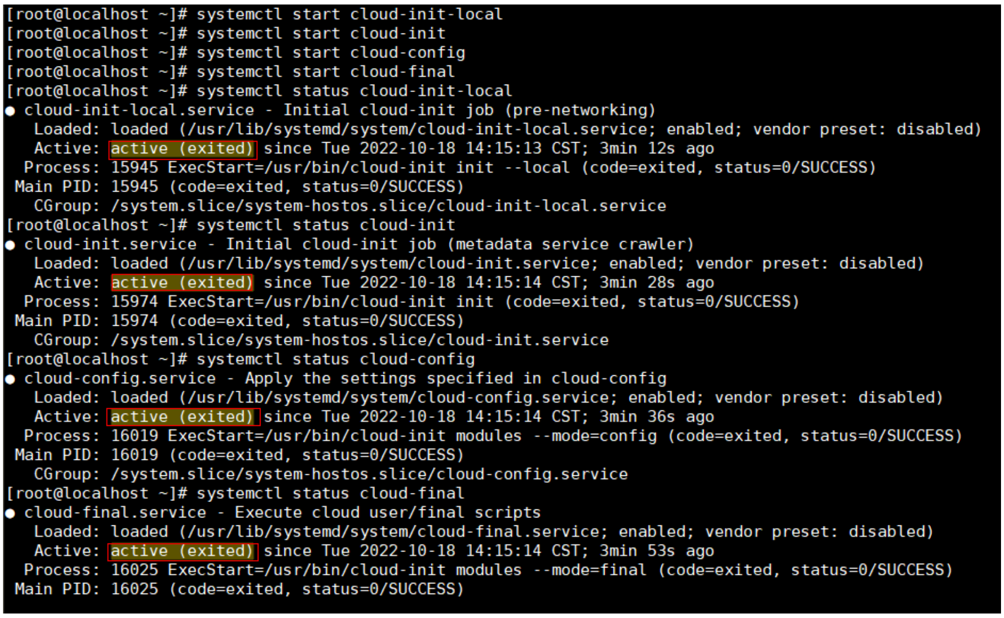
   systemctl start cloud-init-local

   systemctl start cloud-init

   systemctl start cloud-config

   systemctl start cloud-final

4. Run the commands in **1** to check whether the Cloud-Init status is **active**.



```
[root@localhost ~]# systemctl start cloud-init-local
[root@localhost ~]# systemctl start cloud-init
[root@localhost ~]# systemctl start cloud-config
[root@localhost ~]# systemctl start cloud-final
[root@localhost ~]# systemctl status cloud-init-local
● cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init-local.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:13 CST; 3min 12s ago
  Process: 15945 ExecStart=/usr/bin/cloud-init init --local (code=exited, status=0/SUCCESS)
 Main PID: 15945 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-init-local.service
[root@localhost ~]# systemctl status cloud-init
● cloud-init.service - Initial cloud-init job (metadata service crawler)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 28s ago
  Process: 15974 ExecStart=/usr/bin/cloud-init init (code=exited, status=0/SUCCESS)
 Main PID: 15974 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-init.service
[root@localhost ~]# systemctl status cloud-config
● cloud-config.service - Apply the settings specified in cloud-config
   Loaded: loaded (/usr/lib/systemd/system/cloud-config.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 36s ago
  Process: 16019 ExecStart=/usr/bin/cloud-init modules --mode=config (code=exited, status=0/SUCCESS)
 Main PID: 16019 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-config.service
[root@localhost ~]# systemctl status cloud-final
● cloud-final.service - Execute cloud user/final scripts
   Loaded: loaded (/usr/lib/systemd/system/cloud-final.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 53s ago
  Process: 16025 ExecStart=/usr/bin/cloud-init modules --mode=final (code=exited, status=0/SUCCESS)
 Main PID: 16025 (code=exited, status=0/SUCCESS)
```

3.9.4 EulerOS/OpenEuler

1. Check whether the Cloud-init services will automatically start when the system starts.

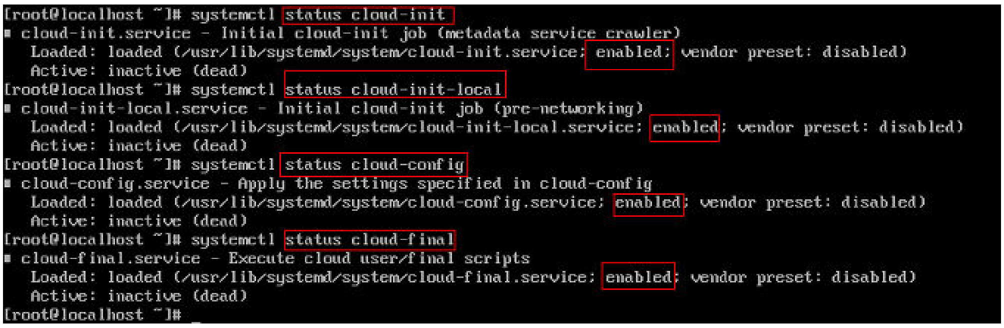
   systemctl status cloud-init-local

   systemctl status cloud-init

   systemctl status cloud-config

   systemctl status cloud-final

2. **enabled** indicates that the service will automatically start.



```
[root@localhost ~]# systemctl status cloud-init
● cloud-init.service - Initial cloud-init job (metadata service crawler)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost ~]# systemctl status cloud-init-local
● cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init-local.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost ~]# systemctl status cloud-config
● cloud-config.service - Apply the settings specified in cloud-config
   Loaded: loaded (/usr/lib/systemd/system/cloud-config.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost ~]# systemctl status cloud-final
● cloud-final.service - Execute cloud user/final scripts
   Loaded: loaded (/usr/lib/systemd/system/cloud-final.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost ~]# _
```

   Otherwise, run the following commands to enable automatic startup for them.

   systemctl enable cloud-init-local

   systemctl enable cloud-init

   systemctl enable cloud-config

   systemctl enable cloud-final

3. Run the following commands to start Cloud-Init:

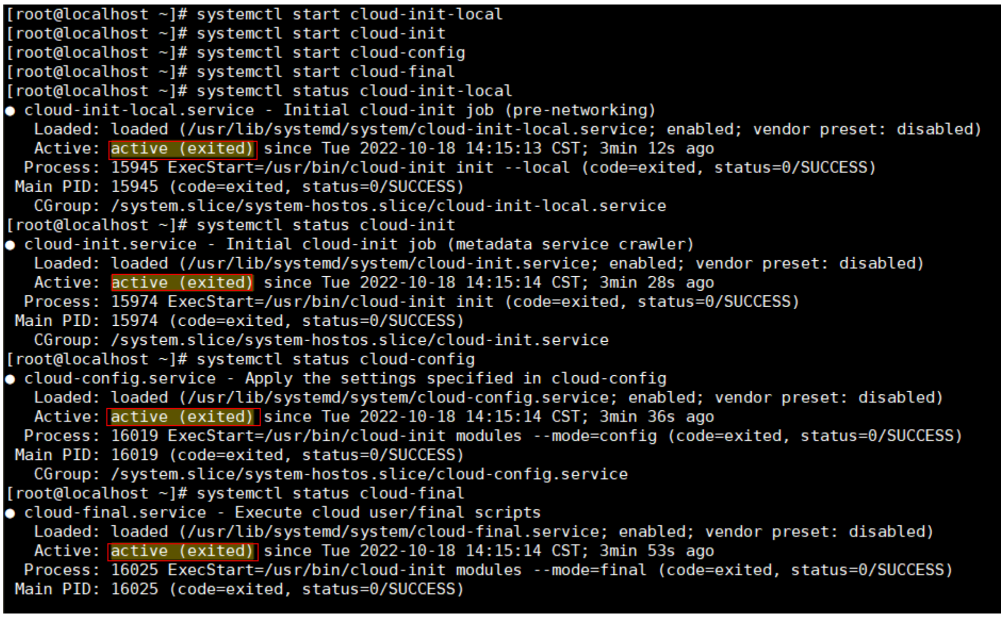
   systemctl start cloud-init-local

   systemctl start cloud-init

   systemctl start cloud-config

systemctl start cloud-final

4. Run the commands in 1 to check whether the Cloud-Init status is **active**.



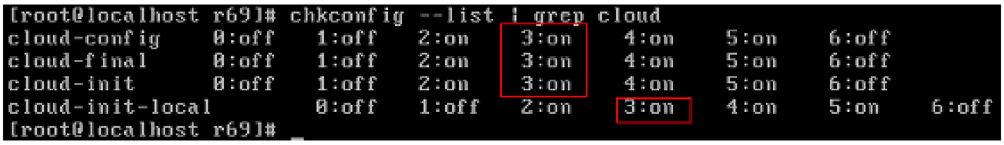
```
[root@localhost ~]# systemctl start cloud-init-local
[root@localhost ~]# systemctl start cloud-init
[root@localhost ~]# systemctl start cloud-config
[root@localhost ~]# systemctl start cloud-final
[root@localhost ~]# systemctl status cloud-init-local
● cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init-local.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:13 CST; 3min 12s ago
  Process: 15945 ExecStart=/usr/bin/cloud-init init --local (code=exited, status=0/SUCCESS)
 Main PID: 15945 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-init-local.service
[root@localhost ~]# systemctl status cloud-init
● cloud-init.service - Initial cloud-init job (metadata service crawler)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 28s ago
  Process: 15974 ExecStart=/usr/bin/cloud-init init (code=exited, status=0/SUCCESS)
 Main PID: 15974 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-init.service
[root@localhost ~]# systemctl status cloud-config
● cloud-config.service - Apply the settings specified in cloud-config
   Loaded: loaded (/usr/lib/systemd/system/cloud-config.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 36s ago
  Process: 16019 ExecStart=/usr/bin/cloud-init modules --mode=config (code=exited, status=0/SUCCESS)
 Main PID: 16019 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-config.service
[root@localhost ~]# systemctl status cloud-final
● cloud-final.service - Execute cloud user/final scripts
   Loaded: loaded (/usr/lib/systemd/system/cloud-final.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 53s ago
  Process: 16025 ExecStart=/usr/bin/cloud-init modules --mode=final (code=exited, status=0/SUCCESS)
 Main PID: 16025 (code=exited, status=0/SUCCESS)
```

3.9.5 Red Hat 6/CentOS 6/Oracle Linux 6

1. Run the following command:

   chkconfig --list | grep cloud

   As shown in the following figure, **on** indicates that automatic startup has been enabled for the service.



```
[root@localhost r69]# chkconfig --list | grep cloud
cloud-config    0:off   1:off   2:on    3:on    4:on    5:on    6:off
cloud-final     0:off   1:off   2:on    3:on    4:on    5:on    6:off
cloud-init      0:off   1:off   2:on    3:on    4:on    5:on    6:off
cloud-init-local        0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@localhost r69]# _
```

2. If automatic startup is not enabled for Cloud-Init services, run the following commands to enable it:

   chkconfig cloud-init on

   chkconfig cloud-init-local on

   chkconfig cloud-config on

   chkconfig cloud-final on

3.9.6 Ubuntu 16.04/Ubuntu 18.04

1. Run the following commands:

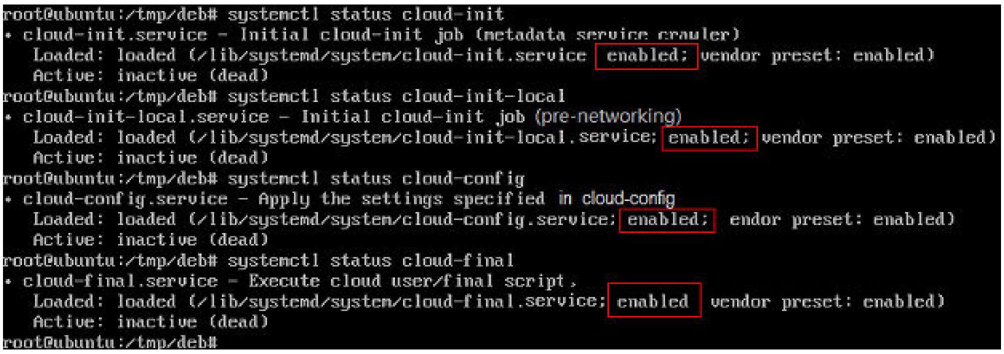
   systemctl status cloud-init

   systemctl status cloud-init-local

   systemctl status cloud-config

   systemctl status cloud-final

   As shown in the following figure, **enable** indicates that automatic startup has been enabled for the service.



```
root@ubuntu:/tmp/deb# systemctl status cloud-init
• cloud-init.service - Initial cloud-init job (metadata service crawler)
   Loaded: loaded (/lib/systemd/system/cloud-init.service  enabled; vendor preset: enabled)
   Active: inactive (dead)
root@ubuntu:/tmp/deb# systemctl status cloud-init-local
• cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/lib/systemd/system/cloud-init-local.service; enabled; vendor preset: enabled)
   Active: inactive (dead)
root@ubuntu:/tmp/deb# systemctl status cloud-config
• cloud-config.service - Apply the settings specified in cloud-config
   Loaded: loaded (/lib/systemd/system/cloud-config.service; enabled;  endor preset: enabled)
   Active: inactive (dead)
root@ubuntu:/tmp/deb# systemctl status cloud-final
• cloud-final.service - Execute cloud user/final script.
   Loaded: loaded (/lib/systemd/system/cloud-final.service; enabled  vendor preset: enabled)
   Active: inactive (dead)
root@ubuntu:/tmp/deb#
```

2. If automatic startup is not enabled for Cloud-Init services, run the following commands to enable it:

   systemctl enable cloud-init

   systemctl enable cloud-init-local

   systemctl enable cloud-config

   systemctl enable cloud-final

3. Run the following commands to start Cloud-Init:

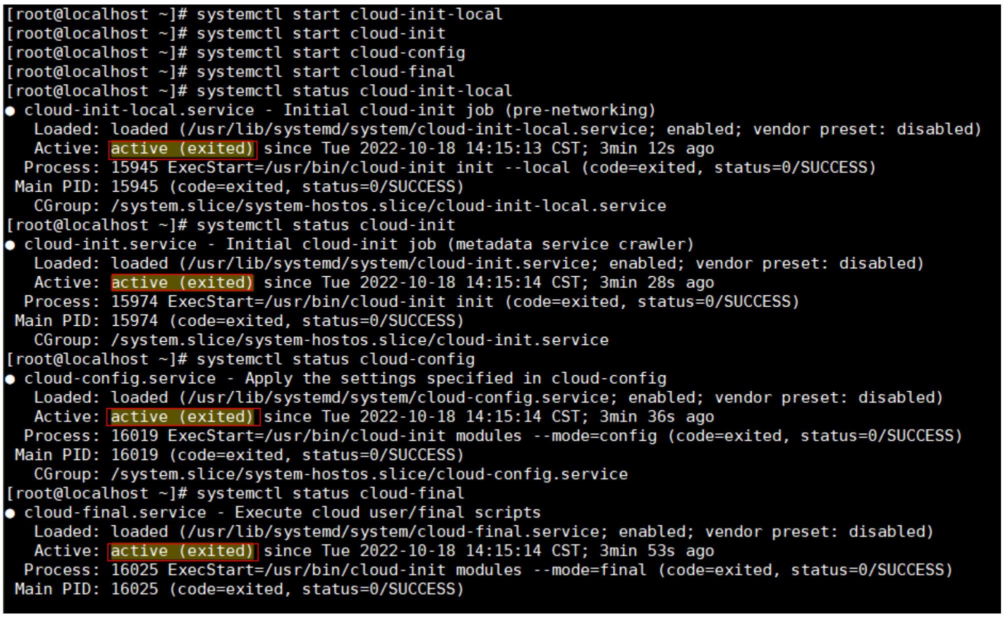
   systemctl start cloud-init-local

   systemctl start cloud-init

   systemctl start cloud-config

   systemctl start cloud-final

4. Run the commands in 1 to check whether the Cloud-Init status is **active**.



```
[root@localhost ~]# systemctl start cloud-init-local
[root@localhost ~]# systemctl start cloud-init
[root@localhost ~]# systemctl start cloud-config
[root@localhost ~]# systemctl start cloud-final
[root@localhost ~]# systemctl status cloud-init-local
● cloud-init-local.service - Initial cloud-init job (pre-networking)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init-local.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:13 CST; 3min 12s ago
  Process: 15945 ExecStart=/usr/bin/cloud-init init --local (code=exited, status=0/SUCCESS)
 Main PID: 15945 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-init-local.service
[root@localhost ~]# systemctl status cloud-init
● cloud-init.service - Initial cloud-init job (metadata service crawler)
   Loaded: loaded (/usr/lib/systemd/system/cloud-init.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 28s ago
  Process: 15974 ExecStart=/usr/bin/cloud-init init (code=exited, status=0/SUCCESS)
 Main PID: 15974 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-init.service
[root@localhost ~]# systemctl status cloud-config
● cloud-config.service - Apply the settings specified in cloud-config
   Loaded: loaded (/usr/lib/systemd/system/cloud-config.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 36s ago
  Process: 16019 ExecStart=/usr/bin/cloud-init modules --mode=config (code=exited, status=0/SUCCESS)
 Main PID: 16019 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/cloud-config.service
[root@localhost ~]# systemctl status cloud-final
● cloud-final.service - Execute cloud user/final scripts
   Loaded: loaded (/usr/lib/systemd/system/cloud-final.service; enabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-10-18 14:15:14 CST; 3min 53s ago
  Process: 16025 ExecStart=/usr/bin/cloud-init modules --mode=final (code=exited, status=0/SUCCESS)
 Main PID: 16025 (code=exited, status=0/SUCCESS)
```

3.9.7 Ubuntu 14.04

Run the following commands:

initctl status cloud-init

initctl status cloud-init-local

initctl status cloud-config

initctl status cloud-final

If Cloud-Init installation information is displayed, the installation is successful.

```
[root@ubuntu:~]# initctl status cloud-init
cloud-init stop/waiting
[root@ubuntu:~]# initctl status cloud-init-local
cloud-init-local stop/waiting
[root@ubuntu:~]# initctl status cloud-config
cloud-config stop/waiting
[root@ubuntu:~]# initctl status cloud-final
cloud-final stop/waiting
```

3.10 Modifying the Hardware Device Drivers That Boot the OS

Scenario

This section describes how to modify the hardware device drivers that are loaded during OS startup.

Prerequisites

You have logged in to the VM.

Procedure

1. Add or modify the configuration file.
   - For Red Hat/Oracle Linux/EulerOS/OpenEuler/SUSE 12/SUSE 15/CentOS, use the vi editor to open the **/etc/dracut.conf** file and change or add the value of **add_drivers**. In the following example, the value of **add_drivers** is a list of RAID drivers.

     ```
     logfile=/var/log/dracut.log
     # fileloglvl=7
     ...
     ...
     # additional kernel modules to the default
     add_drivers+="ahci megaraid_sas mpt3sas mpt2sas virtio_blk virtio_scsi virtio_net"
     ```

     NOTE

     If an error is reported, add a space before and after the driver list in the quotation marks and try again.
   - For Ubuntu 14.04 or Debian, use the vi editor to open the **/etc/initramfs-tools/modules** file and add ahci, megaraid_sas, mpt3sas, and mpt2sas drivers (the format depends on the OS).

     ```
     # List of modules that you want to include in your initramfs.
     # They will be loaded at boot time in the order below.
     #
     # Syntax:  module_name [args ...]
     #
     # You must run update-initramfs(8) to effect this change.
     #
     # Examples:
     #
     # raid1
     # sd_mod
     ahci
     megaraid_sas
     ```

```
mpt3sas
mpt2sas
virtio_blk
virtio_scsi
virtio_net
```

- For Ubuntu 16.04/Ubuntu 18.04, add drivers to the **/etc/dracut.conf** and **/etc/initramfs-tools/modules** files. Before editing the files, install required software.

  i. Run the following command to install dracut:

  apt-get install dracut

  After the installation is complete, add **add_drivers+="ahci megaraid_sas mpt3sas mpt2sas virtio_blk virtio_scsi virtio_net"** to the end of the **/etc/dracut.conf** file by performing operations similar to those for Red Hat and Oracle Linux 7.3.

  NOTE

  If an error is reported, add a space before and after the driver list in the quotation marks and try again.

  ii. Run the following command to install initramfs-tools:

  apt-get install initramfs-tools

  After the installation is complete, add the ahci, megaraid_sas, mpt3sas, mpt2sas, and virtio_blk virtio_scsi virtio_net drivers to the end of the **/etc/initramfs-tools/modules** file by performing operations similar to those for Ubuntu 14.04.

- For Ubuntu 16.04 ARM, run the following commands to update the kernel and drivers, and then restart the VM:

  sudo apt-get update

  sudo apt-get dist-upgrade

- For SUSE 11 SP4, use the vi editor to open the **/etc/sysconfig/kernel** file, and add or change the value of **INITRD_MODULES**. In the following example, the value of **INITRD_MODULES** is a list of RAID drivers.

```
...
#
INITRD_MODULES="ahci megaraid_sas mpt3sas mpt2sas virtio_blk virtio_scsi virtio_net"
## Type:   string(yes)
...
```

NOTE

You can enter multiple RAID drivers and separate them with spaces. The RAID driver names can be obtained from the purchased hardware devices. Multiple types of drivers can be added at the same time, such as mpt3sas, mpt2sas, and megaraid_sas. If any hardware driver cannot be installed here, you can install it after the BMS is created.

2. Update the kernel. For Ubuntu 16.04 ARM and Ubuntu 18.04 ARM, skip this step.

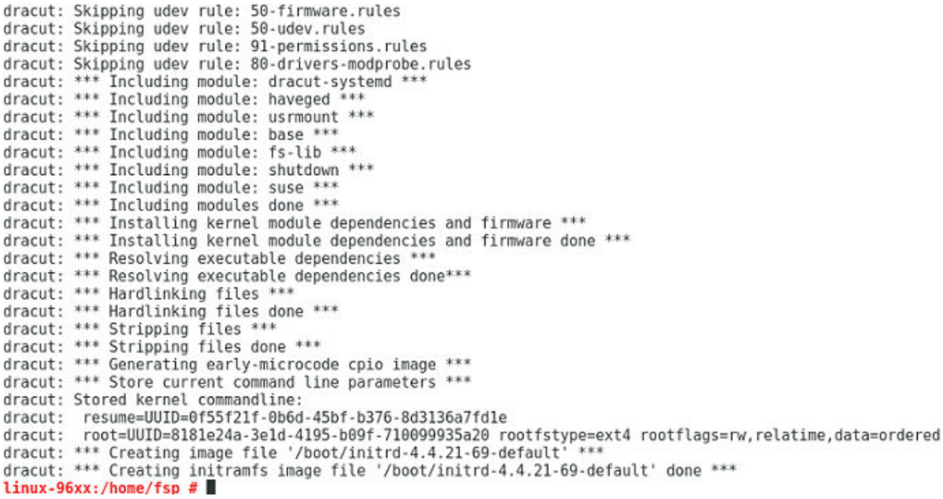
   For Rad Hat/Oracle Linux/EulerOS/SUSE 12/SUSE 15/Ubuntu 16.04/Ubuntu 18.04/CentOS run the **dracut -f** command.

   - For Rad Hat/Oracle Linux/EulerOS/OpenEuler/CentOS, run the **dracut -f** command. Wait for several seconds. If no command output is returned, the drivers have been loaded.
   - For SUSE 12 SP1, run the **dracut -f** command. Check the command output in the last few lines. If message "Some kernel modules could not

be included. This is not necessarily an error:" is displayed and drivers not loaded are displayed (excluding the RAID drivers), the RAID drivers are loaded successfully.

```
...
Some kernel modules could not be included
This is not necessarily an error:
pcmcia
sdhci_acpi
swap
```

– For SUSE 12/SUSE 15, run the **dracut -f** command. The kernel is updated successfully if information similar to the following is displayed.



```
dracut: Skipping udev rule: 50-firmware.rules
dracut: Skipping udev rule: 50-udev.rules
dracut: Skipping udev rule: 91-permissions.rules
dracut: Skipping udev rule: 80-drivers-modprobe.rules
dracut: *** Including module: dracut-systemd ***
dracut: *** Including module: haveged ***
dracut: *** Including module: usrmount ***
dracut: *** Including module: base ***
dracut: *** Including module: fs-lib ***
dracut: *** Including module: shutdown ***
dracut: *** Including module: suse ***
dracut: *** Including modules done ***
dracut: *** Installing kernel module dependencies and firmware ***
dracut: *** Installing kernel module dependencies and firmware done ***
dracut: *** Resolving executable dependencies ***
dracut: *** Resolving executable dependencies done***
dracut: *** Hardlinking files ***
dracut: *** Hardlinking files done ***
dracut: *** Stripping files ***
dracut: *** Stripping files done ***
dracut: *** Generating early-microcode cpio image ***
dracut: *** Store current command line parameters ***
dracut: Stored kernel commandline:
dracut:  resume=UUID=0f55f21f-0b6d-45bf-b376-8d3136a7fd1e
dracut:  root=UUID=8181e24a-3e1d-4195-b09f-710099935a20 rootfstype=ext4 rootflags=rw,relatime,data=ordered
dracut: *** Creating image file '/boot/initrd-4.4.21-69-default' ***
dracut: *** Creating initramfs image file '/boot/initrd-4.4.21-69-default' done ***
linux-96xx:/home/fsp #
```

– For Ubuntu 14.04/Ubuntu 16.04/Ubuntu 18.04/Debian, run the following command to generate initrd:

update-initramfs -u

Run the following commands to check whether the ahci, megaraid_sas, mpt3sas, and mpt2sas drivers have been loaded:

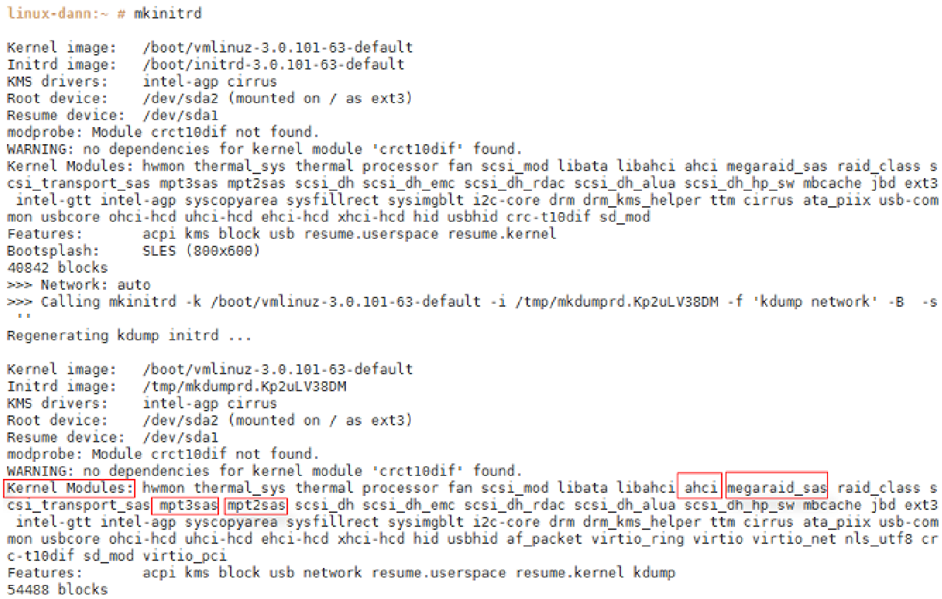
lsinitramfs /boot/initrd.img-`uname -r` |grep ahci

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

lsinitramfs /boot/initrd.img-`uname -r` |grep mpt3sas

lsinitramfs /boot/initrd.img-`uname -r` |grep mpt2sas

– For SUSE 11 SP4, run the **mkinitrd** command to check whether the value of **Kernel Modules** contains the manually added drivers. If the following command output is displayed, the drivers are successfully loaded.



```
linux-dann:~ # mkinitrd

Kernel image:   /boot/vmlinuz-3.0.101-63-default
Initrd image:   /boot/initrd-3.0.101-63-default
KMS drivers:    intel-agp cirrus
Root device:    /dev/sda2 (mounted on / as ext3)
Resume device:  /dev/sda1
modprobe: Module crct10dif not found.
WARNING: no dependencies for kernel module 'crct10dif' found.
Kernel Modules: hwmon thermal_sys thermal processor fan scsi_mod libata libahci ahci megaraid_sas raid_class s
csi_transport_sas mpt3sas mpt2sas scsi_dh scsi_dh_emc scsi_dh_rdac scsi_dh_alua scsi_dh_hp_sw mbcache jbd ext3
 intel-gtt intel-agp syscopyarea sysfillrect sysimgblt i2c-core drm drm_kms_helper ttm cirrus ata_piix usb-com
mon usbcore ohci-hcd uhci-hcd ehci-hcd xhci-hcd hid usbhid crc-t10dif sd_mod
Features:       acpi kms block usb resume.userspace resume.kernel
Bootsplash:     SLES (800x600)
40842 blocks
>>> Network: auto
>>> Calling mkinitrd -k /boot/vmlinuz-3.0.101-63-default -i /tmp/mkdumprd.Kp2uLV38DM -f 'kdump network' -B  -s
 ''

Regenerating kdump initrd ...

Kernel image:   /boot/vmlinuz-3.0.101-63-default
Initrd image:   /tmp/mkdumprd.Kp2uLV38DM
KMS drivers:    intel-agp cirrus
Root device:    /dev/sda2 (mounted on / as ext3)
Resume device:  /dev/sda1
modprobe: Module crct10dif not found.
WARNING: no dependencies for kernel module 'crct10dif' found.
Kernel Modules: hwmon thermal_sys thermal processor fan scsi_mod libata libahci ahci megaraid_sas raid_class s
csi_transport_sas mpt3sas mpt2sas scsi_dh scsi_dh_emc scsi_dh_rdac scsi_dh_alua scsi_dh_hp_sw mbcache jbd ext3
 intel-gtt intel-agp syscopyarea sysfillrect sysimgblt i2c-core drm drm_kms_helper ttm cirrus ata_piix usb-com
mon usbcore ohci-hcd uhci-hcd ehci-hcd xhci-hcd hid usbhid af_packet virtio_ring virtio virtio_net nls_utf8 cr
c-t10dif sd_mod virtio_pci
Features:       acpi kms block usb network resume.userspace resume.kernel kdump
54488 blocks
```

3. For SUSE 11 SP4, change the virtual disks in the VM file to physical disks. For other OSs, such as Rad Hat, CentOS, Oracle Linux, SUSE 12, and EulerOS, skip this step.

   NOTE

   If LVM is used, perform **3.a** to **3.e** to change the drive letter mode.

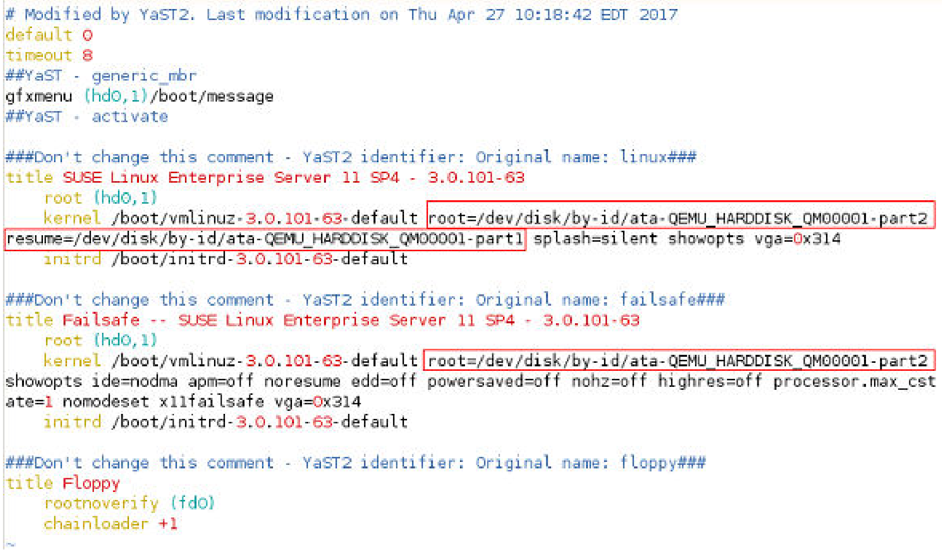
   a. In the **/boot/grub** directory of the VM, run the **blkid** command to check whether disk partitions are normal.

      linux-a5d6:/boot/grub # **blkid**
      /dev/sda1: UUID="c23d47f8-ef1b-4c4e-9a3b-5ae138ef7184" TYPE="swap"
      /dev/sda2: UUID="27644978-e244-4a8c-996a-03119fdaff71" TYPE="ext3"

      If some disk partitions do not have UUIDs, check whether the VM OS is properly installed. If it is not, install it again.

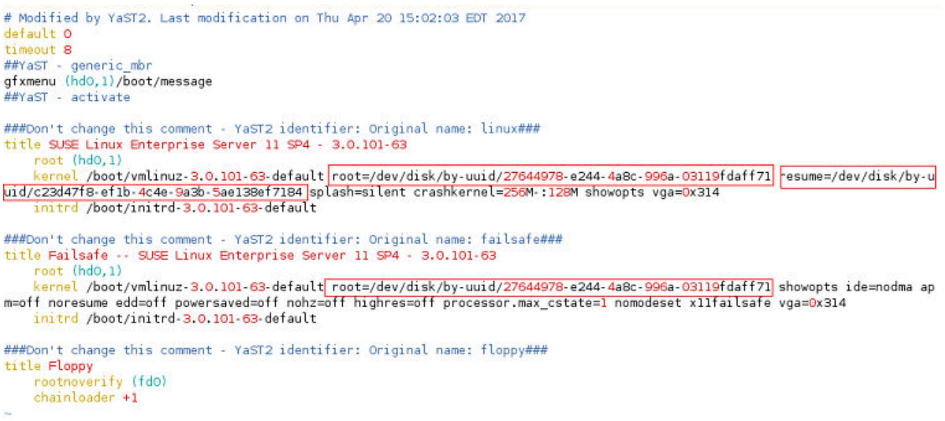
   b. Use the vi editor to open the **/boot/grub/menu.lst** file, modify the OS boot parameters, and save the configuration.

      Original **menu.lst** file



```
# Modified by YaST2. Last modification on Thu Apr 27 10:18:42 EDT 2017
default 0
timeout 8
##YaST - generic_mbr
gfxmenu (hd0,1)/boot/message
##YaST - activate

###Don't change this comment - YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63
    root (hd0,1)
    kernel /boot/vmlinuz-3.0.101-63-default root=/dev/disk/by-id/ata-QEMU_HARDDISK_QM00001-part2
resume=/dev/disk/by-id/ata-QEMU_HARDDISK_QM00001-part1 splash=silent showopts vga=0x314
    initrd /boot/initrd-3.0.101-63-default

###Don't change this comment - YaST2 identifier: Original name: failsafe###
title Failsafe -- SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63
    root (hd0,1)
    kernel /boot/vmlinuz-3.0.101-63-default root=/dev/disk/by-id/ata-QEMU_HARDDISK_QM00001-part2
showopts ide=nodma apm=off noresume edd=off powersaved=off nohz=off highres=off processor.max_cst
ate=1 nomodeset x11failsafe vga=0x314
    initrd /boot/initrd-3.0.101-63-default

###Don't change this comment - YaST2 identifier: Original name: floppy###
title Floppy
    rootnoverify (fd0)
    chainloader +1
~
```

      Modified **menu.lst** file



```
# Modified by YaST2. Last modification on Thu Apr 20 15:02:03 EDT 2017
default 0
timeout 8
##YaST - generic_mbr
gfxmenu (hd0,1)/boot/message
##YaST - activate

###Don't change this comment - YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63
    root (hd0,1)
    kernel /boot/vmlinuz-3.0.101-63-default root=/dev/disk/by-uuid/27644978-e244-4a8c-996a-03119fdaff71 resume=/dev/disk/by-uuid/c23d47f8-ef1b-4c4e-9a3b-5ae138ef7184 splash=silent crashkernel=256M-:128M showopts vga=0x314
    initrd /boot/initrd-3.0.101-63-default

###Don't change this comment - YaST2 identifier: Original name: failsafe###
title Failsafe -- SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63
    root (hd0,1)
    kernel /boot/vmlinuz-3.0.101-63-default root=/dev/disk/by-uuid/27644978-e244-4a8c-996a-03119fdaff71 showopts ide=nodma apm=off noresume edd=off powersaved=off nohz=off highres=off processor.max_cstate=1 nomodeset x11failsafe vga=0x314
    initrd /boot/initrd-3.0.101-63-default

###Don't change this comment - YaST2 identifier: Original name: floppy###
title Floppy
    rootnoverify (fd0)
    chainloader +1
~
```

c. Use the vi editor to open the **/boot/grub/device.map** file.

Original **device.map** file

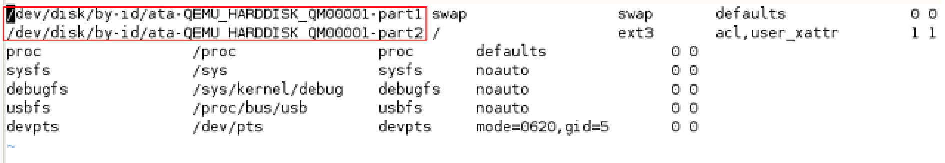
```
(hd0)    /dev/disk/by-id/ata-QEMU_HARDDISK_QM00001
~
```

Modified **device.map** file

```
(hd0)    /dev/sda
```

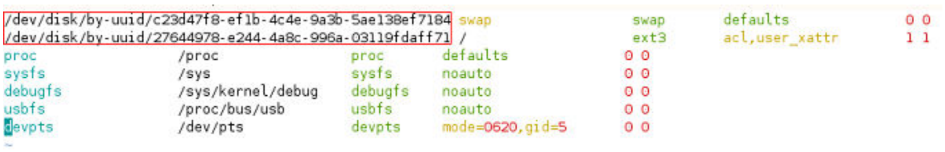
d. Use the vi editor to open the **/etc/fstab** file.

Original **fstab** file



```
/dev/disk/by-id/ata-QEMU_HARDDISK_QM00001-part1 swap                 swap       defaults          0 0
/dev/disk/by-id/ata-QEMU_HARDDISK_QM00001-part2 /                    ext3       acl,user_xattr    1 1
proc                 /proc                proc       defaults              0 0
sysfs                /sys                 sysfs      noauto                0 0
debugfs              /sys/kernel/debug    debugfs    noauto                0 0
usbfs                /proc/bus/usb        usbfs      noauto                0 0
devpts               /dev/pts             devpts     mode=0620,gid=5       0 0
~
```

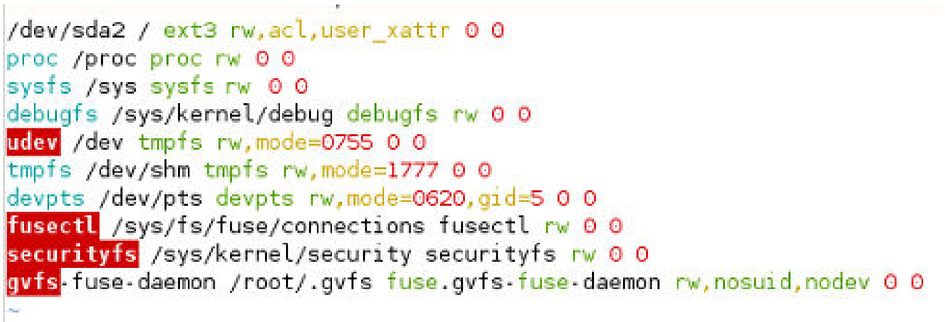
Modified **fstab** file



```
/dev/disk/by-uuid/c23d47f8-ef1b-4c4e-9a3b-5ae138ef7184 swap          swap       defaults          0 0
/dev/disk/by-uuid/27644978-e244-4a8c-996a-03119fdaff71 /             ext3       acl,user_xattr    1 1
proc                 /proc                proc       defaults              0 0
sysfs                /sys                 sysfs      noauto                0 0
debugfs              /sys/kernel/debug    debugfs    noauto                0 0
usbfs                /proc/bus/usb        usbfs      noauto                0 0
devpts               /dev/pts             devpts     mode=0620,gid=5       0 0
~
```

e. Use the vi editor to open the **/etc/mtab** file, delete the line where CDROM of **/dev/sr0** is located, and save the configuration.

Modified **mtab** file



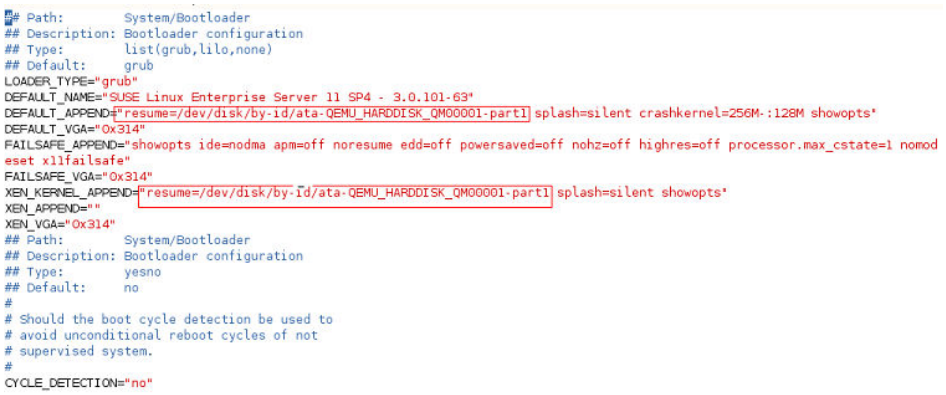
```
/dev/sda2 / ext3 rw,acl,user_xattr 0 0
proc /proc proc rw 0 0
sysfs /sys sysfs rw 0 0
debugfs /sys/kernel/debug debugfs rw 0 0
udev /dev tmpfs rw,mode=0755 0 0
tmpfs /dev/shm tmpfs rw,mode=1777 0 0
devpts /dev/pts devpts rw,mode=0620,gid=5 0 0
fusectl /sys/fs/fuse/connections fusectl rw 0 0
securityfs /sys/kernel/security securityfs rw 0 0
gvfs-fuse-daemon /root/.gvfs fuse.gvfs-fuse-daemon rw,nosuid,nodev 0 0
~
```

NOTE

If the **/dev/sr0** configuration item does not exist, skip this step.

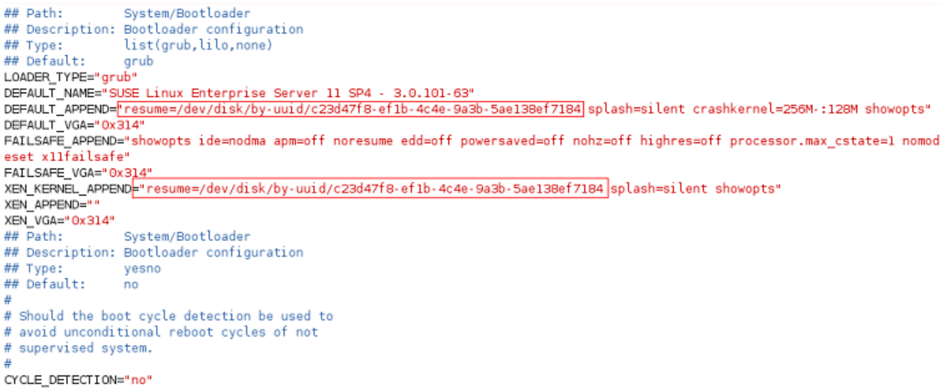
f. Use the vi editor to open the **/etc/sysconfig/bootloader** file.

Original **bootloader** file



```
## Path:        System/Bootloader
## Description: Bootloader configuration
## Type:        list(grub,lilo,none)
## Default:     grub
LOADER_TYPE="grub"
DEFAULT_NAME="SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63"
DEFAULT_APPEND="resume=/dev/disk/by-id/ata-QEMU_HARDDISK_QM00001-part1 splash=silent crashkernel=256M-:128M showopts"
DEFAULT_VGA="0x314"
FAILSAFE_APPEND="showopts ide=nodma apm=off noresume edd=off powersaved=off nohz=off highres=off processor.max_cstate=1 nomod
eset x11failsafe"
FAILSAFE_VGA="0x314"
XEN_KERNEL_APPEND="resume=/dev/disk/by-id/ata-QEMU_HARDDISK_QM00001-part1 splash=silent showopts"
XEN_APPEND=""
XEN_VGA="0x314"
## Path:        System/Bootloader
## Description: Bootloader configuration
## Type:        yesno
## Default:     no
#
# Should the boot cycle detection be used to
# avoid unconditional reboot cycles of not
# supervised system.
#
CYCLE_DETECTION="no"
```

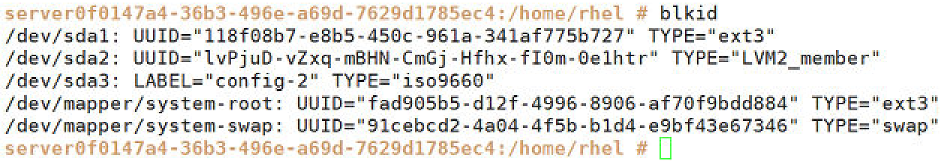
Modified **bootloader** file



```
## Path:        System/Bootloader
## Description: Bootloader configuration
## Type:        list(grub,lilo,none)
## Default:     grub
LOADER_TYPE="grub"
DEFAULT_NAME="SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63"
DEFAULT_APPEND="resume=/dev/disk/by-uuid/c23d47f8-ef1b-4c4e-9a3b-5ae138ef7184 splash=silent crashkernel=256M-:128M showopts"
DEFAULT_VGA="0x314"
FAILSAFE_APPEND="showopts ide=nodma apm=off noresume edd=off powersaved=off nohz=off highres=off processor.max_cstate=1 nomod
eset x11failsafe"
FAILSAFE_VGA="0x314"
XEN_KERNEL_APPEND="resume=/dev/disk/by-uuid/c23d47f8-ef1b-4c4e-9a3b-5ae138ef7184 splash=silent showopts"
XEN_APPEND=""
XEN_VGA="0x314"
## Path:        System/Bootloader
## Description: Bootloader configuration
## Type:        yesno
## Default:     no
#
# Should the boot cycle detection be used to
# avoid unconditional reboot cycles of not
# supervised system.
#
CYCLE_DETECTION="no"
```

If SUSE 11 SP4 uses LVM, replace the virtual disks in the VM file with the actual physical disks.

a. In the **/boot/grub** directory of the VM, run the **blkid** command to check whether disk partitions are normal.

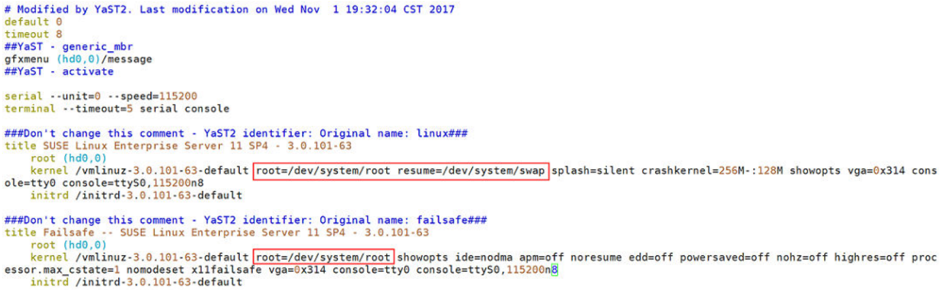


```
server0f0147a4-36b3-496e-a69d-7629d1785ec4:/home/rhel # blkid
/dev/sda1: UUID="118f08b7-e8b5-450c-961a-341af775b727" TYPE="ext3"
/dev/sda2: UUID="lvPjuD-vZxq-mBHN-CmGj-Hfhx-fI0m-0e1htr" TYPE="LVM2_member"
/dev/sda3: LABEL="config-2" TYPE="iso9660"
/dev/mapper/system-root: UUID="fad905b5-d12f-4996-8906-af70f9bdd884" TYPE="ext3"
/dev/mapper/system-swap: UUID="91cebcd2-4a04-4f5b-b1d4-e9bf43e67346" TYPE="swap"
server0f0147a4-36b3-496e-a69d-7629d1785ec4:/home/rhel #
```

If some disk partitions do not have UUIDs, check whether the VM OS is properly installed. If it is not, install it again.

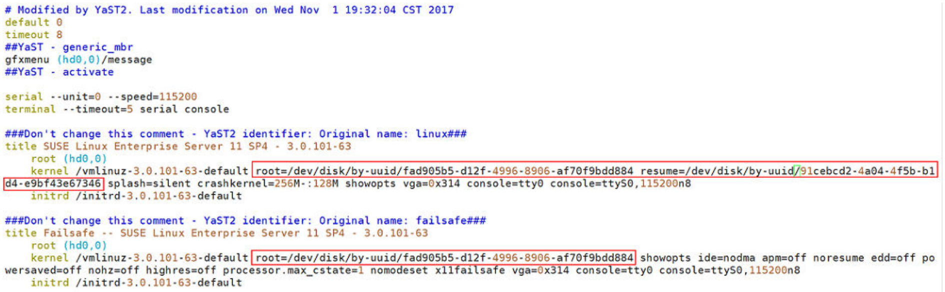
b. Use the vi editor to open the **/boot/grub/menu.lst** file, modify the OS boot parameters, and save the configuration.

Original **menu.lst** file



```
# Modified by YaST2. Last modification on Wed Nov  1 19:32:04 CST 2017
default 0
timeout 8
##YaST - generic_mbr
gfxmenu (hd0,0)/message
##YaST - activate

serial --unit=0 --speed=115200
terminal --timeout=5 serial console

###Don't change this comment - YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63
    root (hd0,0)
    kernel /vmlinuz-3.0.101-63-default root=/dev/system/root resume=/dev/system/swap splash=silent crashkernel=256M-:128M showopts vga=0x314 cons
ole=tty0 console=ttyS0,115200n8
    initrd /initrd-3.0.101-63-default

###Don't change this comment - YaST2 identifier: Original name: failsafe###
title Failsafe -- SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63
    root (hd0,0)
    kernel /vmlinuz-3.0.101-63-default root=/dev/system/root showopts ide=nodma apm=off noresume edd=off powersaved=off nohz=off highres=off proc
essor.max_cstate=1 nomodeset x11failsafe vga=0x314 console=tty0 console=ttyS0,115200n8
    initrd /initrd-3.0.101-63-default
```

Modified **menu.lst** file



```
# Modified by YaST2. Last modification on Wed Nov  1 19:32:04 CST 2017
default 0
timeout 8
##YaST - generic_mbr
gfxmenu (hd0,0)/message
##YaST - activate

serial --unit=0 --speed=115200
terminal --timeout=5 serial console

###Don't change this comment - YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63
    root (hd0,0)
    kernel /vmlinuz-3.0.101-63-default root=/dev/disk/by-uuid/fad905b5-d12f-4996-8906-af70f9bdd884 resume=/dev/disk/by-uuid/91cebcd2-4a04-4f5b-b1
d4-e9bf43e67346 splash=silent crashkernel=256M-:128M showopts vga=0x314 console=tty0 console=ttyS0,115200n8
    initrd /initrd-3.0.101-63-default

###Don't change this comment - YaST2 identifier: Original name: failsafe###
title Failsafe -- SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63
    root (hd0,0)
    kernel /vmlinuz-3.0.101-63-default root=/dev/disk/by-uuid/fad905b5-d12f-4996-8906-af70f9bdd884 showopts ide=nodma apm=off noresume edd=off po
wersaved=off nohz=off highres=off processor.max_cstate=1 nomodeset x11failsafe vga=0x314 console=tty0 console=ttyS0,115200n8
    initrd /initrd-3.0.101-63-default
```

c. Use the vi editor to open the **/boot/grub/device.map** file.

Original **device.map** file

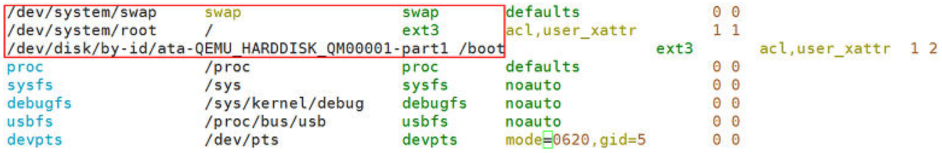
```
(hd0)    /dev/disk/by-id/ata-QEMU_HARDDISK_QM00001
```

Modified **device.map** file

```
(hd0)    /dev/sda
~
```

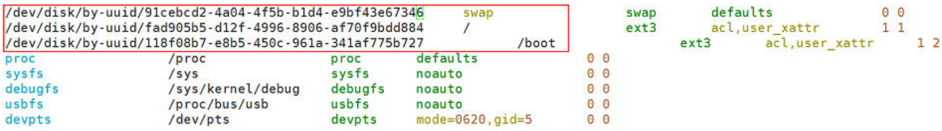
d. Use the vi editor to open the **/etc/fstab** file.

Original **fstab** file



```
/dev/system/swap     swap                 swap      defaults             0 0
/dev/system/root     /                    ext3      acl,user_xattr       1 1
/dev/disk/by-id/ata-QEMU_HARDDISK_QM00001-part1 /boot          ext3       acl,user_xattr  1 2
proc                 /proc                proc      defaults             0 0
sysfs                /sys                 sysfs     noauto               0 0
debugfs              /sys/kernel/debug    debugfs   noauto               0 0
usbfs                /proc/bus/usb        usbfs     noauto               0 0
devpts               /dev/pts             devpts    mode=0620,gid=5      0 0
```

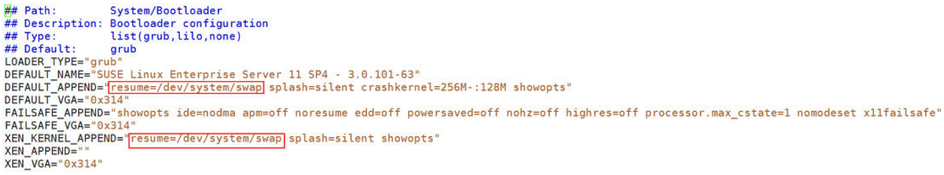
Modified **fstab** file



```
/dev/disk/by-uuid/91cebcd2-4a04-4f5b-b1d4-e9bf43e67346     swap                swap       defaults          0 0
/dev/disk/by-uuid/fad905b5-d12f-4996-8906-af70f9bdd884     /                   ext3       acl,user_xattr    1 1
/dev/disk/by-uuid/118f08b7-e8b5-450c-961a-341af775b727           /boot               ext3       acl,user_xattr     1 2
proc                 /proc               proc       defaults          0 0
sysfs                /sys                sysfs      noauto            0 0
debugfs              /sys/kernel/debug   debugfs    noauto            0 0
usbfs                /proc/bus/usb       usbfs      noauto            0 0
devpts               /dev/pts            devpts     mode=0620,gid=5   0 0
```

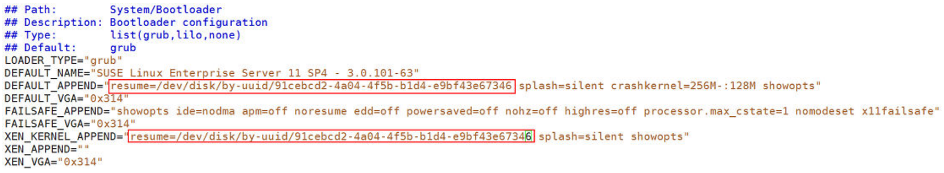
e. Use the vi editor to open the **/etc/sysconfig/bootloader** file.

Original **bootloader** file



```
## Path:        System/Bootloader
## Description: Bootloader configuration
## Type:        list(grub,lilo,none)
## Default:     grub
LOADER_TYPE="grub"
DEFAULT_NAME="SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63"
DEFAULT_APPEND="resume=/dev/system/swap splash=silent crashkernel=256M-:128M showopts"
DEFAULT_VGA="0x314"
FAILSAFE_APPEND="showopts ide=nodma apm=off noresume edd=off powersaved=off nohz=off highres=off processor.max_cstate=1 nomodeset x11failsafe"
FAILSAFE_VGA="0x314"
XEN_KERNEL_APPEND="resume=/dev/system/swap splash=silent showopts"
XEN_APPEND=""
XEN_VGA="0x314"
```

Modified **bootloader** file



```
## Path:        System/Bootloader
## Description: Bootloader configuration
## Type:        list(grub,lilo,none)
## Default:     grub
LOADER_TYPE="grub"
DEFAULT_NAME="SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63"
DEFAULT_APPEND="resume=/dev/disk/by-uuid/91cebcd2-4a04-4f5b-b1d4-e9bf43e67346 splash=silent crashkernel=256M-:128M showopts"
DEFAULT_VGA="0x314"
FAILSAFE_APPEND="showopts ide=nodma apm=off noresume edd=off powersaved=off nohz=off highres=off processor.max_cstate=1 nomodeset x11failsafe"
FAILSAFE_VGA="0x314"
XEN_KERNEL_APPEND="resume=/dev/disk/by-uuid/91cebcd2-4a04-4f5b-b1d4-e9bf43e67346 splash=silent showopts"
XEN_APPEND=""
XEN_VGA="0x314"
```

After the configuration is complete, run the **mkinitrd** command. If the value of **resume** is not **by-uuid**, run the **reboot** and then **mkinitrd** commands to ensure that the value of **resume** is **by-uuid**.

4. For Ubuntu 18.04 and Ubuntu 16.04 ARM, modify the **grub**, **fstab**, and **interfaces** files.

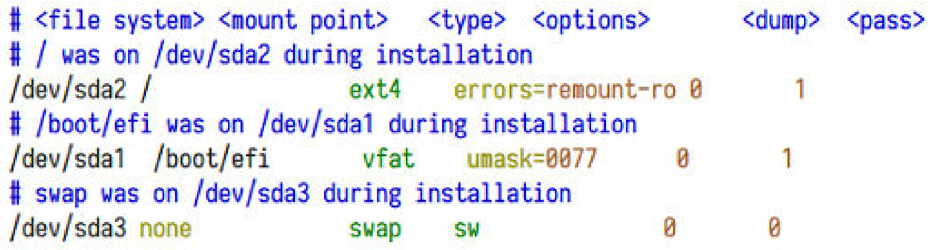
   a. Modify parameters in the **/etc/default/grub** configuration file.

      Set **GRUB_DISABLE_LINUX_UUID** to **true**.

```
...
# Uncomment if you don't want GRUB to pass "root=UUID=xxx" parameter to linux
GRUB_DISABLE_LINUX_UUID=true

# Uncomment to disable generation of recovery mode menu entries
...
```

Then, run the **sudo update-grub2** command.

b. Change the UUID in the **/etc/fstab** file to that of **/dev/sdax**, which can be obtained by running the **sudo blkid** command.



```
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda2 during installation
/dev/sda2 /               ext4    errors=remount-ro 0       1
# /boot/efi was on /dev/sda1 during installation
/dev/sda1  /boot/efi       vfat    umask=0077      0       1
# swap was on /dev/sda3 during installation
/dev/sda3 none            swap    sw              0       0
```

c. Delete all interface information except **lo interface** from the **/etc/network/interfaces** file.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces (5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface to inet loopback

~
~
```

3.11 Installing bms-network-config

Scenario

Install bms-network-config to work with Cloud-Init for the network configuration of the BMSs with centralized BMGW. For the BMSs with distributed BMGW (that is, BMSs with SDI 3.0 or SDI 2.2 cards), you do not need to perform operations in this section. **Table 3-6** describes the BMS flavors for which bms-network-config needs to be installed.

Table 3-6 BMS flavors

BMS Type	Flavor
General-purpose	physical.s3.large, physical.s3.xlarge, physical.s3.2xlarge, physical.s4.medium, physical.s4.large, physical.s4.xlarge, physical.s4.2xlarge, physical.s4.3xlarge
Disk-intensive	physical.d1.large, physical.d2.tiny, physical.d2.large, physical.d2.xmedium
Memory-optimized	physical.m2.small, physical.m2.medium, physical.m2.large, physical.m2.xlarge

BMS Type	Flavor
I/O-optimized	physical.io1.large, physical.io2.xlarge
GPU-accelerated	physical.p1.large, physical.p2.large, physical.g1.small, physical.p3.large, physical.pi6.3xlarge.6
High-performance computing	physical.h2.large, physical.hc2.xlarge
Kunpeng	physical.ks1.2xlarge

Prerequisites

- You have logged in to the VM.
- Cloud-Init has been installed on the VM.
- You have downloaded the bms-network-config software package and SHA256 checksum by referring to **Software** and verified the software package integrity (for details, see**How Do I Verify Software Package Integrity?**).

  NOTE

  Download the RPM package depending on the OS. Ubuntu and Debian use the .deb package, and CentOS and EulerOS (Arm) use the aarch .rpm package.

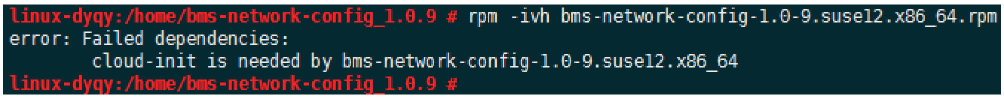
Procedure

1. Enter the directory where the bms-network-config software package is stored and run the **rpm -ivh***bms-network-config-1.0-7.centosRedhat7.x86_64.rpm* command.

```
[root@localhost r74]# rpm -ivhbms-network-config-1.0-7.centosRedhat7.x86_64.rpm
Preparing...                ################################# [100%]
Updating / installing...
   1:bms-network-config-1.0.7.centosRe################################# [100%]
```

NOTE

If the error shown in the following figure is displayed when you install bms-network-config for SUSE 12/SUSE 15, run the **rpm -ivh bms-network-config-1.0-9.suse12.x86_64.rpm --nodeps --force** command.



```
linux-dyqy:/home/bms-network-config_1.0.9 # rpm -ivh bms-network-config-1.0-9.suse12.x86_64.rpm
error: Failed dependencies:
        cloud-init is needed by bms-network-config-1.0-9.suse12.x86_64
linux-dyqy:/home/bms-network-config_1.0.9 #
```

For Ubuntu/Debian, run the **dpkg -i***xxx* command (*xxx* indicates the .deb package name).

```
root@ubuntu:~/file# dpkg -i bms-network-config-1.0.7.ubuntu1604-918.deb
Selecting previously unselected package bms-network-config.
(Reading database ... 97630 files and directories currently installed.)
Preparing to unpack bms-network-config-1.0.7.ubuntu1604-918.deb ...
Unpacking bms-network-config (1.0) ...
Setting up bms-network-config (1.0) ...
root@ubuntu:~/file# dpkg -s bms-network-config
```

NOTE

The names of the .rpm and .deb packages vary according to the actual situation.

2. After the installation is complete, run the **rpm -qa | grep bms-network-config** command. The installation is successful if the following information is displayed:

   ```
   [root@localhost r74]# rpm -qa | grep bms
   bms-network-config-1.0.7.centosRedhat7.x86_64
   ```

   For Ubuntu/Debian, run the **dpkg -s bms-network-config** command.

3. Check the bms-network-config status.
   - For Oracle Linux 7, Red Hat 7, CentOS 7, Ubuntu 16.04, Ubuntu 18.04, SUSE 12, SUSE 15, or EulerOS, run the **service bms-network-config status** command to check the service status. If the status is not **enabled**, run the **systemctl enable bms-network-config** command to enable the service.

     ```
     [root@localhost r74]# service bms-network-config status
     Redirecting to /bin/systemctl status bms-network-config.service
       bms-network-config.service - Network Config
       Loaded: loaded (/usr/lib/systemd/system/bms-network-config service; enabled vendor preset: disabled)
       Active: inactive (dead)
     ```

   - For Red Hat 6, CentOS 6, SUSE 11 SP4, Oracle Linux 6.8, or Oracle Linux 6.9, run the **chkconfig --list | grep bms-network-config** command to check the service status. If the status is not **on**, run the **chkconfig bms-network-config on** command to enable the service.

     ```
     [root@localhost r69]# chkconfig --list | grep bms
     bms-network-config   0:off   1:off   2:on   3:on   4:off   5:on   6:off
     ```

   - For Ubuntu 14.04/Debian, run the **initctl status bms-network_config** command to check the service status.

     ```
     root@ubuntu:~# initctl status bms-network_config
     bms-network_config stop/waiting
     ```

4. Check the startup dependencies between bms-network-config and other services.

   Run the **systemctl cat bms-network-config** command to check the configuration file and ensure that the file content is as follows:

   ```
   [Unit]
   Description=NetworkConfig
   DefaultDependencies=no
   After=dbus.service
   Wants=dbus.service

   [Service]
   Type=oneshot
   ExecStart=/usr/bin/bms-network_config rhel
   RemainAfterExit=yes
   TimeoutSec=0

   [Install]
   WantedBy=multi-user.target
   ```

   If the startup sequence is incorrect, use the **vim /usr/lib/systemd/system/bms-network-config.service** command to correct it.

3.12 Installing the Network Service

Scenario

By default, the network service is not installed for CentOS 8, EulerOS 2.9, Red Hat 8, Ubuntu 20, or later. For BMSs with centralized BMGW, the network service and network scripts are required to configure the network. For BMSs with distributed BMGW (that is, BMSs with SDI 3.0 or SDI 2.2 cards), skip this section.

Procedure

EulerOS 2.10 is used as an example.

1. Log in to the VM and query the network status.

   ```
   [root@euler210-arm-new ~]# systemctl status network
   Unit network.service could not be found.
   ```

2. Use the yum source to install network-scripts.

   ```
   [root@euler210-arm-new network-scripts]# yum install network-scripts
   ```

3. After the installation is complete, check whether the network service exists.

   ```
   [root@euler210-arm-new network-scripts]# systemctl status network
   ● network.service - LSB: Bring up/down networking
   Loaded: loaded (/etc/rc.d/init.d/network; generated)
   Active: inactive (dead)
   Docs: man:systemd-sysv-generator(8)
   ```

3.13 Installing the SDI Driver

Scenario

Currently, there are three types of SDI cards: SDI storage cards, SDI 2.2 (network cards), and SDI 3.0 (integrated storage and network cards). If the BMS uses SDI storage cards (neither SDI 2.2 nor SDI 3.0), the SDI driver needs to be installed on the VM so that EVS disks can be attached to the BMS. In other cases, skip this section. Currently, ARM 64 VMs do not support SDI cards. You do not need to install the SDI driver on such VMs.

Prerequisites

- You have logged in to the VM.
- You have downloaded the SDI driver (scsi_ep_front) as instructed in **Software** and have uploaded it to the VM.

  NOTE

  The scsi_ep_front version must be 1.0.13 or later.

Procedure

The following steps are for reference only.

1. Go to the directory storing the SDI driver installation package and run the following command:

   ```
   rpm -ivh kmod-scsi_ep_front-centos_7.6_1.0.18-3.10.0_957.el7.centos.x86_64.rpm
   ```

NOTE

The Ubuntu and Debian SDI driver uses the .deb installation package. Run the **dpkg -i***xxx* (*xxx* indicates the name of the SDI installation package) command to install the SDI driver.

2. After the installation is complete, run the **rpm -qa | grep scsi** command. The installation is successful if information similar to the following is displayed:

```
[root@localhost ~] rpm -qa | grep scsi
lsscsi-0.27-6.el7.x86_64
kmod-scsi_ep_front-centos_7.6_1.0.18-3.10.0_957.el7.centos.x86_64
```

For Ubuntu 18.04, Ubuntu 16.04, Ubuntu 14.04, and Debian, run the **dkms status** command. If **installed** is displayed, the installation is successful. Run the **update-initramfs -u** command to update the driver in the kernel.

```
...
root@ubuntu:~/file# dkms status
scsi_ep_front, 1.0.13, 4.4.0-21-generic, x86_64: installed
scsi_ep_front, 1.0.13, 4.4.0-59-generic, x86_64: built
scsi_ep_front, 1.0.13, 4.4.0-96-generic, x86_64: installed
```

3. Run the following commands to check whether the SDI driver matches the kernel version:

   a. Run the **uname -r** command to obtain the OS kernel version.

   ```
   [root@localhost r74]# uname -r
   3.10.0-957.el7.x86_64
   ```

   b. Run the **find / -name "*front*.ko"** command to check the SDI card driver matching the kernel version.

   ```
   [root@localhost r74]# find / -name "*front*.ko"
   /usr/lib/modules/3.10.0-957.el7.x86_64/extra/scsi_ep_front/scsi_ep_front.ko
   ```

3.14 Installing the Hi1822 Driver

If the BMS uses Hi1822 NICs, you need to install the Hi1822 driver on the VM.

3.14.1 Hi1822 Standard Cards (for BMSs with Centralized BMGW)

Scenario

If the BMS with centralized BMGW uses Hi1822 NICs, you need to install the Hi1822 driver on the VM. The following uses CentOS 7.6 as an example.

Prerequisites

- You have logged in to the VM.
- You have obtained the Hi1822 driver installation package and management software and uploaded them to the VM.

  For details about how to obtain the packages (.rpm), see **Software**.

  The downloaded Hi1822 driver installation package and management software must match the OS.

Procedure

1. Check whether the hinic driver exists.

rpm -qa | grep hinic

- If yes, go to **2**.
- If no, go to **3**.

2. Uninstall the hinic driver.

   rpm -e kmod-hinic

   rmmod hinic

3. Go to the directory where the .rpm installation package is stored and run the following command to install it:

   rpm -ivh NIC-Hi1822-CentOS7.6-hinic-3.9.0.8-1-x86_64.rpm

4. Run the **modprobe hinic** command to load the latest Hi1822 driver.
5. Install Hi1822 management software (hinicadm package).

   rpm -ivh NIC-Hi1822-CentOS7.6-hinicadm-3.9.0.8-1-x86_64.rpm

3.14.2 Hi1822 Offload Cards (for BMSs with SDI 2.2)

Scenario

If the BMS uses SDI 2.2 cards, you need to install the Hi1822 driver on the VM. The following uses EulerOS 2.3 as an example.

Prerequisites

- You have logged in to the VM.
- You have obtained the Hi1822 driver installation package and management software and uploaded them to the VM.

  Perform the following operations to obtain the package.

  a. Download the .zip package as instructed in **Software**.

  b. The following uses **Hi1822_BM_X86_1.19.3.B036.tar.gz** as an example to describe how to obtain the required installation package.

     Download and decompress the **Hi1822_BM_X86_1.19.3.B036.tar.gz** driver package, and obtain the .rpm package **kmod-hinic-1.8.3.16_3.10.0_514.41.4.28.h70.x86_64-1.x86_64.rpm** based on the OS type and kernel version.

     kmod-hinic-1.8.3.16_3.10.0_514.41.4.28.h70.x86_64-1.x86_64.rpm

Procedure

1. Check whether the hinic driver exists.

   rpm -qa | grep hinic

   - If yes, go to **2**.
   - If no, go to **3**.

2. Uninstall the hinic driver.

   rpm -e kmod-hinic

   rmmod hinic

3. Go to the directory where the .rpm installation package is stored and run the following command to install it:

rpm -ivh kmod-hinic-1.8.3.16_3.10.0_514.41.4.28.h70.x86_64-1.x86_64.rpm

4. Run the **modprobe hinic** command to load the latest Hi1822 driver.

3.14.3 Hi1822 Offload Cards (for BMSs with SDI 3.0)

Scenario

If the BMS uses SDI 3.0 cards, you need to install the Hi1822 driver on the VM. The following uses CentOS 7.6 as an example.

Prerequisites

- You have logged in to the VM.
- You have obtained the Hi1822 driver installation package and management software and uploaded them to the VM.

  Perform the following operations to obtain the package.

  a. Download the .zip package as instructed in **Software**.

  b. The following uses **uNIC_GuestOS_Driver_BM_2.21.8.B070.tar.gz** as an example to describe how to obtain the required installation package.

     Download and decompress the **uNIC_GuestOS_Driver_BM_2.21.8.B070.tar.gz** driver package, and obtain the .rpm package **kmod-hinic-5.0.0.7_3.10.0_957-1.el7.x86_64.rpm** based on the OS type and kernel version.

Procedure

1. Check whether the hinic driver exists.

   rpm -qa | grep hinic

   – If yes, go to **2**.

   – If no, go to **3**.

2. Uninstall the hinic driver.

   rpm -e kmod-hinic

   rmmod hinic

3. Go to the directory where the .rpm installation package is stored and run the following command to install it:

   rpm -ivh kmod-hinic-5.0.0.7_3.10.0_957-1.el7.x86_64.rpm

4. Run the **modprobe hinic** command to load the latest Hi1822 driver.

3.15 (Optional) Installing the IB driver

Scenario

CentOS 7.4 is used as an example.

NOTE

1. The IB driver can be installed only for CentOS 7.3, CentOS 7.4, CentOS 7.6 ARM, RedHat 7.3, RedHat 7.4, SUSE 12 SP3 and Oracle Linux 7.4.
2. You are advised to install the 4.2 or later version.

Prerequisites

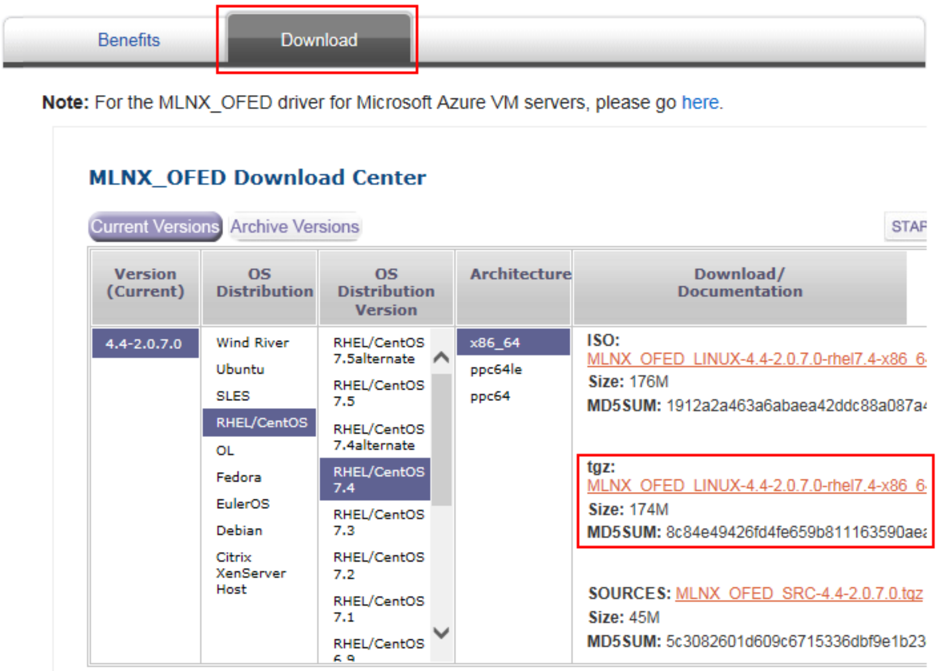
- You have logged in to the VM.
- The required IB driver installation package has been uploaded to the VM.

Procedure

1. Download the OFED package as instructed in **Software**.

   Download the .tgz installation package based on the VM OS and verify the file integrity.

   Take CentOS 7.4 as an example.



Note: For the MLNX_OFED driver for Microsoft Azure VM servers, please go here.

ISO: MLNX_OFED_LINUX-4.4-2.0.7.0-rhel7.4-x86_6
Size: 176M
MD5SUM: 1912a2a463a6abaea42ddc88a087a

tgz: MLNX_OFED_LINUX-4.4-2.0.7.0-rhel7.4-x86_6
Size: 174M
MD5SUM: 8c84e49426fd4fe659b811163590ae

SOURCES: MLNX_OFED_SRC-4.4-2.0.7.0.tgz
Size: 45M
MD5SUM: 5c3082601d609c6715336dbf9e1b23

2. Upload the downloaded OFED installation package to the VM. For details, see **Configuring the VM Environment**.
3. Run the **tar -zxvf** *xxx* command (*xxx* indicates the OFED installation package name) to decompress the package.
4. After the decompression is complete, go to the **MLNX_OFED_LINUX-4.2-1.2.0.0-RHEL7.4-X86_64** folder to install the package.

   ./mlnxofedinstall

```
[root@localhost MLNX_OFED_LINUX-4.2-1.2.0.0-rhel7.4-x86_64]# ./mlnxofedinstall
Logs dir: /tmp/MLNX_OFED_LINUX.1479.logs
General log file: /tmp/MLNX_OFED_LINUX.1479.logs/general.log
Verifying KMP rpms compatibility with target kernel...
Error: One or more required packages for installing MLNX_OFED_LINUX are missing.
Please install the missing packages using your Linux distribution Package Management tool.
Run:
yum install tcl tk
```

5. During the installation, if the dependency package is missing, run the following command to install it:

   yum install tcl tk

6. Run the **./mlnxofedinstall** installation script again.

   If the following information is displayed after a while, the installation is successful:

```
Installation finished successfully.

Preparing...                          ################################# [100%]
Updating / installing...
   1:mlnx-fw-updater-4.2-1.2.0.0              ################################# [100%]

Added 'RUN_FW_UPDATER_ONBOOT=no to /etc/infiniband/openib.conf
...
```

7. After the installation is complete, run the **/etc/init.d/openibd restart** command to load the driver.

```
[root@localhost MLNX_OFED_LINUX-4.2-1.2.0.0-rhel7.4-x86_64]# /etc/init.d/openibd restart
Uploading HCA driver:                                [ OK ]
Loading HCA driver and Access Layer:                       [ OK ]
```

3.16 Installing FusionServer/TaiShanServer iDrivers

3.16.1 Making Preparations

1. Determine the .zip driver packages to be used.

   Examples:

   – CentOS 7.6: FusionServer iDriver-CentOS7.6-Driver-V116.zip
   – RHEL 7.3: FusionServer iDriver-RHEL7.3-Driver-V116.zip
   – Ubuntu 16.04: FusionServer iDriver-Ubuntu16.04-Driver-V116.zip
   – EulerOS 2.8 ARM: TaiShanServer iDriver-EulerOS2.8-Driver-V103.zip
   – CentOS 7.6 ARM: TaiShanServer iDriver-CentOS7.6-Driver-V112.zip

2. Obtain the installation packages. (Example for installing V5 server drivers: CentOS 7.6; examples for installing TaiShan server drivers: EulerOS 2.8 ARM and CentOS 7.6 ARM)

   – CentOS 7.6

     Download and decompress the **FusionServer iDriver-CentOS7.6-Driver-V116.zip** driver package to obtain the **onboard_driver_CentOS7.6.iso** file. Decompress **onboard_driver_CentOS7.6.iso** to obtain the **NIC-X710_X722_XL710_XXV710-CentOS7.6-i40e-2.15.9-1-x86_64.rpm**, **RAID-3008IR_3008IT_3408IT_3416IT-CentOS7.6-mpt3sas-27.00.00.00-1-x86_64.rpm**, and **RAID-3004iMR_3108_3408iMR_3416iMR_3508_3516-CentOS7.6-megaraid_sas-07.716.01.00-1-x86_64.rpm** files.

     The **NIC-X710_X722_XL710_XXV710-CentOS7.6-i40e-2.15.9-1-x86_64.rpm**, **RAID-3008IR_3008IT_3408IT_3416IT-CentOS7.6-mpt3sas-27.00.00.00-1-x86_64.rpm**, and **RAID-3004iMR_3108_3408iMR_3416iMR_3508_3516-CentOS7.6-megaraid_sas-07.716.01.00-1-x86_64.rpm** files are used to install LOM drivers, mpt3 drivers, and megaraid_sas drivers of V5 servers, respectively.

- EulerOS 2.8 ARM

  Download and decompress the **TaiShanServer iDriver-EulerOS2.8-Driver-V103.zip** driver package to obtain **onboard_driver_EulerOS2.8.iso**. Decompress **onboard_driver_EulerOS2.8.iso** to **obtain NIC-IN200-EulerOS2.8-hinic-2.4.1.0-aarch64.rpm**, which is used to install the Hi1822 standard card driver. However, the Hi1822 driver has been installed in **Installing the Hi1822 Driver**. Therefore, you can skip this step.

- CentOS 7.6 ARM

  Download and decompress the **TaiShanServer iDriver-CentOS7.6-Driver-V112.zip** driver package to obtain **onboard_driver_CentOS7.6.iso**. Decompress the **onboard_driver_CentOS7.6.iso** file to obtain the **RAID-3108_3408iMR_3416iMR_3508_3516-CentOS7.6-megaraid_sas-07.716.01.00-aarch64.rpm** and **NIC-Hi1822-CentOS7.6-hinic-3.9.0.8-aarch64.rpm** files for installing the megaraid_sas and Hi1822 drivers. The Hi1822 (hinic) driver has been installed in **Installing the Hi1822 Driver**. Therefore, you do not need to install it again.

3.16.2 Installing the LOM Driver

Scenario

If the BMS uses an X722 LOM, install the LOM driver on the VM.

NOTE

This section uses CentOS 7.6 as an example to describe how to install the LOM driver. The procedure is also applicable to other OSs.

Procedure

1. Upload the **NIC-X710_X722_XL710_XXV710-CentOS7.6-i40e-2.15.9-1-x86_64.rpm** package obtained in **Making Preparations** to the VM.
2. Go to the directory where the .rpm installation package is stored and run the following command to install it:

   rpm -ivh NIC-X710_X722_XL710_XXV710-CentOS7.6-i40e-2.15.9-1-x86_64.rpm

```
[root@localhost i40e]# rpm -ivh NIC-X710_X722_XL710_XXV710-CentOS7.6-i40e-2.15.9-1-
x86_64.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:i40e-2.15.9-1                    ################################# [100%]
original pci.ids saved in /usr/local/share/i40e
Updating initrd...
Using dracut to update initrd...
Successfully updated initrd.
[root@localhost i40e]#
```

3. After the installation is complete, run the **rpm -qa | grep i40e** command. The installation is successful if information similar to the following is displayed:

```
i40e-2.15.9-1.x86_64
```

3.16.3 Installing the mpt3 Driver

Scenario

If the BMS uses 3108 or 3008 RAID cards, you need to install the mpt3sas driver on the VM.

Procedure

1. Upload the **RAID-3008IR_3008IT_3408IT_3416IT-CentOS7.6-mpt3sas-27.00.00.00-1-x86_64.rpm** package obtained in **Making Preparations** to the VM.
2. Install the mpt3 driver.
   a. Go to the directory where the .rpm installation package is stored and run the following command to install it:

      rpm -ivh RAID-3008IR_3008IT_3408IT_3416IT-CentOS7.6-mpt3sas-27.00.00.00-1-x86_64.rpm

      ```
      [root@localhost mpt3-82599]# rpm -ivh RAID-3008IR_3008IT_3408IT_3416IT-CentOS7.6-
      mpt3sas-27.00.00.00-1-x86_64.rpm
      Preparing...                          ################################# [100%]
      Updating / installing...
         1:kmod-mpt3sas-27.00.00.00_el7.6-1     #################################
      [100%]
      [root@localhost mpt3-82599]#
      ```

   b. Run the **dracut -f** command to update the kernel:
3. After the installation is complete, run the **rpm -qa | grep mpt3** command. The installation is successful if the following information is displayed:

   ```
   kmod-mpt3sas-27.00.00.00_el7.6-1.x86_64
   ```

3.16.4 Installing the megaraid_sas Driver

Scenario

If the BMS uses 3408 or 3508 RAID cards, you need to install the megaraid_sas driver on the VM.

Procedure

1. Upload the **RAID-3004iMR_3108_3408iMR_3416iMR_3508_3516-CentOS7.6-megaraid_sas-07.716.01.00-1-x86_64.rpm** package obtained in **Making Preparations** to the VM.
2. Install the megaraid_sas driver.
   a. Go to the directory where the .rpm installation package is stored and run the following commands to install it:

      rpm -ivh RAID-3004iMR_3108_3408iMR_3416iMR_3508_3516-CentOS7.6-megaraid_sas-07.716.01.00-1-x86_64.rpm

      ```
      [root@localhost 3408]# rpm -ivh RAID-3004iMR_3108_3408iMR_3416iMR_3508_3516-
      CentOS7.6-megaraid_sas-07.716.01.00-1-x86_64.rpm
      Preparing...                     ##################################### [100%]
      Updating / installing...
         1:kmod-megaraid_sas-07.716.01.00_el#####################################
      [100%]
      [root@localhost 3408]#
      ```

   b. Run the **dracut -f** command to update the kernel:

3. After the installation is complete, run the **rpm -qa | grep raid** command to check whether the installation is successful.

```
kmod-megaraid_sas-07.716.01.00-1-x86_64
```

3.17 (Optional) Installing the Multipath Software

Scenario

Install the multipath software when FC storage needs to be mounted to servers using HBA cards.

Procedure

1. Install the multipath software by following the operations in *OceanStor UltraPath for Linux xxx User Guide*.

   NOTE

   Obtain the software and documents of the required version. For details, see **Software**.

2. Run **reboot** to restart the VM and make the software take effect.
3. Check the software version.

   upadmin show version

3.18 Performing Security Configuration

3.18.1 Modifying SSH Configuration Items

Scenario

You can select the BMS login mode or account type. If special configuration is required, you can perform the operations in this section.

Procedure

1. To improve security of BMSs, disable remote login using the passwords and retain only the certificate login mode.
   - Check whether the **/etc/cloud/cloud.cfg** file contains parameter **ssh_pwauth** and its value is **false**. If not, add the parameter and/or set its value to **false**. This ensures that passwords cannot be used when you log in to the BMSs using Xshell.
   - Check whether the **/etc/ssh/sshd_config** file contains parameter **ChallengeResponseAuthentication** and its value is **no**. If not, add the parameter and/or set its value to **no**. This ensures that passwords cannot be entered using the keyboard inactive method for logging in to the BMSs using Xshell.
2. Enable remote login as user **root** and SSH permissions of user **root**.

⚠ CAUTION

This operation may cause risks. Exercise caution before performing this operation.

a. Modify the Cloud-Init configuration file **/etc/cloud/cloud.cfg**.

   Take CentOS 6.7 as an example. Modify the following parameters:

```
users:
  - name: root
    lock_passwd: false

disable_root: 0
ssh_pwauth: 1
```

   Parameter description:

   - If the value of **lock_passwd** is **false**, user passwords are not locked.
   - **disable_root** specifies whether to disable remote SSH login as user **root**. Set the value to **0**, indicating that the remote SSH login as user **root** is enabled. (In some OSs, value **true** indicates disabled but **false** indicates enabled.)
   - **ssh_pwauth** specifies whether to support SSH password login. Set the value to **1**, indicating that SSH password login is supported.

b. Open the **/etc/ssh/sshd_config** file.

   vi /etc/ssh/sshd_config

   Change the value of **PasswordAuthentication** to **yes** and the value of **UseDNS** to **no**.

   NOTE

   - For SUSE and openSUSE, set the value of **PasswordAuthentication** and of **ChallengeResponseAuthentication** in the **sshd_config** file to **yes**.
   - For Ubuntu OSs, set the value of **PermitRootLogin** to **yes**.

c. Modify the **shadow** file to lock the initial password of user **root** in the image template.

   i. Open the **/etc/shadow** file using the vi editor.

      vi /etc/shadow

      Add **!!** to the password hash value of user **root**. The modified configuration file is as follows:

```
# cat /etc/shadow | grep root
 root:!!$6$SphQRPXu$Nvg6izXbhDPrcY3j1vRiHaQFVRpNiV3HD/
bjDgnZrACOWPXwJahx78iaut1IigIUrwavVGSYQ1JOIw.rDlVh7.:17376:0:99999:7:::
```

   ii. Press **Esc** and enter **:wq** to save and exit the file.

      NOTE

      For Ubuntu, delete the user created during OS installation. For example, if the created user is **ubuntu**, run **userdel -rf ubuntu** to delete the user.

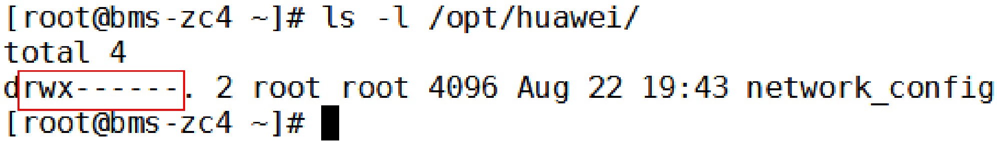
3.18.2 (Optional) Modifying the Network Script Permission

Scenario

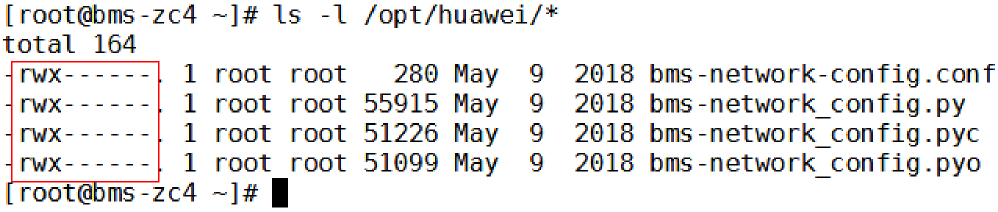
After installing bms-network-config for an image of a centralized BMS, you need to modify the network script permission to meet security requirements.

Procedure

1. Run **chmod 700 -R /opt/huawei/** to change the permission.
2. Run **ls -l /opt/huawei/** and **ls -l /opt/huawei/*** to check the permission.



```
[root@bms-zc4 ~]# ls -l /opt/huawei/
total 4
drwx------. 2 root root 4096 Aug 22 19:43 network_config
[root@bms-zc4 ~]#
```



```
[root@bms-zc4 ~]# ls -l /opt/huawei/*
total 164
-rwx------. 1 root root   280 May  9  2018 bms-network-config.conf
-rwx------. 1 root root 55915 May  9  2018 bms-network_config.py
-rwx------. 1 root root 51226 May  9  2018 bms-network_config.pyc
-rwx------. 1 root root 51099 May  9  2018 bms-network_config.pyo
[root@bms-zc4 ~]#
```

3.18.3 (Optional) Modifying the /etc/motd Configuration Item

Scenario

You can modify the **motd** configuration item to remind users of changing passwords at their first login to BMSs to improve security.

Procedure

1. Create or open **/etc/motd** using the vi editor.

   vi /etc/motd

   NOTE

   /etc/motd is used to store prompts displayed after you log in to Linux OSs.
2. Press **I** to enter editing mode and add the content to be displayed at the end of the file.
3. Press **Esc** and enter **:wq** to save and exit the file.

3.18.4 Modifying Historical Record Configuration Items

Scenario

Modify the **/etc/profile.d/history.sh** configuration file to sort historical records by date and time. A maximum of 1000 historical records can be stored.

NOTE

This method applies to all OSs except EulerOS.

Procedure

1. Open the **/etc/profile.d/history.sh** file.

   vi /etc/profile.d/history.sh

2. Press **i** to enter editing mode and add the following content at the end of the file:

   ```
   export HISTTIMEFORMAT="%F %T `whoami` "
   export HISTSIZE=1000
   ```

3. Press **Esc** and enter **:wq** to save and exit the file.

3.18.5 Optimizing the udev Configuration

Delete the **/etc/udev/rules.d/70-persistent-net.rules** file.

3.18.6 Optimizing SELinux

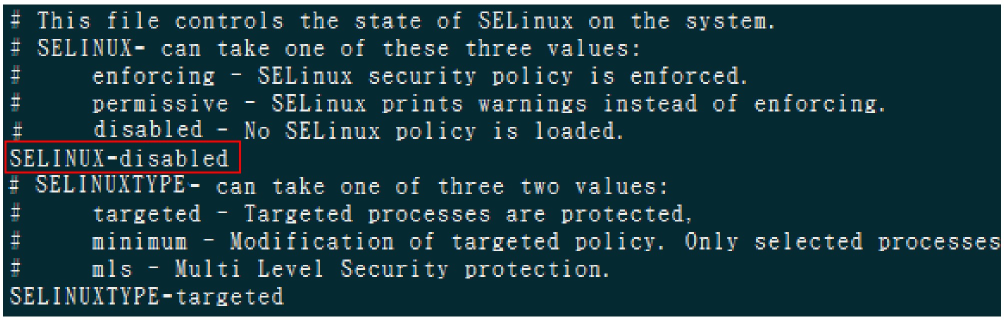
NOTE

SUSE does not have the SELinux configuration file. Skip this configuration item.

1. Open the **/etc/selinux/config** file.

   vi /etc/selinux/config

2. Press **I** to enter editing mode and set the value of **SELINUX** to **disabled**.



```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

3. Press **Esc** and enter **:wq** to save and exit the file.

3.18.7 Uninstalling denyhosts

Check whether denyhosts has been installed. If it is installed, uninstall it. This is because denyhosts may cause functional problems, for example, SSH login failure.

Run the following commands to query and uninstall denyhosts:

rpm -qa | grep denyhosts

rpm -e denyhosts

3.18.8 (Optional) Setting Automatic Hostname Update

NOTE

After the restart, the hostname is restored to the console or the previous one. **localhost** in the **/etc/hosts** file is restored to the console name or the previous name. To prevent this problem, change the console name to be the same as the hostname.

Check methods

- In the **/etc/cloud/cloud.cfg** file, check whether the **update_hostname** and **manage_etc_hosts** parameters are commented out or whether the value of **preserve_hostname** is **true**.
- In Network Manager, check whether the value of **hostname-mode** in **/etc/NetworkManager/NetworkManager.conf** is set to **none**.
- Check whether the value of **enable_preserve_hostname** in the **/opt/huawei/network_config/bms-network-config.conf** file is **True**.

Commands

- Centralized BMS gateway

# Avoid the network from changing the hostname.

sed -i 's/enable_preserve_hostname = False/enable_preserve_hostname = True/g' /opt/huawei/network_config/bms-network-config.conf

# Avoid **/etc/hosts** from being modified after restart.

sed -i '/manage_etc_hosts/s/^/#/g' /etc/cloud/cloud.cfg

#Avoid hostname updates.

sed -i '/- update_hostname/s/^/#/g' /etc/cloud/cloud.cfg

- Distributed BMS gateway

# Avoid **/etc/hosts** from being modified after restart.

sed -i '/manage_etc_hosts/s/^/#/g' /etc/cloud/cloud.cfg

#Avoid hostname updates.

sed -i '/- update_hostname/s/^/#/g' /etc/cloud/cloud.cfg

# Avoid NetworkManager from changing the name.

sed -i '/\[main\]/a\hostname-mode=none' /etc/NetworkManager/NetworkManager.conf

3.18.9 (Optional) Installing Common O&M Tools

NOTE

Common built-in software required for O&M is continuously updated. Common software is as follows:

gcc, perl, python2-pip, strace, sysstat, tcpdump, vim-common, vim-enhanced, vim-filesystem, wget, and telnet

CentOS and Red Hat can connect to the Internet, and the software can be installed using the yum source. The following are commands for installing the software:

yum install gcc

yum install perl

yum install python2-pip

yum install strace

yum install sysstat

yum install tcpdump

yum install vim-common

yum install vim-enhanced

yum install vim-filesystem

yum install wget

yum install telnet

3.18.10 (Optional) Setting the Password Validity Period

1. Check the password validity period.

   vi /etc/login.defs

   The value of parameter **PASS_MAX_DAYS** is the password validity period.

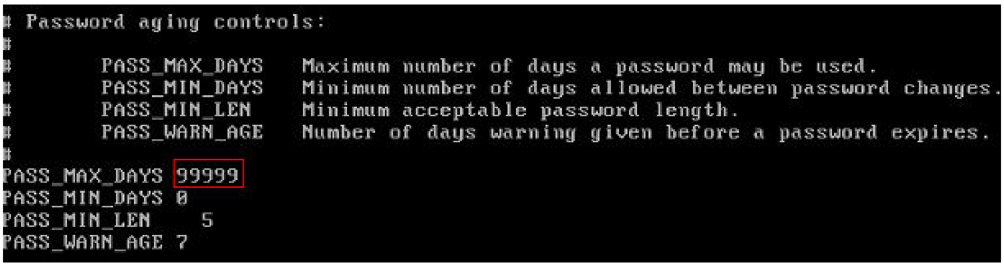
2. Change the value of parameter **PASS_MAX_DAYS**.

   chage -M *99999 user_name*

   99999 is the password validity period, and *user_name* is a system user.

   Configure the password validity period as needed and change it on a regular basis.

3. Run **vi /etc/login.defs** to verify that the configuration has taken effect.



```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_MIN_LEN     5
PASS_WARN_AGE 7
```

3.19 Configuring Remote Login to a BMS

To enable BMS remote login, configure the OS to ensure that it can be displayed on the serial port. This section provides guidance for administrators on how to configure the serial port during image creation to enable users to log in to the BMS remotely. The configuration method varies depending on the OS.

3.19.1 x86: Oracle Linux 7.3/Oracle Linux 7.4/Red Hat 7/CentOS 7.2/CentOS 7.4/CentOS 7.5/CentOS 7.6

NOTE

This section uses the configuration files of CentOS 7.2 as an example. Configuration files of other types of OSs may be different.

1. Use the vi editor to open the **/etc/sysconfig/grub** file and add **consoleblank=600 console=tty0 console=ttyS0,115200n8** after the **GRUB_CMDLINE_LINUX** field.

```
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="crashkernel=512M rhgb quiet consoleblank=600 console=tty0
console=ttyS0,115200n8"
GRUB_DISABLE_RECOVERY="true"
~
~
```

2. Run the following commands to update the configuration:

   stty -F /dev/ttyS0 speed 115200

   grub2-mkconfig -o /boot/grub2/grub.cfg

   systemctl enable serial-getty@ttyS0

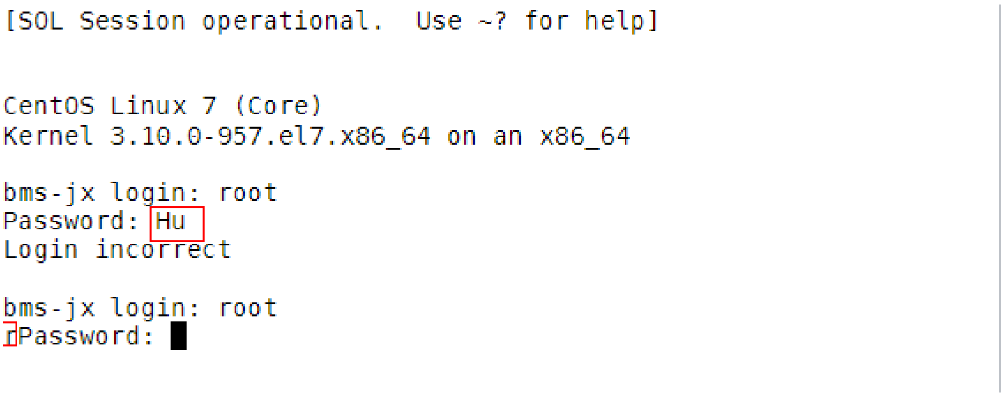
3. To enable user **root** to log in to the BMS through a serial port, add **ttyS0** to the end of the security configuration file **/etc/securetty**.

```
vc/1
...
vc/9
vc/10
vc/11
tty1
...
tty9
tty10
tty11
ttyS0
"securetty" 39L, 221C
```

NOTE

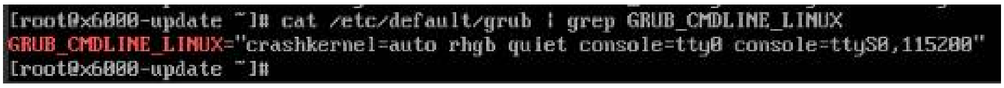
For CentOS 7, if garbled characters are displayed over the serial port, as shown in **Figure 3-1**, perform the following operations:

Figure 3-1 Garbled characters during login



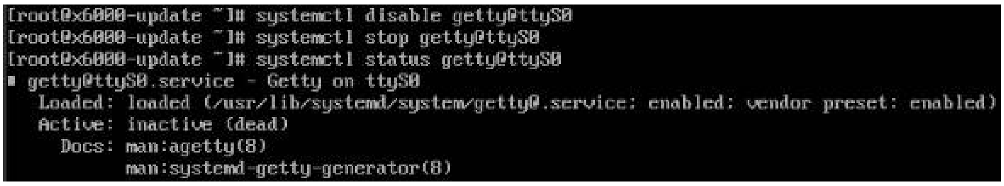
```
[SOL Session operational.  Use ~? for help]


CentOS Linux 7 (Core)
Kernel 3.10.0-957.el7.x86_64 on an x86_64

bms-jx login: root
Password: Hu
Login incorrect

bms-jx login: root
rPassword:
```

a. Use the vi editor to open the **/etc/default/grub** file and add **115200** to the end of the **GRUB_CMDLINE_LINUX** field.



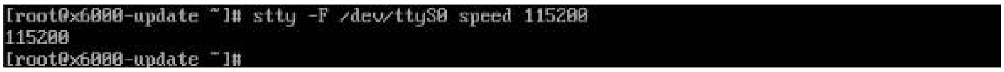
```
[root@x6000-update ~]# cat /etc/default/grub | grep GRUB_CMDLINE_LINUX
GRUB_CMDLINE_LINUX="crashkernel=auto rhgb quiet console=tty0 console=ttyS0,115200"
[root@x6000-update ~]#
```

b. Run the **systemctl disable getty@ttyS0** and **systemctl stop getty@ttyS0** commands to change the getty@ttyS0 service status as follows.



```
[root@x6000-update ~]# systemctl disable getty@ttyS0
[root@x6000-update ~]# systemctl stop getty@ttyS0
[root@x6000-update ~]# systemctl status getty@ttyS0
■ getty@ttyS0.service - Getty on ttyS0
   Loaded: loaded (/usr/lib/systemd/system/getty@.service; enabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:agetty(8)
           man:systemd-getty-generator(8)
```

c. Run the **stty -F /dev/ttyS0 speed 115200** command to change the baud speed to **115200**.

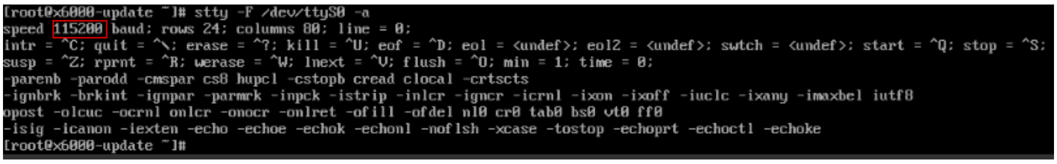


```
[root@x6000-update ~]# stty -F /dev/ttyS0 speed 115200
115200
[root@x6000-update ~]#
```

d. Run the **grub2-mkconfig -o /boot/grub2/grub.cfg** command again. (The directory of the **grub.cfg** file is an example only.)

e. Run the following command to check whether the baud speed is **115200**:

stty -F /dev/ttyS0 -a



```
[root@x6000-update ~]# stty -F /dev/ttyS0 -a
speed 115200 baud; rows 24; columns 80; line = 0;
intr = ^C; quit = ^\; erase = ^?; kill = ^U; eof = ^D; eol = <undef>; eol2 = <undef>; swtch = <undef>; start = ^Q; stop = ^S;
susp = ^Z; rprnt = ^R; werase = ^W; lnext = ^V; flush = ^O; min = 1; time = 0;
-parenb -parodd -cmspar cs8 hupcl -cstopb cread clocal -crtscts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr -icrnl -ixon -ixoff -iuclc -ixany -imaxbel iutf8
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0 ff0
-isig -icanon -iexten -echo -echoe -echok -echonl -noflsh -xcase -tostop -echoprt -echoctl -echoke
[root@x6000-update ~]#
```

3.19.2 x86: Oracle Linux 6 series/Red Hat 6 series/CentOS 6

NOTE

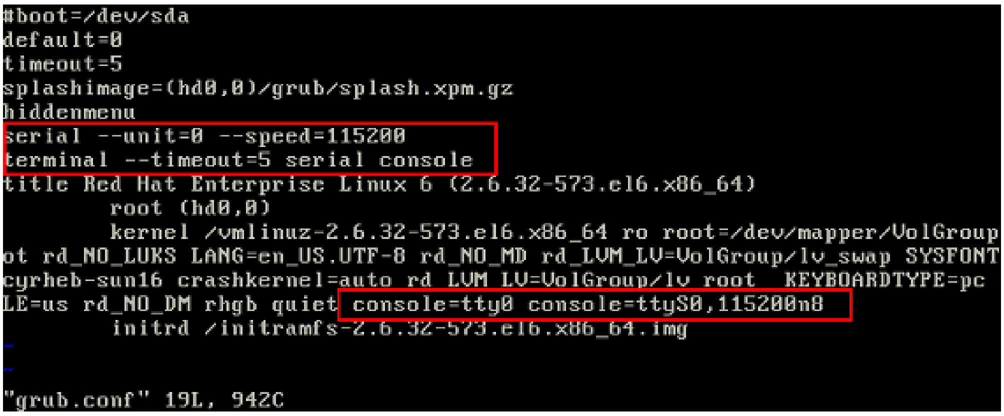
This section uses the configuration files of Red Hat 6.7 as an example. Configuration files of other types of OSs may be different.

1. Use the vi editor to open the **/boot/grub/grub.conf** file, locate **hiddenmenu**, and add the following information after **hiddenmenu**:

   ```
   serial --unit=0 --speed=115200
   terminal --timeout=5 serial console
   ```

   Add the following information to the end of the line that contains **kernel**:

   ```
   consoleblank=600 console=tty0 console=ttyS0,115200n8
   ```

   ```
   #boot=/dev/sda
   default=0
   timeout=5
   splashimage=(hd0,0)/grub/splash.xpm.gz
   hiddenmenu
   serial --unit=0 --speed=115200
   terminal --timeout=5 serial console
   title Red Hat Enterprise Linux 6 (2.6.32-573.el6.x86_64)
           root (hd0,0)
           kernel /vmlinuz-2.6.32-573.el6.x86_64 ro root=/dev/mapper/VolGroup
   ot rd_NO_LUKS LANG=en_US.UTF-8 rd_NO_MD rd_LVM_LV=VolGroup/lv_swap SYSFONT
   cyrheb-sun16 crashkernel=auto rd_LVM_LV=VolGroup/lv_root  KEYBOARDTYPE=pc
   LE=us rd_NO_DM rhgb quiet console=tty0 console=ttyS0,115200n8
           initrd /initramfs-2.6.32-573.el6.x86_64.img
   ~
   ~
   "grub.conf" 19L, 942C
   ```

2. To enable user **root** to log in to the BMS through a serial port, add **ttyS0** to the end of the security configuration file **/etc/securetty**.

3.19.3 x86: SUSE 11 SP4

1. Use the vi editor to open the **/etc/inittab** file and add the following information to the end of the file:

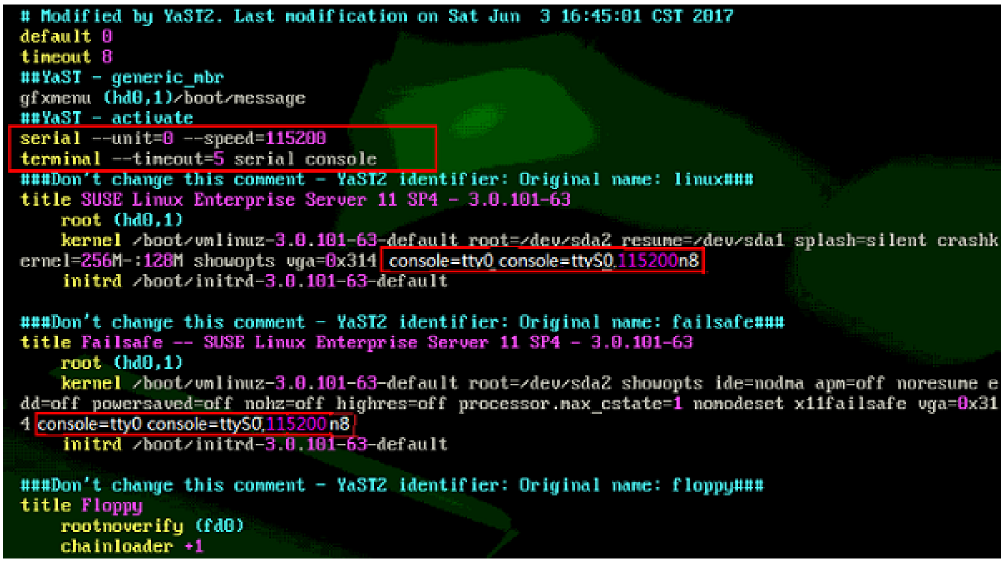
   ```
   S0:12345:respawn:/sbin/agetty -L 115200 ttyS0
   ```

2. Modify the **/boot/grub/menu.lst** file and add the following information after **gfxmenu (hd0,1)/boot/message**:

   ```
   serial --unit=0 --speed=115200
   terminal --timeout=5 serial console
   ```

   Add the following information to the rows that contain kernel:

   ```
   consoleblank=600 console=tty0 console=ttyS0,115200n8
   ```

   ```
   # Modified by YaST2. Last modification on Sat Jun  3 16:45:01 CST 2017
   default 0
   timeout 8
   ##YaST - generic_mbr
   gfxmenu (hd0,1)/boot/message
   ##YaST - activate
   serial --unit=0 --speed=115200
   terminal --timeout=5 serial console
   ###Don't change this comment - YaST2 identifier: Original name: linux###
   title SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63
       root (hd0,1)
       kernel /boot/vmlinuz-3.0.101-63-default root=/dev/sda2 resume=/dev/sda1 splash=silent crashk
   ernel=256M-:128M showopts vga=0x314 console=tty0 console=ttyS0,115200n8
       initrd /boot/initrd-3.0.101-63-default

   ###Don't change this comment - YaST2 identifier: Original name: failsafe###
   title Failsafe -- SUSE Linux Enterprise Server 11 SP4 - 3.0.101-63
       root (hd0,1)
       kernel /boot/vmlinuz-3.0.101-63-default root=/dev/sda2 showopts ide=nodma apm=off noresume e
   dd=off powersaved=off nohz=off highres=off processor.max_cstate=1 nomodeset x11failsafe vga=0x31
   4 console=tty0 console=ttyS0,115200n8
       initrd /boot/initrd-3.0.101-63-default

   ###Don't change this comment - YaST2 identifier: Original name: floppy###
   title Floppy
       rootnoverify (fd0)
       chainloader +1
   ```

3. To enable user **root** to log in to the BMS through a serial port, add **ttyS0** to the end of the security configuration file **/etc/securetty**.

3.19.4 ARM: CentOS 7

1. Use the vi editor to open the **/boot/efi/EFI/centos** file, locate the line **linux / vmlinuz-***xxx***.aarch64 root=/dev/mapper/cla-root ro crashkernel=auto rd.lvm.lv=cla/root rd.lvm.lv=cla/swap LANG=en_US.UTF-8**, and add the following information to the end of the line:
   ```
   consoleblank=600 console=tty0 console=ttyAMA0,115200
   ```
2. To allow user **root** to log in to the BMS using a serial port, check whether the **/etc/securetty** configuration file contains **ttyAMA0**. If not, add it.

3.19.5 x86: SUSE 12/SUSE 15/CentOS 7.3/EulerOS/OpenEuler/ Oracle Linux 7.2

> **NOTE**
>
> This section uses the configuration files of SUSE 12 SP1 as an example. Configuration files of other types of OSs may be different.

1. Use the vi editor to open the **/etc/default/grub** file and add the following information after the **GRUB_CMDLINE_LINUX** field:
   ```
   consoleblank=600 console=tty0 console=ttyS0,115200
   ```
2. Run the following commands to update the configuration:

   stty -F /dev/ttyS0 speed 115200

   grub2-mkconfig -o /boot/grub2/grub.cfg

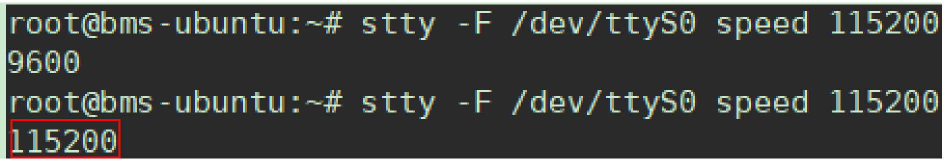
   systemctl enable serial-getty@ttyS0
3. To enable user **root** to log in to the BMS through a serial port, add **ttyS0** to the end of the security configuration file **/etc/securetty**.

3.19.6 ARM: EulerOS/OpenEuler

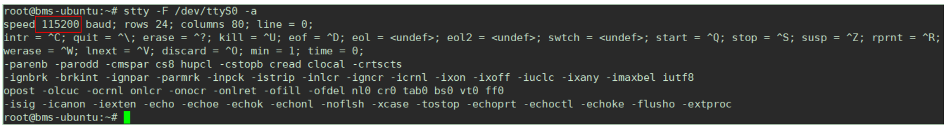
1. Use the vi editor to open the **/boot/EFI/grub2/grub.cfg** file, locate the **linux/ vmlinuz-xxx.aarch64 root=/** line, and add the following information to the end of the line:
   ```
   consoleblank=600 console=tty0 console=ttyAMA0,115200
   ```
2. To allow user **root** to log in to the BMS using a serial port, check whether the **/etc/securetty** configuration file contains **ttyAMA0**. If not, add it.

3.19.7 x86: Ubuntu 16.04/Ubuntu 18.04

1. Use the vi editor to open the **/etc/default/grub** file and add the following information after the **GRUB_CMDLINE_LINUX** field:
   ```
   consoleblank=600 console=tty0 console=ttyS0,115200
   ```
2. Run the following commands to update the configuration:
   - Run the **stty -F /dev/ttyS0 speed 115200** command to change the baud speed to **115200**.

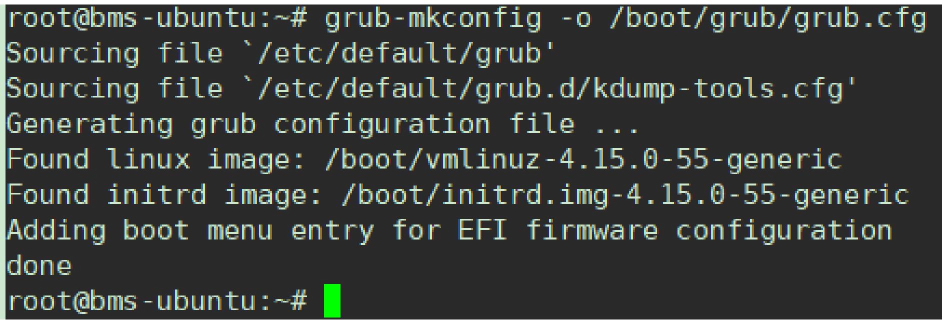
     

     ```
     root@bms-ubuntu:~# stty -F /dev/ttyS0 speed 115200
     9600
     root@bms-ubuntu:~# stty -F /dev/ttyS0 speed 115200
     115200
     ```
   - Run the **stty -F /dev/ttyS0 -a** command to check whether the baud speed is **115200**.



```
root@bms-ubuntu:~# stty -F /dev/ttyS0 -a
speed 115200 baud; rows 24; columns 80; line = 0;
intr = ^C; quit = ^\; erase = ^?; kill = ^U; eof = ^D; eol = <undef>; eol2 = <undef>; swtch = <undef>; start = ^Q; stop = ^S; susp = ^Z; rprnt = ^R;
werase = ^W; lnext = ^V; discard = ^O; min = 1; time = 0;
-parenb -parodd -cmspar cs8 hupcl -cstopb cread clocal -crtscts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr -icrnl -ixon -ixoff -iuclc -ixany -imaxbel iutf8
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0 ff0
-isig -icanon -iexten -echo -echoe -echok -echonl -noflsh -xcase -tostop -echoprt -echoctl -echoke -flusho -extproc
root@bms-ubuntu:~#
```

- Run the **grub-mkconfig -o /boot/grub/grub.cfg** command.

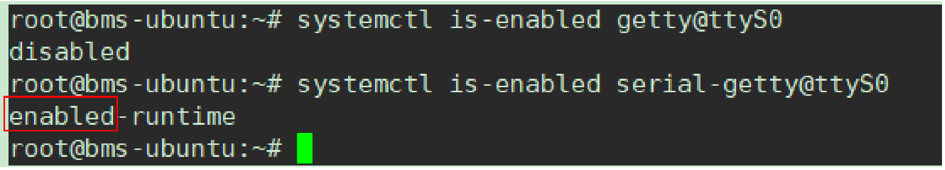


```
root@bms-ubuntu:~# grub-mkconfig -o /boot/grub/grub.cfg
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/kdump-tools.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-4.15.0-55-generic
Found initrd image: /boot/initrd.img-4.15.0-55-generic
Adding boot menu entry for EFI firmware configuration
done
root@bms-ubuntu:~#
```

3. Use the vi editor to open the **/etc/rc.local** file and add the following content to the file:

```
systemctl stop getty@ttyS0
```

4. To enable user **root** to log in to the BMS through a serial port, add **ttyS0** to the end of the security configuration file **/etc/securetty**.
5. Run the **systemctl is-enabled serial-getty@ttyS0** command to check whether serial-getty@ttyS0 is set to automatically start upon system startup.



```
root@bms-ubuntu:~# systemctl is-enabled getty@ttyS0
disabled
root@bms-ubuntu:~# systemctl is-enabled serial-getty@ttyS0
enabled-runtime
root@bms-ubuntu:~#
```

3.19.8 Arm: Ubuntu 16.04/Ubuntu 18.04

1. Use the vi editor to open the **/etc/default/grub** file and modify parameters as follows:
   - Set **GRUB_CMDLINE_LINUX** to **consoleblank=600 console=tty0 console=ttyAMA0,115200**.
   - Set **GRUB_TERMINAL** to **serial**.
   - Set **GRUB_SERIAL_COMMAND** to **serial --speed=115200 --unit=0 --word=8 --parity=no --stop=1**.

   Run the following command:

   sudo update-grub2
2. To enable user **root** to log in to the BMS through a serial port, add **ttyS0** to the end of the security configuration file **/etc/securetty**.

   For x86, check whether **ttyS0** is contained in the file. For ARM64, check whether **ttyAMA0** is contained in the file. If they are not, add them.

3.19.9 x86: Ubuntu 14.04/Debian

1. Use the vi editor to open the **/etc/default/grub** file and add the following information after the **GRUB_CMDLINE_LINUX** field:

```
consoleblank=600 console=tty0 console=ttyS0,115200
```

2. Run the following commands to update the configuration:

   stty -F /dev/ttyS0 speed 115200

   grub-mkconfig -o /boot/grub/grub.cfg

3. Create the **/etc/init/ttyS0.conf** file and use the vi editor to modify the file as follows:

```
start on stopped rc RUNLEVEL=[12345]
stop on runlevel [!12345]
respawn
exec /sbin/getty -L 115200 ttyS0 vt102
```

4. Run the following command to start ttyS0:

   sudo start ttyS0

5. To allow user **root** to log in to the BMS using a serial port, modify the security configuration file. Add **ttyS0** to the end of the **/etc/securetty** file.

3.20 Configuring the Root Partition to Be Automatically Extended

3.20.1 Overview

You can install growpart to automatically extend the root partition. For SUSE, growpart is installed by default. However, for SUSE 11 SP4, you need to install growpart with an earlier version to replace the default one. For other SUSE distributions, you do not need to install growpart. For Ubuntu, growpart is installed by default and the version meets requirements. Therefore, you do not need to install growpart.

NOTE

If the boot mode is UEFI (for example, it is UEFI for Arm), run the **yum install gdisk** command to install gdisk.

3.20.2 CentOS 6/RedHat 6

NOTE

For CentOS 6 and Red Hat 6, you need to install cloud-init, cloud-utils-growpart, and dracut-modules-growroot. Cloud-Init has been installed in **Installing Cloud-Init**.

This section uses CentOS 6.9 as an example to describe how to install them.

1. Check whether cloud-init, cloud-utils-growpart, and dracut-modules-growroot have been installed. If no, perform the following steps to install them.

```
[root@localhost ~]# rpm -qa | grep cloud-init
cloud-init-0.7.5-10.el6.centos.2.x86_64
[root@localhost ~]# rpm -qa | grep growpart
[root@localhost ~]# rpm -qa | grep growroot
[root@localhost ~]#
```

2. Download cloud-utils-growpart-*0.27-10.el6.x86_64*.rpm and upload it to the VM as instructed in **Upload Required Software Packages**.

   You can download the package from:

   https://dl.fedoraproject.org/pub/epel/

3. Run the following command to install cloud-utils-growpart:

   rpm -ivh *cloud-utils-growpart-0.27-10.el6.x86_64.rpm*

   ```
   [root@localhost redhat]# rpm -ivh cloud-utils-growpart-0.27-10.el6.x86_64.rpm
   Preparing...                ################################ [100%]
      1:cloud-utils-growpart   ################################ [100%]
   [root@localhost redhat]#
   ```

4. Install dracut-modules-growroot.
   a. Run the following command:

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

   b. Run the **yum install dracut-modules-growroot** command to install dracut-modules-growroot online.

      Enter **y** when the message **Is this ok [y/N]** is displayed.

   c. Run the **dracut -f** command to update the kernel.
5. Run the commands in 1 again to check whether cloud-init, cloud-utils-growpart and dracut-modules-growroot are successfully installed.

3.20.3 CentOS 7/RedHat 7/Oracle Linux 7

NOTE

CentOS 7, RedHat 7, and Oracle Linux 7 use the 3.10 (>3.8) kernel. Therefore, you do not need to install dracut-modules-growroot. You only need to install cloud-init and cloud-utils-growpart. Cloud-Init has been installed in **Installing Cloud-Init**.

This section uses CentOS 7.3 as an example to describe how to install them.

1. Check whether cloud-init and cloud-utils-growpart have been installed. If no, perform the following steps to install them.

   ```
   [root@localhost ~]# rpm -qa | grep cloud-init
   cloud-init-0.7.5-10.el7.centos.1.x86_64
   [root@localhost ~]# rpm -qa | grep growpart
   [root@localhost ~]#
   ```

2. Run the following **yum** command to install cloud-utils-growpart online.

   yum install cloud-utils-growpart

3. Check whether cloud-utils-growpart is installed successfully.

   ```
   [root@localhost ~]# rpm -qa | grep growpart
   cloud-utils-growpart-0.29-2.el7.noarch
   ```

3.20.4 CentOS/EulerOS ARM/OpenEuler ARM

NOTE

For CentOS and EulerOS ARM, you need to install cloud-init, cloud-utils-growpart, and gdisk. Cloud-Init has been installed in **Installing Cloud-Init**.

This section uses CentOS 7.6 ARM as an example to describe how to install them.

1. Check whether cloud-init and cloud-utils-growpart have been installed. If no, perform the following steps to install them.

   ```
   [root@localhost ~]# rpm -qa | grep cloud-init
   cloud-init-0.7.5-10.el7.centos.1.x86_64
   [root@localhost ~]# rpm -qa | grep growpart
   [root@localhost ~]#
   ```

2. Run the following **yum** command to install cloud-utils-growpart online.

   yum install cloud-utils-growpart

3. Check whether gdisk is installed.

   rpm -qa | grep gdisk

   ```
   [root@localhost ~]# rpm -qa | grep gdisk
   [root@localhost ~]#
   ```

   If no, run the **yum install gdisk** command to install it.

4. Check whether cloud-utils-growpart and gdisk are installed successfully.

   ```
   [root@localhost ~]# rpm -qa | grep growpart
   cloud-utils-growpart-0.29-2.el7.noarch
   [root@localhost ~]# rpm -qa | grep gdisk
   gdisk-0.8.10-3.el7.x86_64
   ```

3.20.5 EulerOS/OpenEuler

NOTE

For EulerOS, you do not need to install dracut-modules-growroot package. You only need to install cloud-init and cloud-utils-growpart. Cloud-Init has been installed in **Installing Cloud-Init**.

1. Check whether cloud-init and cloud-utils-growpart have been installed. If no, perform the following steps to install them.

   ```
   [root@localhost ~]# rpm -qa | grep cloud-init
   cloud-init-0.7.6-3.x86_64
   [root@localhost ~]# rpm -qa | grep growpart
   [root@localhost ~]#
   ```

2. Download the **cloud-utils-growpart-0.27-10.x86_64.rpm** package (from **http://repo.huaweicloud.com/euler/2.2/os/x86_64/Packages/**), upload the package to the VM, and run the following commands to install it:

   rpm -ivh *cloud-utils-growpart-0.27-10.x86_64.rpm*

   ```
   [root@bms-eulor22 home]# rpm -ivh cloud-utils-growpart-0.27-10.x86_64.rpm
   Preparing...                          ################################# [100%]
   Updating / installing...
      1:cloud-utils-growpart-0.27-10     ################################# [100%]
   ```

   You can also use an ISO file as the local repo source and run the **yum install cloud-utils-growpart** command to install it.

3. Run the commands in **1** again to check whether cloud-utils-growpart is successfully installed.

   ```
   [root@localhost ~]# rpm -qa | grep growpart
   cloud-utils-growpart-0.27-10.x86_64
   ```

3.20.6 Debian

NOTE

For Debian, you only need to install growroot.

1. Run the **apt-get install cloud-initramfs-growroot** command to install growroot.

2. Run the following command to check whether cloud-initramfs-growroot has been installed:

   dpkg -l | grep cloud-initramfs-growroot

   If information similar to the following is displayed, growroot is installed successfully:

   ```
   root@bms:/home/bzqd# dpkg -l | grep cloud-initramfs-growroot
   ii cloud-initrramfs-growroot      0.18.debian5      all      automatically resize the root partition on first
   boot
   ```

3.21 Installing and Upgrading Drivers and Firmware for Ascend BMSs

3.21.1 Installation and Maintenance

3.21.1.1 Before You Start

For Ascend BMSs, install NPU driver 20.2.0.spc300 or later versions. NPU firmware is released with the driver. If you install the NPU driver or firmware again, you can only install a version no earlier than the current one.

To query the NPU name, log in to the OS and run **npu-smi info**.

3.21.1.2 Preparations for Installation

3.21.1.2.1 Obtaining Software Packages

Before the installation, obtain driver and firmware packages based on the OS. **Obtaining Software Packages** describes the details.

Table 3-7 Software packages

Component	OS	Software Package	Execution User
Firmware	EulerOS 2.8/Ubuntu 18.04/ CentOS 7.6/CentOS 8.2/ BC_Linux 7.6/Kylin OS V10SP1/ BC_Linux 7.7 Note: Kylin OS V10SP1 and BC_Linux 7.7 are only supported by NPU driver 21.0.rc1 and later versions.	A800-9000-npu-firmware_x.x.x.run	root
Driver	EulerOS 2.8 (AArch64)	A800-9000-npu-driver_*x.x.x*_euleros2.8-aarch64.run	root
Driver	Ubuntu 18.04 (AArch64)	A800-9000-npu-driver_*x.x.x*_ubuntu18.04-aarch64.run	root
Driver	CentOS 7.6 (AArch64)	A800-9000-npu-driver_*x.x.x*_centos7.6-aarch64-.run	root

Component	OS	Software Package	Execution User
Driver	CentOS 8.2 (AArch64)	A800-9000-npu-driver_*x.x.x*_linux-aarch64.run	root
Driver	BC_Linux 7.6 (AArch64)	A800-9000-npu-driver_*x.x.x*_centos7.6-aarch64-.run A800-9000-npu-driver_x.x.x_linux-aarch64.run	root
Driver	Kylin OS V10SP1 (AArch64) Note: Kylin OS V10SP1 and BC_Linux 7.7 are only supported by NPU driver 21.0.rc1 and later versions.	A800-9000-npu-driver_*x.x.x*_linux-aarch64.run	root
Driver	BC_Linux 7.7 (AArch64) Note: Kylin OS V10SP1 and BC_Linux 7.7 are only supported by NPU driver 21.0.rc1 and later versions.	A800-9000-npu-driver_*x.x.x*_linux-aarch64.run	root

NOTE

- *x.x.x* indicates the version number.
- The **A800-9000-npu-driver**_*x.x.x*_**linux-aarch64.run** package is compatible with all OSs.

Procedure

1. Visit **https://support.huawei.com/enterprise/en/ascend-computing/a800-9000-pid-250702818/software**.

2. Choose a BMS version **A800-9000** *x.x.x*.

Determine the driver/firmware version by referring to **CANN Version Mapping**.

3. Click **Download** next to a software package (for example, **A800-9000-npu-driver**_*x.x.x*_**euleros2.8-aarch64.run**) to download the software package and digital signature file.

3.21.1.2.2 Verifying Software Package Integrity

To prevent a software package from being maliciously tampered with during transmission or storage, download the corresponding digital signature file for integrity verification while downloading the software package.

After software packages are downloaded, verify their PGP digital signatures by following *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software packages. Contact technical support.

Before a software package is used for installation or upgrade, its digital signature needs to be verified by following instructions provided in the signature verification guide to ensure that the software package is not tampered with.

For carrier users, visit **https://support.huawei.com/carrier/digitalSignatureAction**.

For enterprise users, visit **https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054**.

3.21.1.2.3 Checking the OS and Kernel

Table 3-8 and **Table 3-9** list the OSs and kernels required by different driver and firmware packages.

Table 3-8 OS and kernel versions required by binary driver packages

BMS	OS	Kernel	GCC Version
Atlas 800 9000 (AArch64)	Ubuntu 18.04	4.15.0-45-generic Note: If the kernel does not match the OS, install DKMS to compile the driver source code before you install the driver. For details about how to install DKMS, see **Driver Source Code Compilation**.	7.4.0
Atlas 800 9000 (AArch64)	EulerOS 2.8	4.19.36-vhulk1907.1.0.h475	7.3.0
Atlas 800 9000 (AArch64)	CentOS 7.6	4.14.0-115.el7a.0.1.aarch64	-
Atlas 800 9000 (AArch64)	BC_Linux 7.6	4.19	-

Table 3-9 OS and kernel versions required by general driver packages

BMS	OS	Kernel	GCC Version
Atlas 800 9000 (AArch64)	CentOS 8.2	4.18.X Note: The kernel can be upgraded to 5.6.14.	8.3.1
Atlas 800 9000 (AArch64)	BC_Linux 7.6	4.19	-
Atlas 800 9000 (AArch64)	Kylin OS V10SP1 Note: Kylin OS V10SP1 is only supported by NPU driver 21.0.rc1 and later versions.	4.19.90-17.ky10.aarch64	8.3.1-4.5
Atlas 800 9000 (AArch64)	BC_Linux 7.7 Note: BC_Linux 7.7 is only supported by NPU driver 21.0.rc1 and later versions.	4.19.25-203.e17.bclinux.aarch64	4.8.5

1. Check the OS version.

Run the **uname -m && cat /etc/*release** command to query the OS version and architecture.

The OS version and architecture must comply with **Table 3-8** or **Table 3-9**.

2. Check general driver packages.

- Check whether the **make** tool has been installed. Run the **make -v** command. If a **make** tool version is displayed, the **make** tool has been installed.
- Ensure that at least either of the following conditions is met.
  - Dependent tools such as DKMS have been installed. For details about how to install DKMS, see **Driver Source Code Compilation**.
  - The default source code directory (**/lib/modules/`uname -r`/build**) of the kernel exists. Run the **ls /lib/modules/`uname -r`/build** command to check whether the directory exists.
    - If it does, the kernel is automatically used to compile the driver.
    - If it does not, you can provide it during driver installation. For details, see 5.

3. Check the OS kernel version.

Run the **uname -r** command to query the kernel version.

- For a binary driver package, the kernel version must comply with **Table 3-8**. If it does not, perform either of the following operations:
  - Compile the source code again. For details, see **Driver Source Code Compilation**.
  - Check whether the driver package has been installed as instructed in **Check whether the software package has been installed in the OS**. If it has not been installed, upgrade the kernel. If it has been installed, uninstall the driver package and then upgrade the kernel.
- For a general driver package, the kernel version must comply with **Table 3-9**. Otherwise, the driver package may fail to be installed or driver functions may be affected.

4. Check whether NPU driver and firmware packages have ever been installed in the OS.

If you need to upgrade the kernel, ensure that NPU driver and firmware packages have never been installed in the OS. Otherwise, the packages to be used will fail to be started after the kernel is upgraded. You can rectify this issue by referring to **What Do I Do If the Software Package Is Unavailable Because It Is Not Uninstalled When Updating the OS Kernel?** Run the **lsmod|grep drv** command to check whether the packages have been installed.

- If no information is displayed, the packages have never been installed. You can upgrade the kernel without additional actions.
- If driver information is displayed, the software packages have been installed. Uninstall them and then upgrade the kernel. For details, see **Uninstalling the NPU Driver and Firmware**.

3.21.1.2.4 Creating an Execution User

- Installation as the **root** user

  A non-root user is required for executing software. Therefore, you need to create such a user before the installation.
  - If the non-root user is **HwHiAiUser**, the system will specify it as the execution user by default when you install a software package.
  - If the non-root user is not **HwHiAiUser**, you need to specify an execution user by configuring the **--install-username=***username* **--install-usergroup=***usergroup* parameter when installing a software package.
- Installation as a non-root user

  The installation user must be the same as the execution user.
  - If a non-root user already exists, you do not need to create a new one.

    If you want to use a new non-root user, create one and set a password for it by performing the following operations as the **root** user:

    i. Create a non-root user.
    ```
    groupadd usergroup
    useradd -g usergroup-d /home/username -m username
    ```
    ii. Set a password for the user.
    ```
    passwd username
    ```

NOTE

- An execution user is specified for a driver only and will also be applied to firmware. You cannot specify an execution user for firmware separately.
- *username* indicates the username of the non-root user to be created. Replace it with an actual username, for example, **HwHiAiUser**.
- Permission control may cause security risks. You are not advised to add the new user to the **root** user group.
- Do not disable login authentication for the **HwHiAiUser** user.
- The password validity period is 90 days. You can change the password validity period in the **/etc/login.defs** file or by running the **chage** command. For details, see **Configuring Password Aging**.

Configuring Password Aging

For security purposes, run the **chage** command to set the validity period of a password.

The command is as follows:

chage [**-m** *minimum days*] [**-M** *maximum days*] [**-d** *last day*] [**-I** *inactive*] [**-E** *expiration date*] [**-W** *warning days*] *user*

Table 3-10 describes the parameters.

Table 3-10 Password aging

Parameter	Description
-m	Minimum number of days between password changes. **0** indicates that you can change your password at any time.
-M	Maximum number of days during which a password is valid. **-1** will remove checking a password's validity and may cause security risks. You are not advised to set this parameter to **-1** unless extremely necessary.
-d	Date of the last password change.
-I	Number of inactive days after the password expiration before the account is locked.
-E	Date on which the account is locked.
-W	Number of days of warning before a password change is required.
-l	Lists account aging information.

NOTE

- **Table 3-10** lists only common **chage** parameters. You can run the **chage --help** command to learn other **chage** parameters.
- The date is in the format of *YYYY-MM-DD*. For example, **chage -E 2019-12-01 test** indicates that the **test** user will expire on December 1, 2019.
- If *user* is not specified, the settings will be applied to the **root** user by default.

For example, to make the **test** user expire on December 31, 2019, run the following command:

chage -E 2019-12-31 test

3.21.1.3 Installing the Network Script

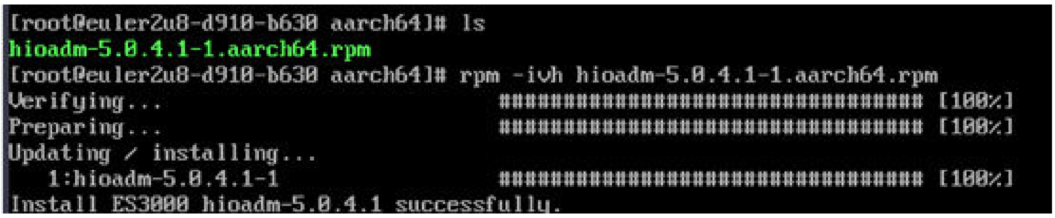
See **Installing bms-network-config**.

3.21.1.4 Installing the NVMe Driver

Obtain the NVMe driver from **https://support.huawei.com/enterprise/en/category/accelerator-components-pid-1548148324389?submodel=software**.

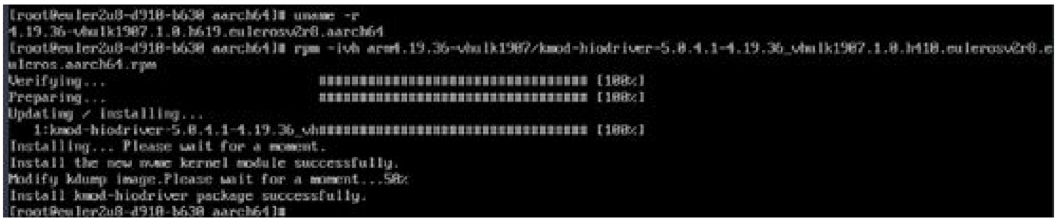
Install hioadm and kmod-hiodriver.

1. Run the **rpm -ivh hioadm-*xxx*.rpm** command to install hioadm.



```
[root@euler2u8-d910-b630 aarch64]# ls
hioadm-5.0.4.1-1.aarch64.rpm
[root@euler2u8-d910-b630 aarch64]# rpm -ivh hioadm-5.0.4.1-1.aarch64.rpm
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
Updating / installing...
   1:hioadm-5.0.4.1-1                 ################################# [100%]
Install ES3000 hioadm-5.0.4.1 successfully.
```

2. Run the **rpm -ivh kmod-hiodriver-*xxx*.rpm** command to install kmod-hiodriver.



```
[root@euler2u8-d910-b630 aarch64]# uname -r
4.19.36-vhulk1907.1.0.h619.eulerosv2r8.aarch64
[root@euler2u8-d910-b630 aarch64]# rpm -ivh arm4.19.36-vhulk1907/kmod-hiodriver-5.0.4.1-4.19.36_vhulk1907.1.0.h410.eulerosv2r8.e
uleros.aarch64.rpm
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
Updating / installing...
   1:kmod-hiodriver-5.0.4.1-4.19.36_vh################################# [100%]
Installing... Please wait for a moment.
Install the new nvme kernel module successfully.
Modify kdump image.Please wait for a moment...58%
Install kmod-hiodriver package successfully.
[root@euler2u8-d910-b630 aarch64]#
```

3.21.1.5 Installing the NPU Driver and Firmware

Prerequisites

Preparations for the installation have been made by referring to **Preparations for Installation**.

Procedure

Install a driver and then the firmware. The procedures for installing a driver and firmware are the same. Replace the asterisk (*) with an actual package name in commands.

1. Log in to the OS as the **root** user and upload the ***.run** package to any directory, for example, **/opt**.

2. Grant the execute permission on the package to the installation user.

   You can run the **ls -l** command in the directory where the package is stored to check whether the installation user has the permission to execute the file. If it does not, run the following command to grant the permission:

   chmod +x *.run

3. Run the following command to check the consistency and integrity of the package:

   ./*.run --check

4. Install the software package.

If you want to install the software package in a specified directory, for example, **/test/HiAI/**, run the **./*.run --full --install-path=***/test/HiAI/* command.

If you want to install the software package in the default directory, run the **./*.run –full** command.

The following uses EulerOS 2.8 as an example to describe how to install a driver. (The method for installing firmware package is the same.) Go to the directory where the software package is stored and run the **./A800-9000-npu-driver_***xxx***_euleros2.8-aarch64.run --full --install-for-all** command. (If the command does not contain **--install-for-all**, a certificate error may be reported when a non-root user uses the driver.)

NOTE

- Drivers can be installed on VMs. Firmware can only be installed on BMSs.
- If the **root** user is specified as an execution user, **--install-for-all** must be contained in the command.
- Default installation directory: **/usr/local/Ascend**
- Installation log directory: **/var/log/ascend_seclog/ascend_install.log**
- The installation directory, installation command, and user information are stored in **/etc/ascend_install.info** after the installation complete.

5. For a general driver package, if the following information is displayed, DKMS is not installed and the default kernel source code directory **/lib/modules/`uname -r`/build** does not exist.

```
[WARNING]rebuild ko has something wrong, detail in /var/log/ascend_seclog/ascend_rebuild.log Do you
want to try build driver after input kernel absolute path? [y/n]:
```

If you want to continue the installation, enter **y**.

When the following information is displayed, enter the path of the kernel source code, for example, **/lib/modules/`uname -r`/build-bak**.

```
Please input your kernel absolute path:
```

Press **Enter** to continue with the installation.

NOTE

- If DKMS and related components such as kernel-header and kernel-devel have been installed, the system will automatically compile driver source code and install the driver.
- If DKMS is not installed but the default kernel source code directory **/lib/modules/`uname -r`/build** exists, the kernel will be automatically used for driver compilation.

6. If information similar to the following is displayed, the installation is successful:
   - Driver: **Driver package install success! Reboot needed for installation/upgrade to take effect!**
   - Firmware: **Firmware package install success! Reboot needed for installation/upgrade to take effect!**
7. Restart the OS.
8. Check the driver version.

In the software package installation directory, for example, the default directory of the **root** user **/usr/local/Ascend/$**{*package_name*}, run the following command to check the driver version:

cat version.info

```
Version=1.73.T105.0.B050
```

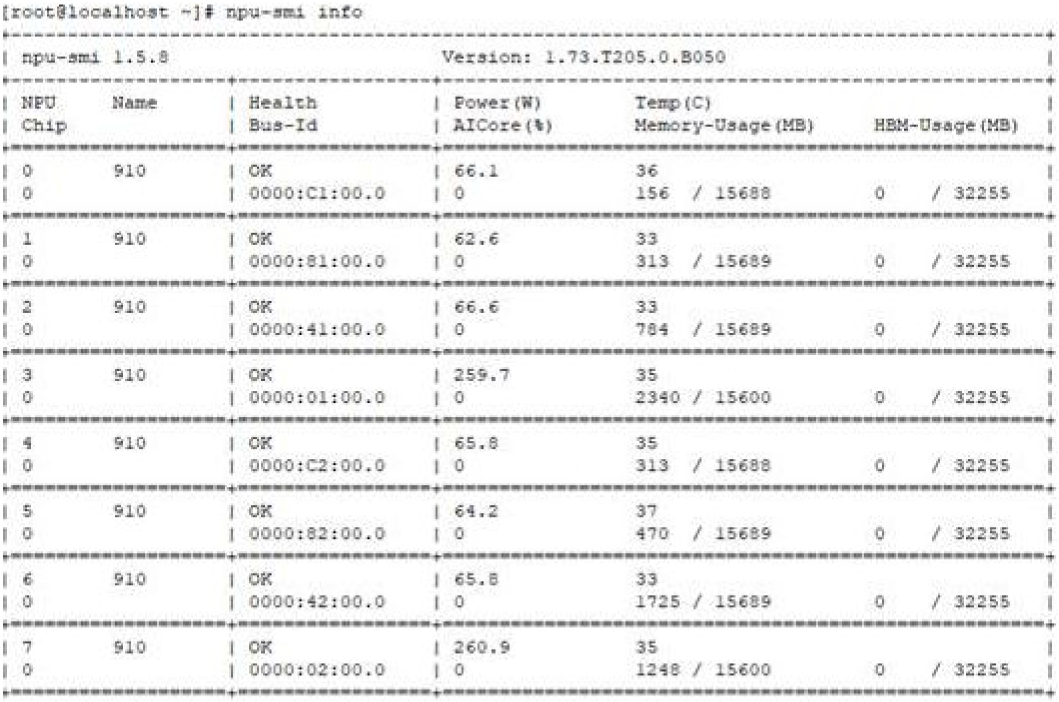
9. Check the firmware version.

/usr/local/Ascend/driver/tools/upgrade-tool --device_index -1 --component -1 --version

```
Get component version(1.73.5.0.b050) succeed for deviceId(0), componentType(0).          {"device_id":0, "component":nve, "version":1.73.5.0.b050}  Get component version(1.73.5.0.b050) succeed for deviceId(0), componentType(3).          {"device_id":0, "component":uefi, "version":1.73.5.0.b050}  Get component version(1.73.5.0.b050) succeed for deviceId(0), componentType(8).          {"device_id":0, "component":imu, "version":1.73.5.0.b050}  Get component version(1.73.105.0.b050) succeed for deviceId(0), componentType(9).          {"device_id":0, "component":imp, "version":1.73.105.0.b050}
```

10. Run the **npu-smi info** command to check whether the **npu-smi** tool is successfully installed.

The tool is installed successfully if the following information is displayed. Otherwise, the installation fails. Contact technical support.



```
[root@localhost ~]# npu-smi info
+------------------------------------------------------------------------------------------------+
| npu-smi 1.5.8                    Version: 1.73.T205.0.B050                                     |
+----------------------+----------------------+--------------------------------------------------+
| NPU     Name         | Health               | Power(W)          Temp(C)                        |
| Chip                 | Bus-Id               | AICore(%)         Memory-Usage(MB)    HBM-Usage(MB) |
+======================+======================+==================================================+
| 0       910          | OK                   | 66.1              36                             |
| 0                    | 0000:C1:00.0         | 0                 156  / 15688        0    / 32255 |
+======================+======================+==================================================+
| 1       910          | OK                   | 62.6              33                             |
| 0                    | 0000:81:00.0         | 0                 313  / 15689        0    / 32255 |
+======================+======================+==================================================+
| 2       910          | OK                   | 66.6              33                             |
| 0                    | 0000:41:00.0         | 0                 784  / 15689        0    / 32255 |
+======================+======================+==================================================+
| 3       910          | OK                   | 259.7             35                             |
| 0                    | 0000:01:00.0         | 0                 2340 / 15600        0    / 32255 |
+======================+======================+==================================================+
| 4       910          | OK                   | 65.8              35                             |
| 0                    | 0000:C2:00.0         | 0                 313  / 15688        0    / 32255 |
+======================+======================+==================================================+
| 5       910          | OK                   | 64.2              37                             |
| 0                    | 0000:82:00.0         | 0                 470  / 15689        0    / 32255 |
+======================+======================+==================================================+
| 6       910          | OK                   | 65.8              33                             |
| 0                    | 0000:42:00.0         | 0                 1725 / 15689        0    / 32255 |
+======================+======================+==================================================+
| 7       910          | OK                   | 260.9             35                             |
| 0                    | 0000:02:00.0         | 0                 1248 / 15600        0    / 32255 |
+======================+======================+==================================================+
```

NOTE

- **npu-smi** indicates the tool version, and **Version** indicates the NPU driver version.
- For details about other **npu-smi** commands, see **Atlas 800 AI Training Server npu-smi Command Reference (Model 9000)**.

Important Notes

- Logs are recorded based on the system time. NPU synchronizes the system time. To change the system time, run the **date** command.

  For example, to set the system time to **17:55:55**, run the **date -s 17:55:55** command.

3.21.1.6 Uninstalling the NPU Driver and Firmware

Procedure

You can uninstall the driver and firmware in any sequence. Replace the asterisk (*) with an actual package name in commands.

1. Log in to the OS as the **root** user.
2. You can use either of the following methods to uninstall the driver and firmware.
   - Run the following command in the directory where the *.**run** package is stored, for example, **/opt**:

     ./*.run --uninstall
   - Run the following command in any directory:

     bash *{install_path}*/*{package_name}***/script/uninstall.sh**

   NOTE

   - **npu-smi** indicates the tool version, and **Version** indicates the NPU driver version.
   - For details about other **npu-smi** commands, see **Atlas 800 AI Training Server npu-smi Command Reference (Model 9000)**.

   3. If no error information is displayed, the uninstallation is successful. You can determine whether to restart the OS based on the prompt information.

3.21.2 Upgrade

3.21.2.1 Before You Start

Impacts

You are not allowed to perform any other maintenance operations during the upgrade.

The system will be reset during driver/firmware upgrade of Atlas 800 (model 9000) training servers. This will cause service interruptions.

Precautions

See **Table 3-11**.

Table 3-11 Precautions for upgrade

No.	Description
1	Before the update, read this document carefully to ensure that you have learned all the content. For any problems or suggestions pertaining to the document, contact technical support.
2	To reduce impacts on services, switch services to other nodes or perform the upgrade during off-peak hours.
3	After the upgrade, ensure that the versions of the driver and firmware are consistent.
4	Before the upgrade, ensure that the OS is running properly and the firmware and dependent drivers are properly loaded. Otherwise, reset the system before performing the upgrade. For details, see **How Do I Check Whether the Device Is Running Properly?**
5	Do not modify the **/etc/ascend_install.info** file unless necessary. Otherwise, system functions will be unavailable.
6	For an upgrade from an earlier version to NPU C72B050 or later, skip **system reboot** in **Upgrading the Ascend NPU Firmware** and **system reboot** in **Upgrading the Ascend NPU Driver**. After the driver upgrade is complete, perform a restart. You can run the following command to check the NPU version: **/usr/local/Ascend/driver/tools/upgrade-tool --device_index -1 --component -1 --version**

Version Requirements

You are advised to use the driver and firmware in the same software matching list for Atlas 800 (model 9000) training server so that the driver matches the firmware.

Upgrade Process

Upgrade the driver and then firmware.

3.21.2.2 Preparing for Upgrade

Performing Pre-upgrade Check

Perform a check according to **Table 3-12** and record the check results.

Table 3-12 Pre-upgrade checklist

No.	Check Item	Checklist
1	Software version	1. Check and record the current version of the Atlas 800 (model 9000) training server. 2. Determine the target version.
2	System status	Check alarms of the Atlas 800 (model 9000) training server. ● If no active alarm exists, perform the upgrade without additional actions. ● If there are active alarms, contact technical support to clear the alarms. Then, perform the upgrade.

Table 3-13 lists the driver/firmware versions supported by different NPUs.

Table 3-13 Compatible software versions

NPU	Driver/Firmware Version
Ascend A	20.0.0, 20.1.0, 20.2.0
Ascend B	20.0.0, 20.1.0, 20.2.0
Ascend Pro A	20.0.0, 20.1.0, 20.2.0
Ascend Pro B	20.2.0.SPC300
Ascend Premium A	20.2.0.SPC300

Obtaining Upgrade Packages

To obtain upgrade packages, perform the following steps:

1. Visit **https://support.huawei.com/enterprise/en/ascend-computing/a800-9000-pid-250702818/software**.

2. Choose a BMS version **A800-9000** *x.x.x*.

Determine the driver/firmware version by referring to **CANN Version Mapping**.

Download upgrade packages to your local PC. **Table 3-14** describes upgrade package details.

NOTE

- *x.x.x* indicates the software version.
- The **A800-9000-npu-driver**_*x.x.x*_**linux-aarch64.run** package is compatible with all OSs.

Table 3-14 Driver and firmware upgrade packages

BMS	OS	Kernel	Driver Package	Firmware Package
Atlas 800 9000 (AArch64)	EulerOS 2.8	4.19.36-vhulk1907.1.0.h475	A800-9000-npu-driver_*x.x.x*_euleros2.8-aarch64.run	A800-9000-npu-firmware_x.x.x.run
	CentOS7.6	4.14.0-115.el7a.0.1.aarch64	A800-9000-npu-driver_*x.x.x*_centos7.6-aarch64-.run	
	Ubuntu18.04	4.15.0-45-generic Note: If the kernel does not match the OS, install DKMS to compile the driver source code before you upgrade the driver. For details about how to install DKMS, see **Driver Source Code Compilation**.	A800-9000-npu-driver_*x.x.x*_ubuntu18.04-aarch64.run	
	CentOS8.2	4.18.X Note: The kernel can be upgraded to 5.6.14.	A800-9000-npu-driver_*x.x.x*_linux-aarch64.run	
	BC_Linux 7.6	4.19	A800-9000-npu-driver_*x.x.x*_centos7.6-aarch64-.run A800-9000-npu-driver_*x.x.x*_linux-aarch64.run	

BMS	OS	Kernel	Driver Package	Firmware Package
	Kylin OS V10SP1 Note: Kylin OS V10SP1 is only supported by NPU driver 21.0.rc1 and later versions.	4.19.90-17.ky10.aarch64	A800-9000-npu-driver_*x.x.x*_linux-aarch64.run	
	BC_Linux 7.7 Note: BC_Linux 7.7 is only supported by NPU driver 21.0.rc1 and later versions.	4.19.25-203.e17.bclinux.aarch64	A800-9000-npu-driver_*x.x.x*_linux-aarch64.run	

Checking the Software Package Integrity

To prevent a software package from being maliciously tampered with during transmission or storage, download the corresponding digital signature file for integrity verification while downloading the software package.

After software packages are downloaded, verify their PGP digital signatures by following *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software packages. Contact technical support.

Before a software package is used for installation or upgrade, its digital signature needs to be verified by following instructions provided in the signature verification guide to ensure that the software package is not tampered with.

For carrier users, visit **https://support.huawei.com/carrier/digitalSignatureAction**.

For enterprise users, visit **https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054**.

3.21.2.3 Upgrading the NPU Driver and Firmware

3.21.2.3.1 Upgrading the Ascend NPU Firmware

You can upgrade the firmware of Ascend NPUs for Atlas 800 (model 9000) training servers. This section uses the **A800-9000-npu-firmware_***x.x.x***.run** package as an example to describe how to upgrade NPU firmware.

Procedure

1. Obtain the software package **A800-9000-npu-firmware_***x.x.x***.run** by referring to **Preparing for Upgrade**.
2. Log in to the Atlas 800 (model: 9000) training server as the **root** user.
3. Upload **A800-9000-npu-firmware_***x.x.x***.run** to any directory in the OS, for example, **/opt**.
4. Go to the directory where **A800-9000-npu-firmware_***x.x.x***.run** is stored.

cd */opt*

5. Run the following command to change the permissions on **A800-9000-npu-firmware_***x.x.x***.run**:

chmod u+x *A800-9000-npu-firmware_x.x.x.run*

6. Run the **./A800-9000-npu-firmware_***x.x.x***.run --check** command to check the consistency and integrity of the software package.
7. Upgrade the firmware.

You can run the **./A800-9000-npu-firmware_***x.x.x***.run --upgrade** command to perform the upgrade.

If information similar to the following is displayed, the upgrade is successful:

```
Firmware package install success! Reboot needed for installation/upgrade to take effect!
```

NOTE

- *x.x.x* indicates the firmware version.
- The logs generated during the upgrade are recorded in the **/var/log/ascend_seclog/ascend_install.log** file. You can run the **vim /var/log/ascend_seclog/ascend_install.log** command to open the log file.

8. Reboot the system.

reboot

9. Check the firmware version.

In the installation directory, run the following command to check whether the firmware version is correct:

cat version.info

NOTE

- The default installation directory is **/usr/local/Ascend/firmware**.

3.21.2.3.2 Upgrading the Ascend NPU Driver

Scenarios

You can upgrade the driver of Ascend NPUs for Atlas 800 (model 9000) training servers.

This section uses the **A800-9000-npu-driver_*x.x.x*_euleros2.8-aarch64.run** package as an example to describe how to upgrade the NPU driver.

NOTE

- Driver upgrade does not change the system username or password.

Impacts on the System

The system will be reset during the driver upgrade of Atlas 800 (model 9000) training servers. This will cause service interruptions. To reduce impacts on services, switch services to other nodes before the upgrade.

Procedure

1. Obtain the driver package **A800-9000-npu-driver_*x.x.x*_euleros2.8-aarch64.run** by referring to **Preparing for Upgrade**.
2. Log in to the Atlas 800 (model: 9000) training server as the **root** user.
3. Upload **A800-9000-npu-driver_*x.x.x*_euleros2.8-aarch64.run** to any directory in the Linux OS, for example, **/opt**.
4. Go to the directory where **A800-9000-npu-driver_*x.x.x*_euleros2.8-aarch64.run** is stored.

cd /*opt*

5. Run the following command to change the permissions on **A800-9000-npu-driver_*x.x.x*_euleros2.8-aarch64.run**:

chmod u+x A800-9000-npu-driver_*x.x.x*_euleros2.8-aarch64.run

6. Run the **./A800-9000-npu-driver_*x.x.x*_euleros2.8-aarch64.run --check** command to check the consistency and integrity of the software package.
7. Upgrade the driver.

You can run the **./A800-9000-npu-driver_*x.x.x*_euleros2.8-aarch64.run --upgrade** command to perform the upgrade.

If information similar to the following is displayed, the upgrade is successful:

```
Driver package install success! Reboot needed for installation/upgrade to take effect!
```

NOTE

- During the driver upgrade, the dynamic library **libdcmi.so** and header file **dcmi_interface_api.h** are copied to the **/usr/local/dcmi/** directory.
- The logs generated during the upgrade are recorded in the **/var/log/ascend_seclog/ascend_install.log** file.

8. Reboot the system.

reboot

9. Check the driver version.

In the installation directory, run the following command to check whether the driver version is correct:

cat version.info

NOTE

- The default installation directory is **/usr/local/Ascend/driver**.

- If you cannot log in to the OS after the upgrade, contact technical support.
- If the upgrade failed or you have upgraded to an incorrect version, perform the upgrade again. If the issue persists, record the fault information and contact technical support.

3.22 Deleting Files

Deleting Uploaded Files

Delete files uploaded to the VM, such as the .rpm packages of bms-network-config and SDI drivers.

Deleting Temporary Files

- Run the following commands to delete user login records:

  echo > /var/log/wtmp

  echo > /var/log/btmp
- Run the following commands to delete temporary files:

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

  rm -rf /var/lib/cloud/*

  rm -rf /var/log/network-config.log
- Delete residual configurations.
  - SUSE: Check for the files whose names start with **ifcfg** in the **/etc/sysconfig/network-scripts/** folder and delete them except **ifcfg-lo** and **ifcfg.template**.

    Command for viewing a file: **ll /etc/sysconfig/network/**

    Command for deleting a file: **rm -rf /etc/sysconfig/network/ifcfg***xxx*
  - RedHat/CentOS/Oracle/Euler: Check for the files whose names start with **ifcfg** in the **/etc/sysconfig/network-scripts/** folder and delete them except **ifcfg-lo**.

    Command for viewing a file: **ll /etc/sysconfig/network-scripts/**

    Command for deleting a file: **rm -rf /etc/sysconfig/network-scripts/ifcfg***xxx*
  - Ubuntu OS: Run the **rm -rf /etc/network/interfaces.d/50-cloud-init.cfg** command to delete the file.
- Run the following command to delete operation records:

  history -w;echo > /root/.bash_history;history -c;history -c;history -c;

4 Windows

4.1 Preparing Hardware and Software

Prepare a Linux physical server as the host and a local Windows jumper server (physical server or VM) used to log in to the host.

The following must be installed on the host:

- vsftpd service
- SSHD service
- VNC service
- virt-manager
- KVM virtualization software

NOTE

You can download virt-manager from its official website or select it from the installation package when you install an OS on the host.

Prepare the software listed in **Table 4-1**. Determine the drivers to be installed based on **Mapping Between BMS Specifications and Drivers**.

Table 4-1 Software

Package	Description	How to Obtain
Host ISO image	CentOS 7.x	Obtain it from the official website.
OS ISO file	ISO file used to create a BMS image. The OSs supported by BMS images are described in **Table 1-2** and **Table 1-3**.	Obtain it from the official website.

Package	Description	How to Obtain
bms-network-config	It is used to automatically configure BMS networks.	Software: **https://bms-image-package.obs.cn-north-1.myhuaweicloud.com/bms-network-config-23.8.0.zip** SHA256 checksum: **https://bms-image-package.obs.cn-north-1.myhuaweicloud.com/bms-network-config-23.8.0.zip.sha256**
SDI driver	With the SDI driver, EVS disks can be attached to BMSs. The EVS disks can be used as system disks from which the BMSs are booted. This facilitates quick BMS provisioning.	**https://support.huawei.com/enterprise/zh/software/250607156-ESW2000158115**
Cloudbase-Init	This is a plug-in used to inject a password into Windows.	Software: **https://bms-image-package.obs.cn-north-1.myhuaweicloud.com/windows/cloudbase_init/CloudbaseInitSetup_x64.msi** SHA256 checksum: **https://bms-image-package.obs.cn-north-1.myhuaweicloud.com/CloudbaseInitSetup_x64.msi.sha256**
x86 V5 server drivers	LAN On Motherboard (LOM), RAID, and motherboard drivers of x86 V5 servers.	Visit **https://support.huawei.com/enterprise/en/servers/fusionserver-idriver-pid-21588909/software**. Click the latest version. Download the driver package based on the image OS.

NOTE

The memory of the BMS must be at least 150 MB larger than that of the created image. Ensure that the created image meets this requirement.

Table 4-2 lists the required tools.

Table 4-2 Tools

Package	Description	How to Obtain
Cross-platform remote access tool	Used to access the host, such as Xshell	Obtain it from the official website.
File transfer tool	Used to transfer files to the VM, such as Xftp	Obtain it from the official website.
VNC	Used to log in to the VM, such as VNC Viewer **NOTE** If the VNC Viewer version is 5.3.2, choose **Options** > **Expert** > **ColorLevel** on the login page and set **ColorLevel** to **rgb222**. Otherwise, you may fail to log in to the VM.	Obtain it from the official website.

4.2 (Optional) Installing x86 V5 Server Drivers

4.2.1 Making Preparations

You can use Dism++ to inject drivers into an ISO file. Then, install software such as Cloudbase-Init and bms-network-config to the VM created from the ISO image.

Before installing server drivers, you need to:

1. Prepare a Windows ISO image file of the required version on the local Windows jump server.
2. Install Dism++ on the local Windows jump server.
3. Download FusionServer server drivers to the local Windows jump server by referring to **Preparing Hardware and Software**.

   Examples:

   – Windows Server 2012 R2: **FusionServer iDriver-Win2K12R2-Driver-V113.zip**

   – Windows Server 2016: **FusionServer iDriver-Win2K16-Driver-V115.zip**
4. Decompress the .zip driver package to obtain the .iso driver file.

   – Windows Server 2012 R2: Decompress **FusionServer iDriver-Win2K12R2-Driver-V113.zip** to obtain the **onboard_driver_win2k12r2.iso** file.

   – Windows Server 2016: Decompress **FusionServer iDriver-Win2K16-Driver-V115.zip** to obtain the **onboard_driver_win2k16.iso** file.

4.2.2 Installing the chipset Driver

Scenario

chipset is a driver living on a Windows motherboard. If this driver is not installed, other hardware drivers may be undermined in performance or even fail to work properly.

NOTE

This document uses Windows Server 2016 as an example to describe how to install the chipset driver. The procedure is also applicable to Windows Server 2012 R2.

Procedure

1. Decompress the **onboard_driver_win2k16.iso** file in **Making Preparations** to obtain the **SetupChipset.exe** file from the folder that contains **chipset** (for example, **Chipset-Win2K16-***XXX*).
2. Extract **SetupChipset.exe** to a new folder.
   a. Click **Start**, enter **cmd** in the **Type here to search** box to open the command-line interface (CLI).
   b. Go to the directory where **SetupChipset.exe** is stored, for example, **D:\windows2016\tmp**.

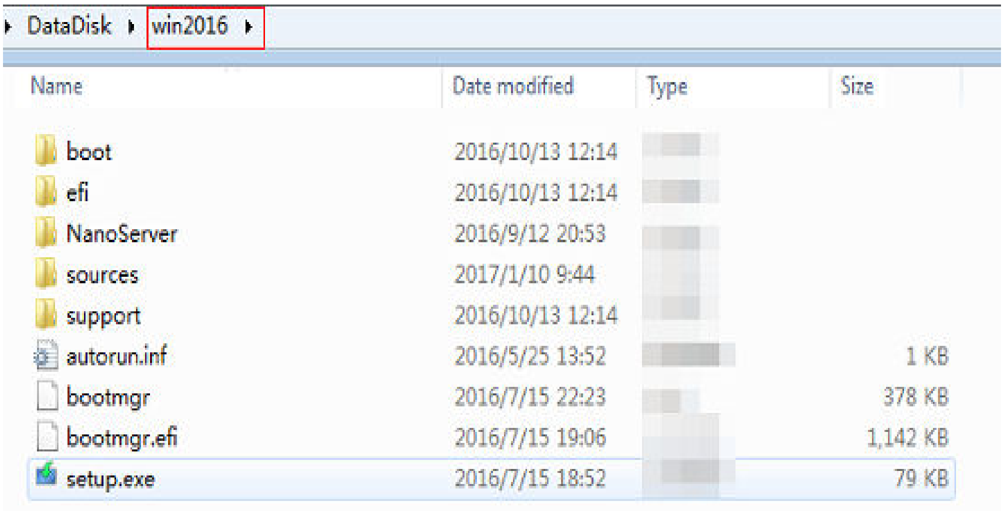
```
D:\windows2016\tmp>dir
2018/04/08   17:25   <DIR>          .
2018/04/08   17:25   <DIR>          ..
2018/03/08   15:14   <DIR>          drivers1
2018/03/08   11:28        3,525,008 SetupChipset.exe

D:\windows2016\tmp>
```

   c. Run the following command to extract **SetupChipset.exe** to a new folder named **driver**:

   .\SetupChipset.exe -extract driver

```
D:\windows2016\tmp>.\SetupChipset.exe -extract driver

D:\windows2016\tmp>dir
2018/04/08   17:32   <DIR>          .
2018/04/08   17:32   <DIR>          ..
2018/04/08   17:32   <DIR>          driver
2018/03/08   15:14   <DIR>          drivers1
2018/03/08   11:28        3,525,008 SetupChipset.exe

D:\windows2016\tmp>
```

3. Decompress the Windows 2016 ISO file to a folder.

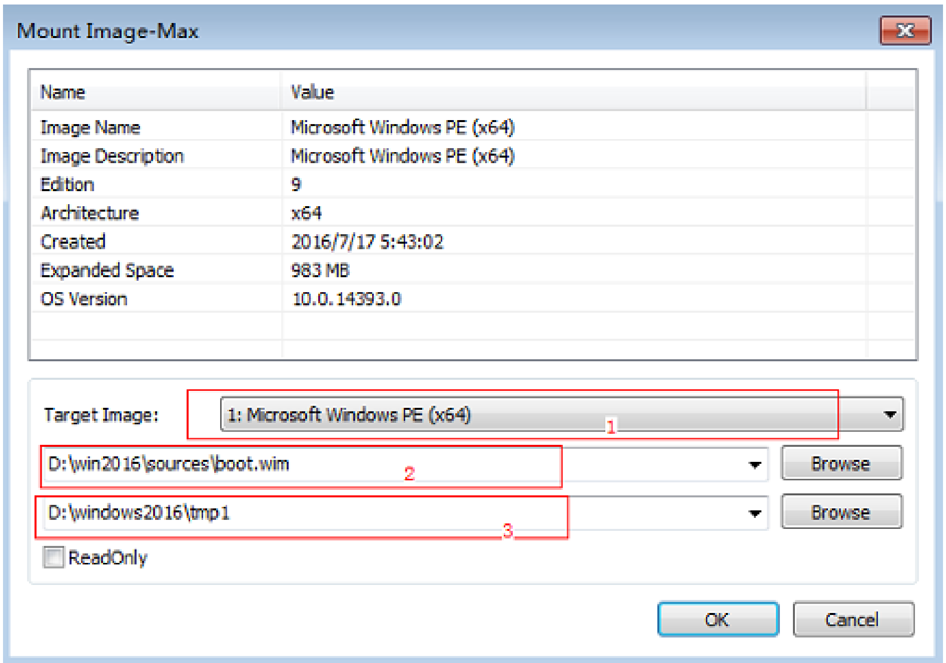


Name	Date modified	Type	Size
boot	2016/10/13 12:14	[redacted]	
efi	2016/10/13 12:14	[redacted]	
NanoServer	2016/9/12 20:53	[redacted]	
sources	2017/1/10 9:44	[redacted]	
support	2016/10/13 12:14	[redacted]	
autorun.inf	2016/5/25 13:52	[redacted]	1 KB
bootmgr	2016/7/15 22:23	[redacted]	378 KB
bootmgr.efi	2016/7/15 19:06	[redacted]	1,142 KB
setup.exe	2016/7/15 18:52	[redacted]	79 KB

4. Mount the image from **boot.wim** to a local directory and inject the chipset driver into the images.

   a. Open Dism++ and choose **File** > **Mount Image**.

   b. In the **Mount Image** window, perform the operations in the following figure in sequence.



Name	Value
Image Name	Microsoft Windows PE (x64)
Image Description	Microsoft Windows PE (x64)
Edition	9
Architecture	x64
Created	2016/7/17 5:43:02
Expanded Space	983 MB
OS Version	10.0.14393.0

Target Image: 1: Microsoft Windows PE (x64)

D:\win2016\sources\boot.wim

D:\windows2016\tmp1

□ ReadOnly

1: Select the target image.

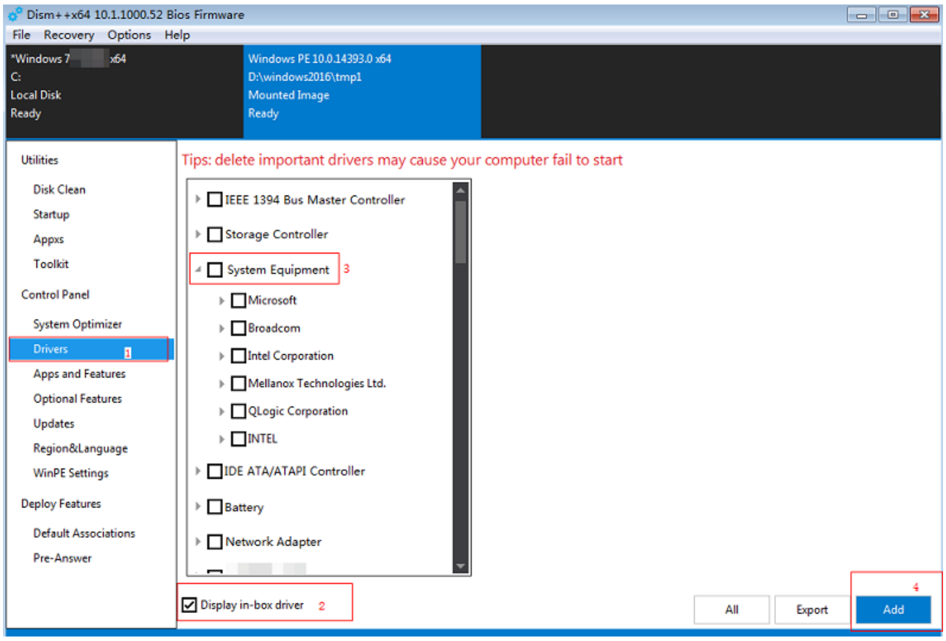
2: Select **boot.wim** in the **sources** folder shown in **3**.

3: Select an empty folder, for example, **tmp1**.

4: Click **OK**. A message is displayed indicating that the image is being mounted.

   c. When the image status changes to **Ready**, click **Open session**.

   d. Perform the operations shown in the following figure in sequence.



1. In the navigation pane, choose **Drivers**.

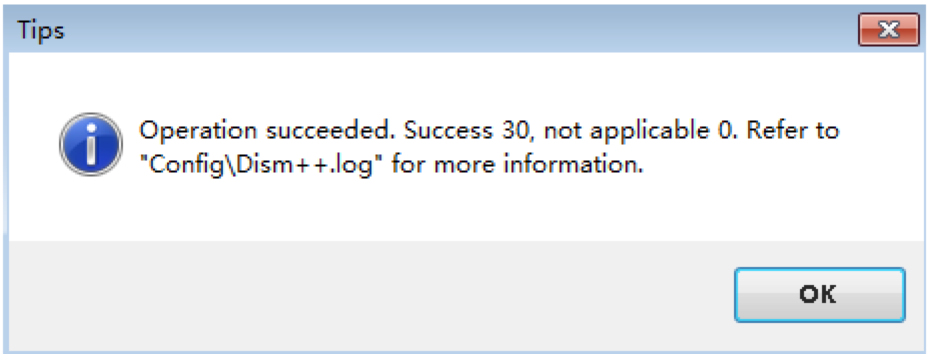
2. Select **Display in-box driver**.

3: Select **System Equipment**.

4. Click **Add**.

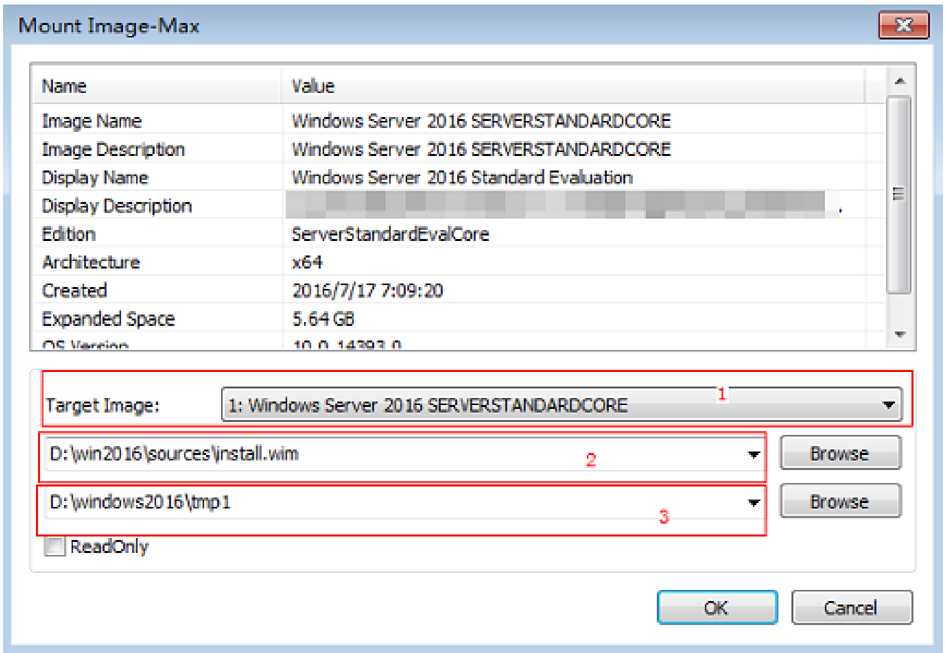
e. Select the **drivers** folder generated in 2.

The following dialog box is displayed.


Tips

Operation succeeded. Success 30, not applicable 0. Refer to "Config\Dism++.log" for more information.

5. Save the added driver and unmount the image.
   a. Choose **File** > **Save Image**. In the displayed dialog box, click **Save**.
   b. Wait for the image status to change from **Saving** to **Ready**.
   c. Choose **File** > **Unmount Image**.
6. Mount the image from **install.wim** to a local directory and inject the chipset driver into the image.
   a. Open Dism++ and choose **File** > **Mount Image**.
   b. In the **Mount Image** window, perform the operations in the following figure in sequence.



Mount Image-Max

Name	Value
Image Name	Windows Server 2016 SERVERSTANDARDCORE
Image Description	Windows Server 2016 SERVERSTANDARDCORE
Display Name	Windows Server 2016 Standard Evaluation
Display Description	[redacted]
Edition	ServerStandardEvalCore
Architecture	x64
Created	2016/7/17 7:09:20
Expanded Space	5.64 GB
OS Version	10.0.14393.0

Target Image: 1: Windows Server 2016 SERVERSTANDARDCORE

D:\win2016\sources\install.wim

D:\windows2016\tmp1

□ ReadOnly

1: By default, **Windows Server 2016 SERVERSTANDARDCORE** is selected. You can also select other versions from the drop-down list as needed.

2: Select **install.wim** in the **sources** folder shown in **3**.

3: Select an empty folder, for example, **tmp1**.

c. When the image status changes to **Ready**, click **Open session**.

d. Add the driver by performing **4.d** to **4.e**.

7. Save the added driver and unmount the image by performing **5**.

4.2.3 (Optional) Installing the LOM Driver of x86 V5 Servers

Scenario

To provision x86 V5 BMSs, you need to install the X722 LOM driver in the ISO image. For other types of BMSs, skip this section.

NOTE

This document uses Windows Server 2016 as an example to describe how to install the LOM driver. The procedure is also applicable to Windows Server 2012 R2.

Procedure

1. Decompress the **onboard_driver_win2k16.iso** file in **Making Preparations** and find the Intel NIC package or folder. For an Intel NIC package, for example, **NIC-82599_I350_X540_X550_X710_X722_XL710_XXV710-Win2K16-*XXX***, decompress it to obtain the **PRO40GB\Winx64\NDIS64** folder.
2. Mount the image from **boot.wim** to a local directory and inject the driver in the NDIS64 folder into the image by referring to **4** in **Installing the chipset Driver**.
3. Save the added driver and unmount the image by referring to **5** in **Installing the chipset Driver**.

4. Mount the image from **install.wim** to a local directory and inject the LOM driver into the image by referring to **6** in **Installing the chipset Driver**.
5. Save the added driver and unmount the image by referring to **7** in **Installing the chipset Driver**.

4.2.4 (Optional) Installing the Avago3408/3508 RAID Driver

Scenario

To provision BMSs with Avago3408/3508 RAID cards, you need to Install the Avago3408/3508 RAID driver in the ISO image. For other types of BMSs, skip this section.

NOTE

This document uses Windows Server 2016 as an example to describe how to install the Avago3408/3508 RAID driver. The procedure is also applicable to Windows Server 2012 R2.

Procedure

1. Decompress the **onboard_driver_win2k16.iso** file in **Making Preparations** to obtain the folder that contains **RAID** and **megasas**, for example, **RAID-3408iMR_3416iMR_3508_3516-Win2K16-megasas35-***XXX*.
2. Mount the image from **boot.wim** to a local directory and inject the driver in the **RAID-3408iMR_3416iMR_3508_3516-Win2K16-megasas35-7.716.3.0-x86_64** folder into the image by referring to **4** in **Installing the chipset Driver**.
3. Save the added driver and unmount the image by referring to **5** in **Installing the chipset Driver**.
4. Mount the image from **install.wim** to a local directory and inject the 3408/3508 RAID driver into the image by referring to **6** in **Installing the chipset Driver**.
5. Save the added driver and unmount the image by referring to **7** in **Installing the chipset Driver**.

4.3 Using Dism++ to Install the VMTools Driver for an ISO File

Scenario

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 describes how to install the VMTools driver for an ISO file using Dism ++.

Prerequisites

You have obtained an ISO file.

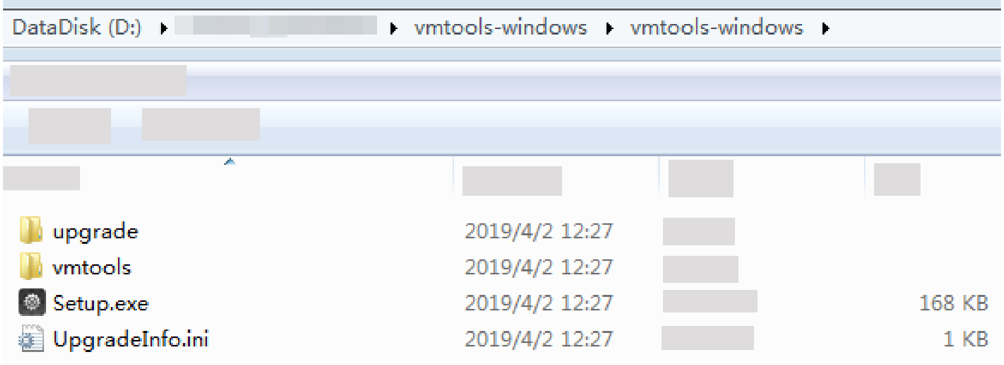
NOTE

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

Procedure

1. Download VMTools matching the OS and decompress it on the local PC.
2. Decompress the **vmtools-windows.zip** file downloaded in 1 to obtain **vmtools-windows.iso**, and then decompress **vmtools-windows.iso** to obtain the **vmtools-windows** folder.

Figure 4-1 vmtools-windows folder

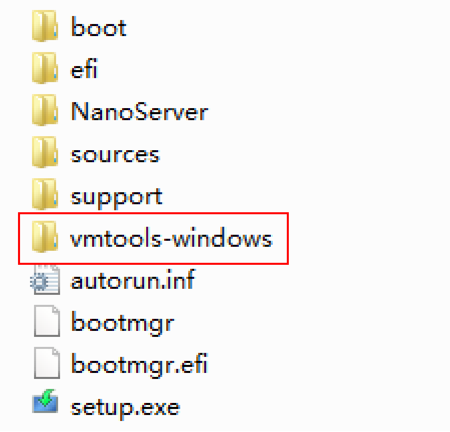


DataDisk (D:) ▸ [redacted] ▸ vmtools-windows ▸ vmtools-windows ▸

[redacted]	[redacted]	[redacted]	[redacted]
upgrade	2019/4/2 12:27	[redacted]	
vmtools	2019/4/2 12:27	[redacted]	
Setup.exe	2019/4/2 12:27	[redacted]	168 KB
UpgradeInfo.ini	2019/4/2 12:27	[redacted]	1 KB

3. Decompress the ISO image file, and copy the **vmtools-windows** folder obtained in 2 to the same directory as the **boot** folder in the ISO image file.

Figure 4-2 ISO image file

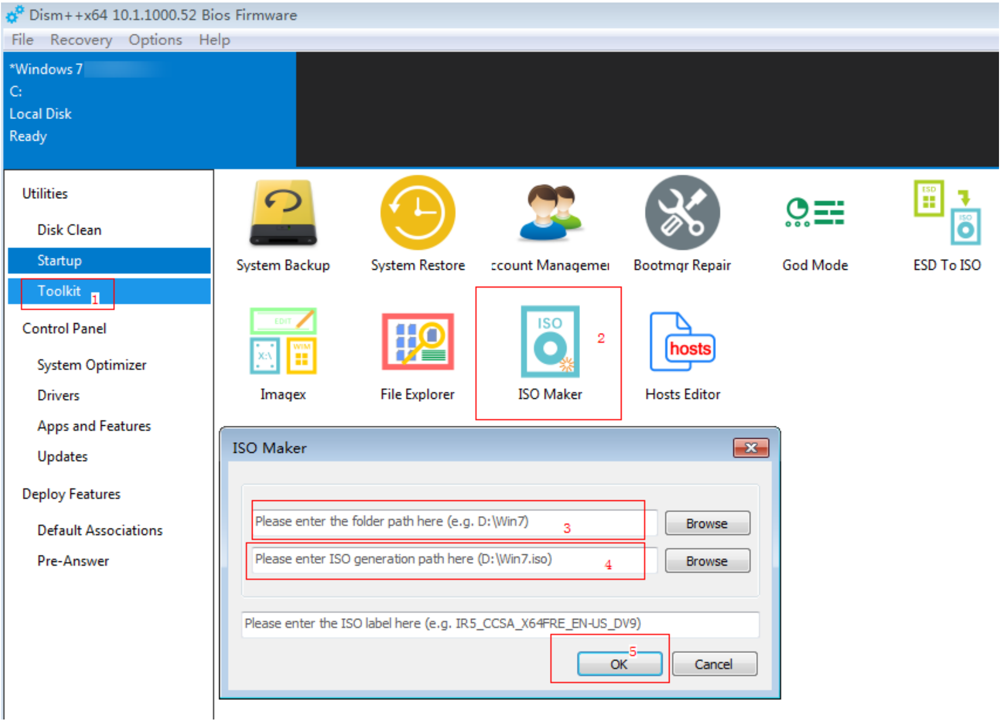


boot
efi
NanoServer
sources
support
vmtools-windows
autorun.inf
bootmgr
bootmgr.efi
setup.exe

4.4 Generating a New ISO File

In Dism++, export the ISO file for which the VMTools driver has been installed to an .iso file on the local PC.

Perform the operations shown in the following figure in sequence.



1. Choose **Toolkit**.

2. Click **ISO Maker**.

3. Select the directory where the original ISO file is stored.

4. Select the directory where the new ISO file is generated.

5. Click **OK**.

4.5 Creating a Windows VM

4.5.1 Creating a VM using virt-manager

4.5.1.1 Creating a VM and Installing an OS (Windows)

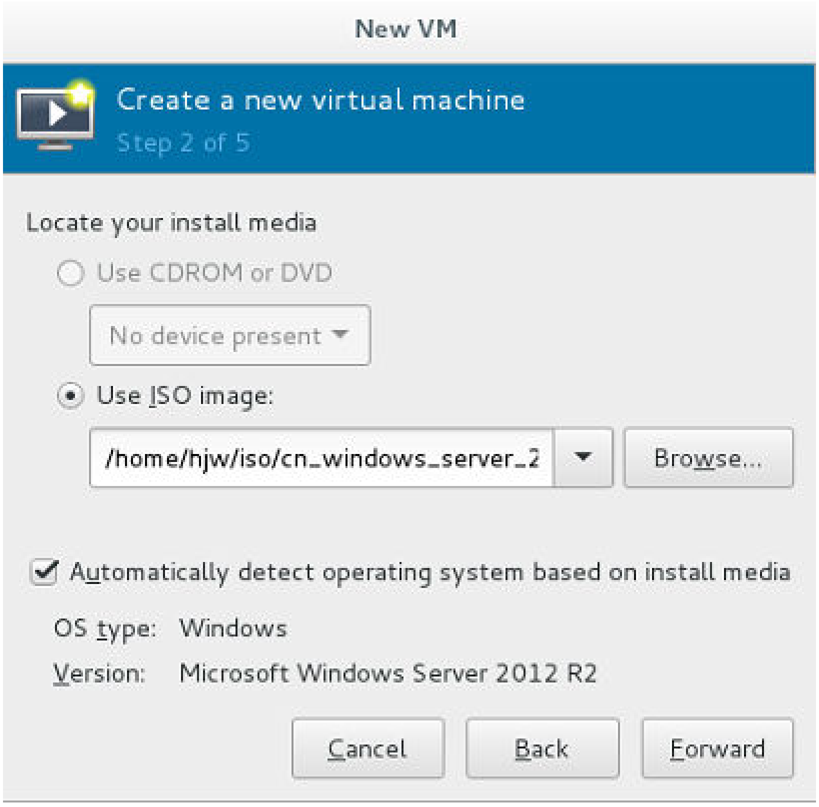
This section uses Windows Server 2012 R2 as an example to describe how to create a Windows VM. The procedure is also applicable to other Windows OSs. The screenshots in the following steps are for reference only.

1. Log in to the host, upload the ISO file generated in **Generating a New ISO File** to it, and start virt-manager.

```
[root@localhost Desktop]# virt-manager
[root@localhost Desktop]#
```

2. Click **Create a new virtual machine**. In the **New VM** dialog box, select **Local install media (ISO image or CDROM)** and click **Forward**.

3. Select the ISO image stored on the host, and select its OS type and version. In this example, the OS type and version are automatically detected by the system.



New VM

Create a new virtual machine
Step 2 of 5

Locate your install media

○ Use CDROM or DVD

No device present

● Use ISO image:

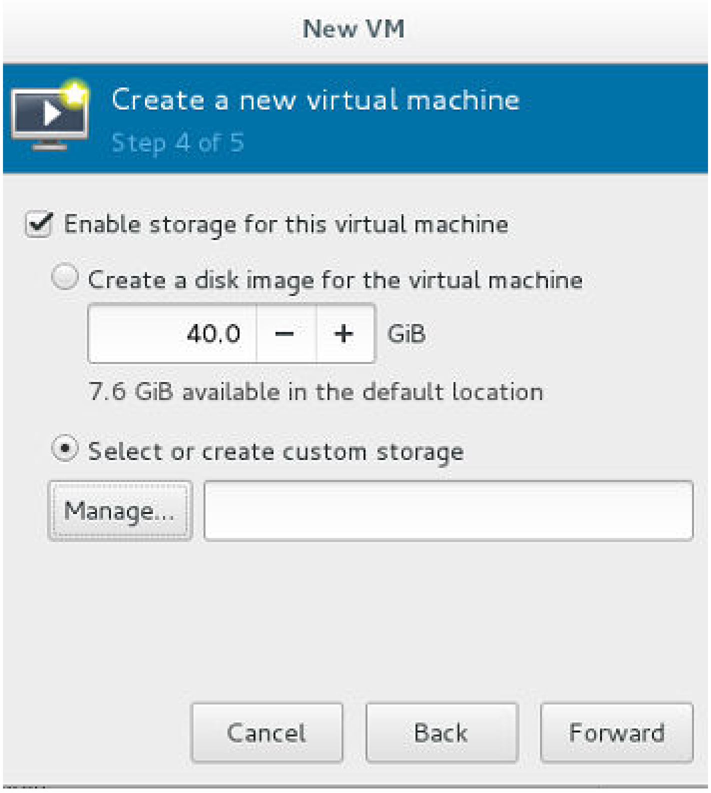
/home/hjw/iso/cn_windows_server_2

☑ Automatically detect operating system based on install media

OS type: Windows

Version: Microsoft Windows Server 2012 R2

4. Configure the VM memory and CPU.
   - Memory (RAM): 4096 MiB
   - CPUs: 4
5. Configure the VM storage by specifying the disk image size. (The image cannot be too large.)



New VM

Create a new virtual machine
Step 4 of 5

☑ Enable storage for this virtual machine

○ Create a disk image for the virtual machine

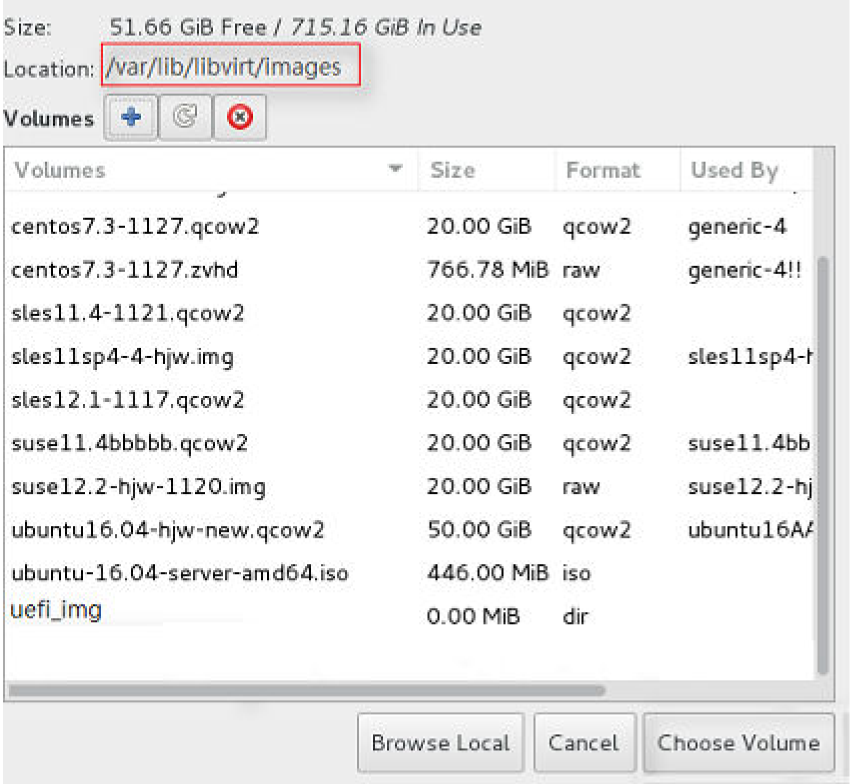
40.0 − + GiB

7.6 GiB available in the default location

● Select or create custom storage

Manage...

6. Click **Manage** and select a storage path, for example, **/var/lib/libvirt/images**.



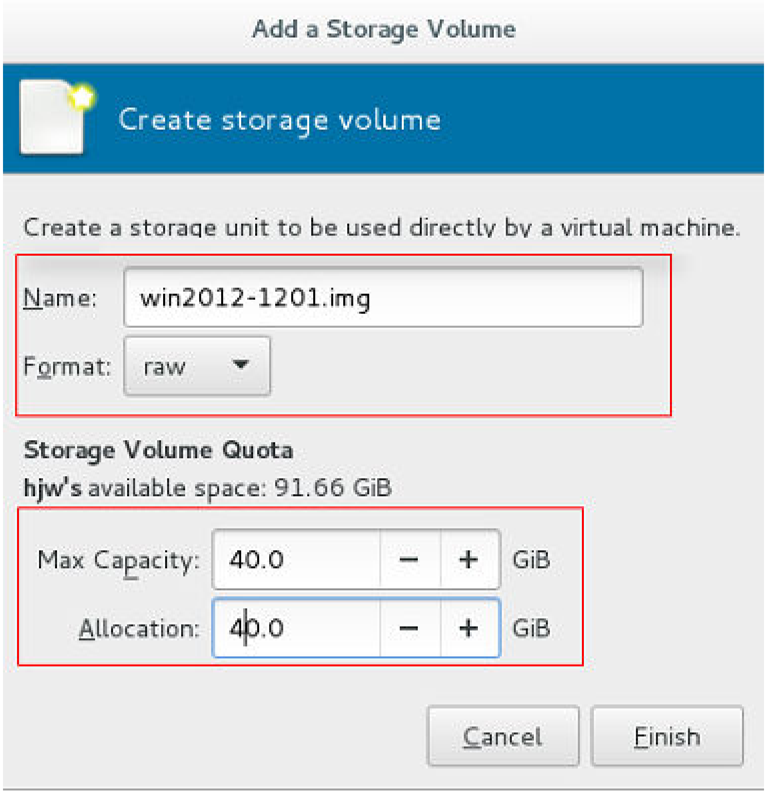
Size: 51.66 GiB Free / *715.16 GiB In Use*

Location: /var/lib/libvirt/images

Volumes

Volumes	Size	Format	Used By
centos7.3-1127.qcow2	20.00 GiB	qcow2	generic-4
centos7.3-1127.zvhd	766.78 MiB	raw	generic-4!!
sles11.4-1121.qcow2	20.00 GiB	qcow2	
sles11sp4-4-hjw.img	20.00 GiB	qcow2	sles11sp4-h
sles12.1-1117.qcow2	20.00 GiB	qcow2	
suse11.4bbbbb.qcow2	20.00 GiB	qcow2	suse11.4bb
suse12.2-hjw-1120.img	20.00 GiB	raw	suse12.2-hj
ubuntu16.04-hjw-new.qcow2	50.00 GiB	qcow2	ubuntu16A
ubuntu-16.04-server-amd64.iso	446.00 MiB	iso	
uefi_img	0.00 MiB	dir	

Click + to create a storage volume. Set **Name** (suffix **.img** is recommended so that the image can be compressed if it is large) and select **raw** (recommended) for **Format**.



Add a Storage Volume

Create storage volume

Create a storage unit to be used directly by a virtual machine.

Name: win2012-1201.img

Format: raw

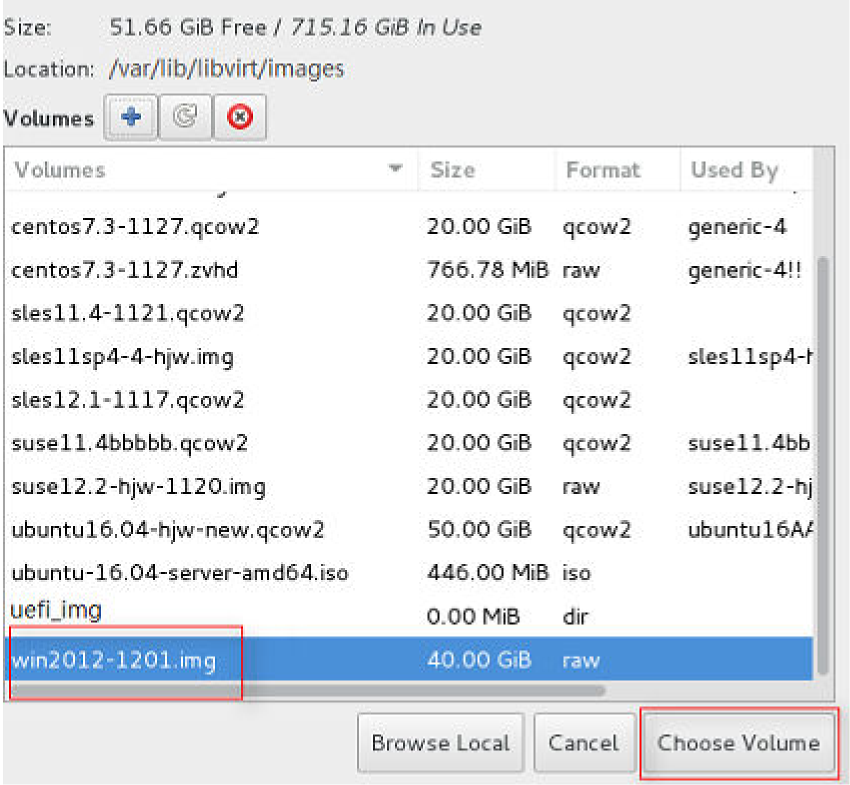
Storage Volume Quota

hjw's available space: 91.66 GiB

Max Capacity: 40.0 GiB

Allocation: 40.0 GiB

Click **Finish**. In the displayed storage volume list, select the created storage volume and click **Choose Volume**.



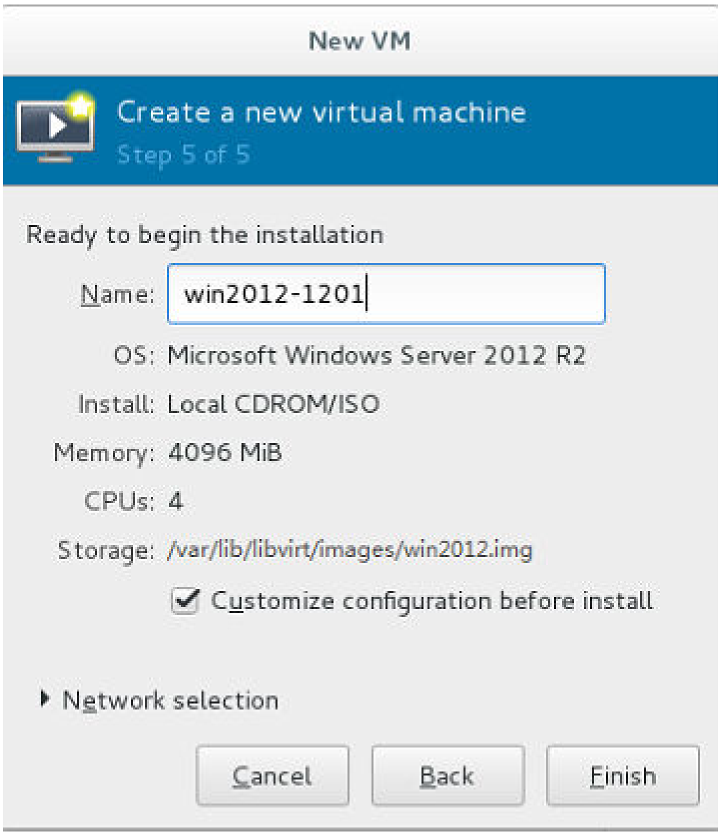
Size: 51.66 GiB Free / *715.16 GiB In Use*

Location: /var/lib/libvirt/images

Volumes

Volumes	Size	Format	Used By
centos7.3-1127.qcow2	20.00 GiB	qcow2	generic-4
centos7.3-1127.zvhd	766.78 MiB	raw	generic-4!!
sles11.4-1121.qcow2	20.00 GiB	qcow2	
sles11sp4-4-hjw.img	20.00 GiB	qcow2	sles11sp4-h
sles12.1-1117.qcow2	20.00 GiB	qcow2	
suse11.4bbbbb.qcow2	20.00 GiB	qcow2	suse11.4bb
suse12.2-hjw-1120.img	20.00 GiB	raw	suse12.2-hj
ubuntu16.04-hjw-new.qcow2	50.00 GiB	qcow2	ubuntu16A/
ubuntu-16.04-server-amd64.iso	446.00 MiB	iso	
uefi_img	0.00 MiB	dir	
win2012-1201.img	40.00 GiB	raw	

7. Enter a name for the VM and select **Customize configuration before install**.



New VM

Create a new virtual machine

Step 5 of 5

Ready to begin the installation

Name: win2012-1201

OS: Microsoft Windows Server 2012 R2

Install: Local CDROM/ISO

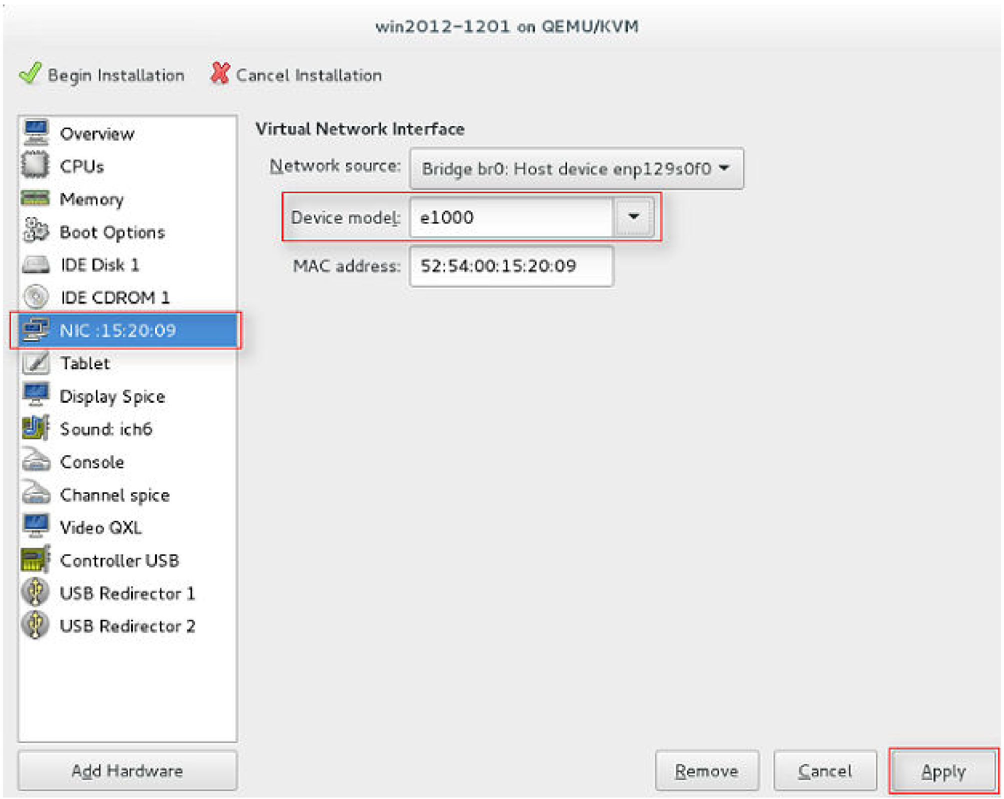
Memory: 4096 MiB

CPUs: 4

Storage: /var/lib/libvirt/images/win2012.img

☑ Customize configuration before install

8. In the navigation pane on the left, choose **NIC**. In the right pane, select **e1000** for **Device model**, and click **Apply**.



win2012-1201 on QEMU/KVM

Virtual Network Interface

Network source: Bridge br0: Host device enp129s0f0

Device model: e1000

MAC address: 52:54:00:15:20:09

9. Click **Begin Installation**. virt-manager creates the VM as you configured.

10. Install Windows on the VM.

    Configure the language, time zone, currency, and other settings by referring to **Installing a Windows OS and the VMTools Driver**. Activate the OS using the Windows Server 2012 R2 product key.

4.5.2 Creating a VM from an ISO Image

4.5.2.1 Registering an ISO File (Windows)

Scenarios

This section describes how to register an external ISO file as a private image (ISO image) on the cloud platform. Before registering an image, upload the ISO image file to an OBS bucket.

Prerequisite

- The file to be registered must be in ISO format.
- The ISO image file has been uploaded to an OBS bucket.

  NOTE

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

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

Step 2 Register an ISO file as an ISO image.

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

Figure 4-3 Creating a private image from an ISO file

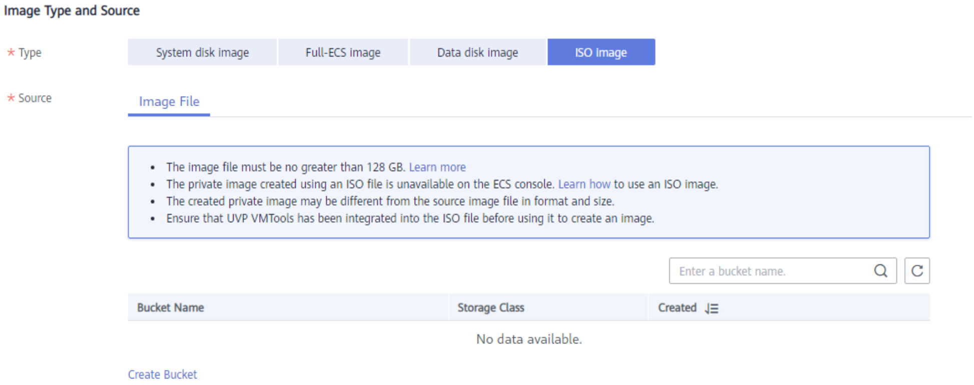


Image Type and Source

* Type: System disk image | Full-ECS image | Data disk image | ISO image

* Source: Image File

- The image file must be no greater than 128 GB. 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

No data available.

Create Bucket

4. In the **Image Information** area, set the following parameters.
   - **Architecture**. Select **x86** or **ARM**.

     NOTE

     This parameter is required only in regions that support both x86 and Arm.
   - **Boot Mode**: Select **BIOS** or **UEFI**. Ensure that the selected boot mode is the same as that in the image file, or the ECSs created from this image will not be able to boot up. The Arm architecture does not support the BIOS boot mode.

     NOTE

     If the boot mode in the image file is **BIOS** but you select **UEFI** here for **Boot Mode**, you will not be able to adjust the resolution.
   - **OS**: Select the OS specified in the ISO file. To ensure that the image can be created and used properly, select an OS consistent with that in the image file.
   - **System Disk**: Set the system disk capacity (value range: 40 GB to 1024 GB), which must be no less than the capacity of the system disk in the image file.
   - **Name**: Enter a name for the image to be created.
   - **Enterprise Project**: Select the enterprise project to which your images belong.
   - **Tag**: (Optional) Add a tag to the image to be created.
   - **Description**: (Optional) Enter image description as needed.
5. Click **Next**.
6. Confirm the settings. Select **Statement of Commitment to Image Creation** and **Huawei Image Disclaimer**. Click **Submit**.

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

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

----End

4.5.2.2 Creating a Windows ECS from an ISO Image

Scenarios

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

Procedure

Step 1 Access the IMS console.

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

   The IMS console is displayed.

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

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

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

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

----End

Follow-up Procedure

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

4.5.2.3 Installing a Windows OS and the VMTools Driver

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

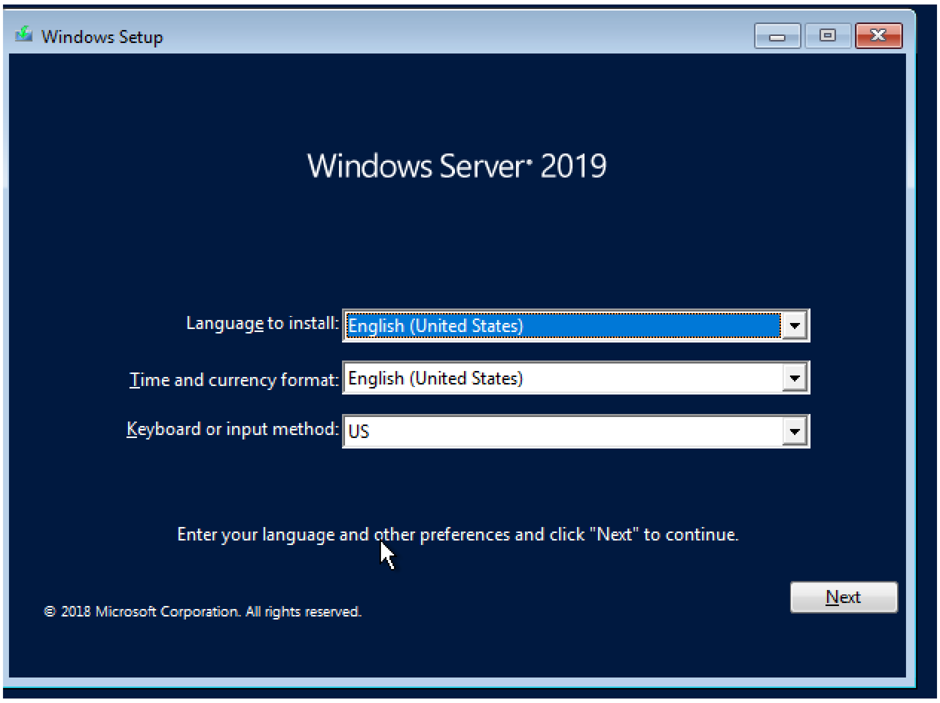
CAUTION

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 4-4 Windows setup



Windows Setup

Windows Server® 2019

Language to install: English (United States)

Time and currency format: English (United States)

Keyboard or input method: US

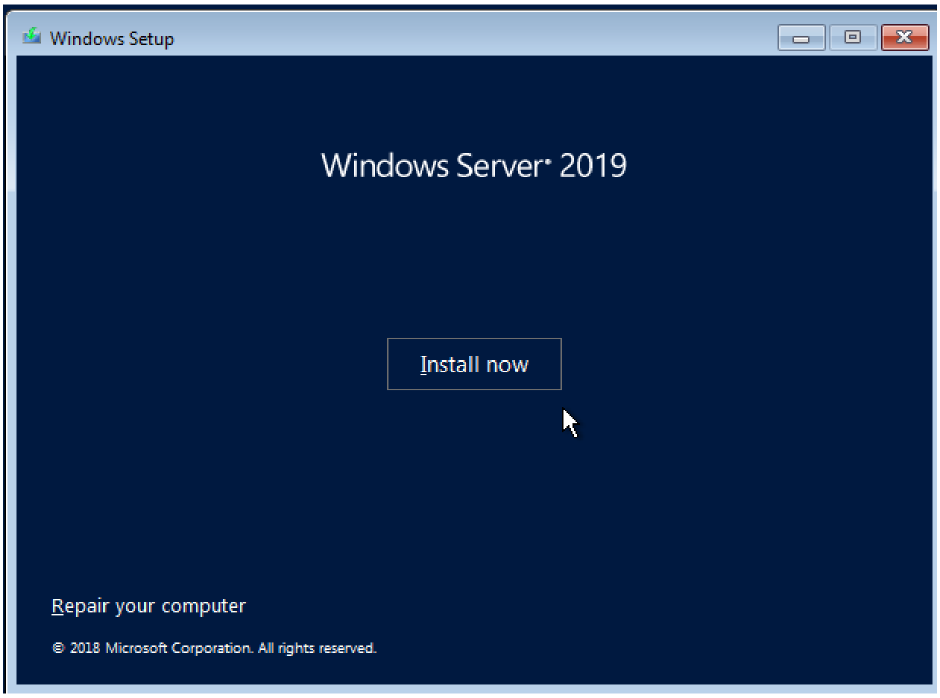
Enter your language and other preferences and click "Next" to continue.

© 2018 Microsoft Corporation. All rights reserved.

2. Click **Next**.

   The installation confirmation window is displayed.

Figure 4-5 Installation confirmation window



Windows Setup

Windows Server® 2019

© 2018 Microsoft Corporation. All rights reserved.

3. Click **Install now**.

   The **Select the operating system you want to install** window is displayed.

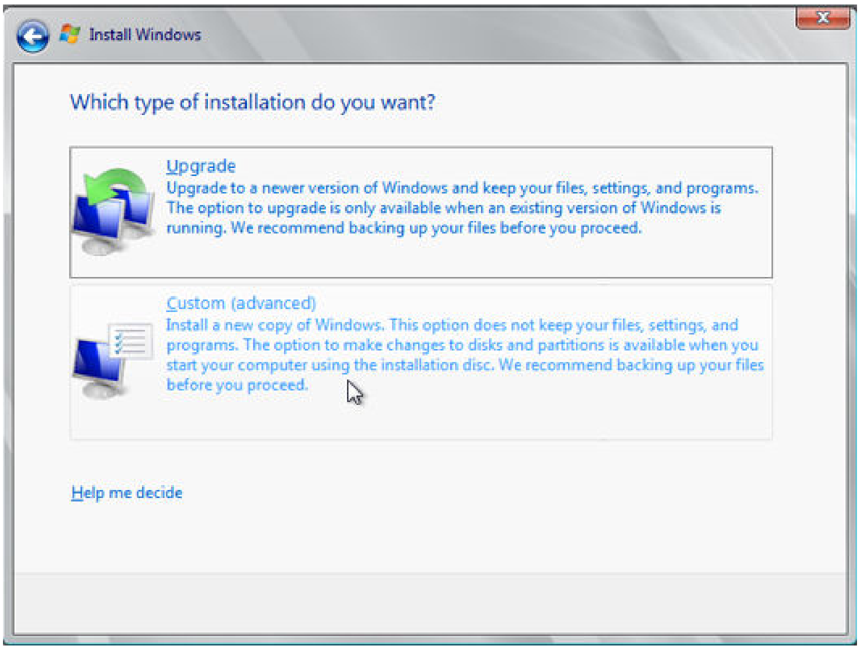
4. Select the version of the OS to be installed and click **Next**.

   The **Please read the license terms** window is displayed.

5. Select **I accept the license terms**, and click **Next**.

   The **Which type of installation do you want?** window is displayed.

   Figure 4-6 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.

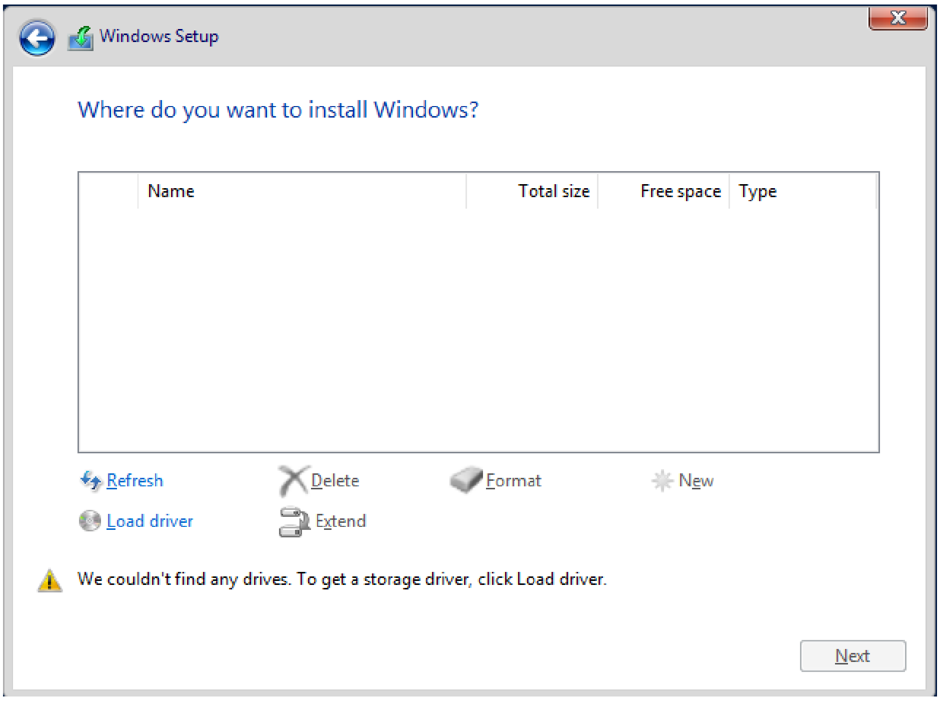
   Custom (advanced)
   Install a new copy of Windows. This option does not keep your files, settings, and programs. The option to make changes to disks and partitions is available when you start your computer using the installation disc. We recommend backing up your files before you proceed.

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

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

   – If the system displays a message indicating that no driver is found, go to **Step 1.7**.

     Figure 4-7 Installation path

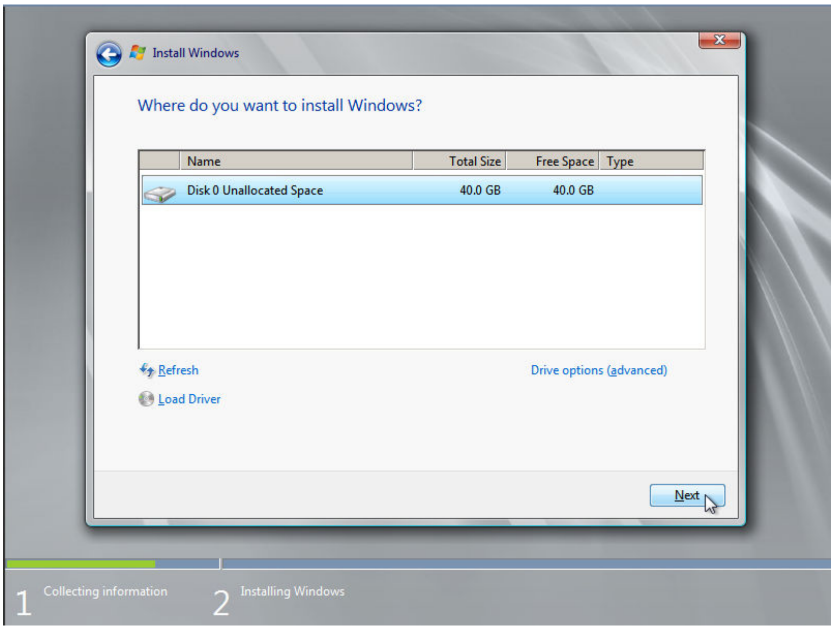
     Where do you want to install Windows?

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 1.10**.

Figure 4-8 Installation path

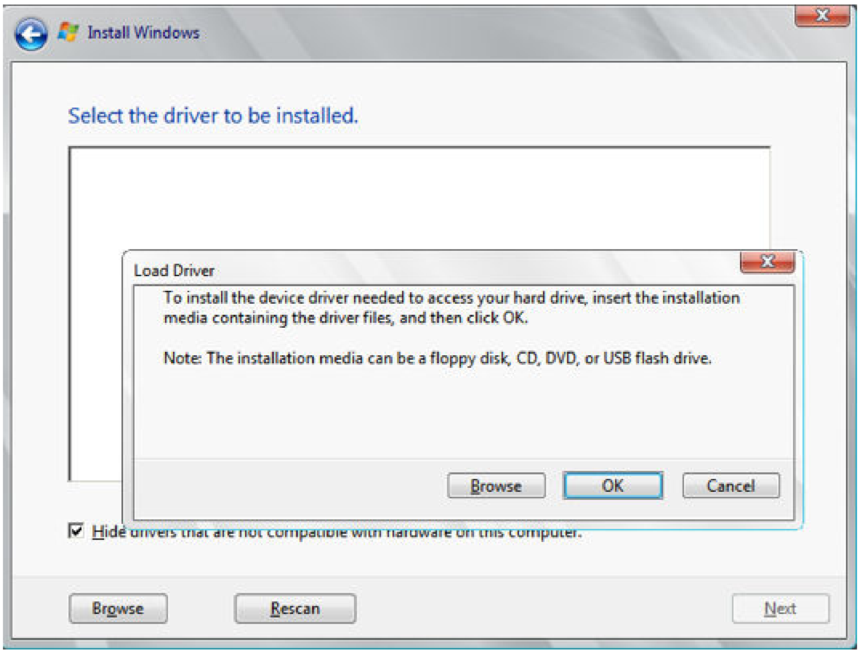


Where do you want to install Windows?

Name	Total Size	Free Space	Type
Disk 0 Unallocated Space	40.0 GB	40.0 GB	

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

Figure 4-9 Loading drivers



Select the driver to be installed.

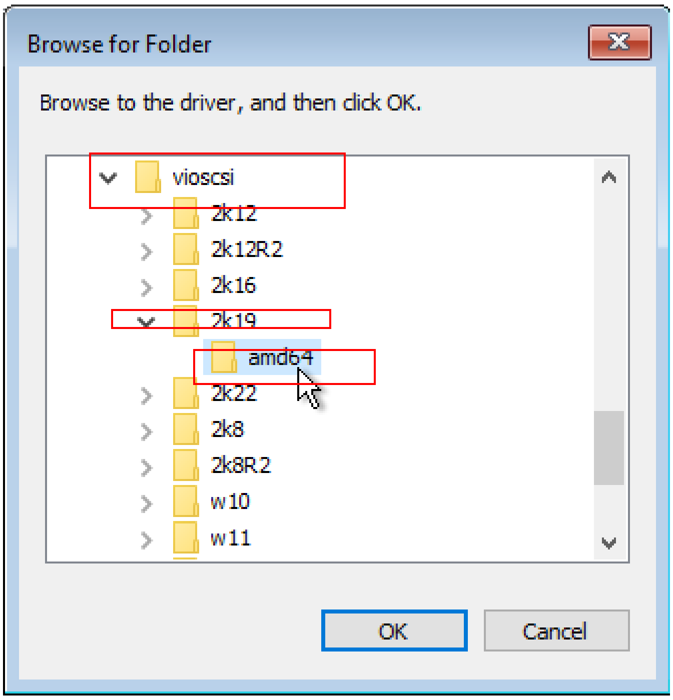
To install the device driver needed to access your hard drive, insert the installation media containing the driver files, and then click OK.

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. Choose **vioscsi** > **2k19** > **amd64** and click **OK**.

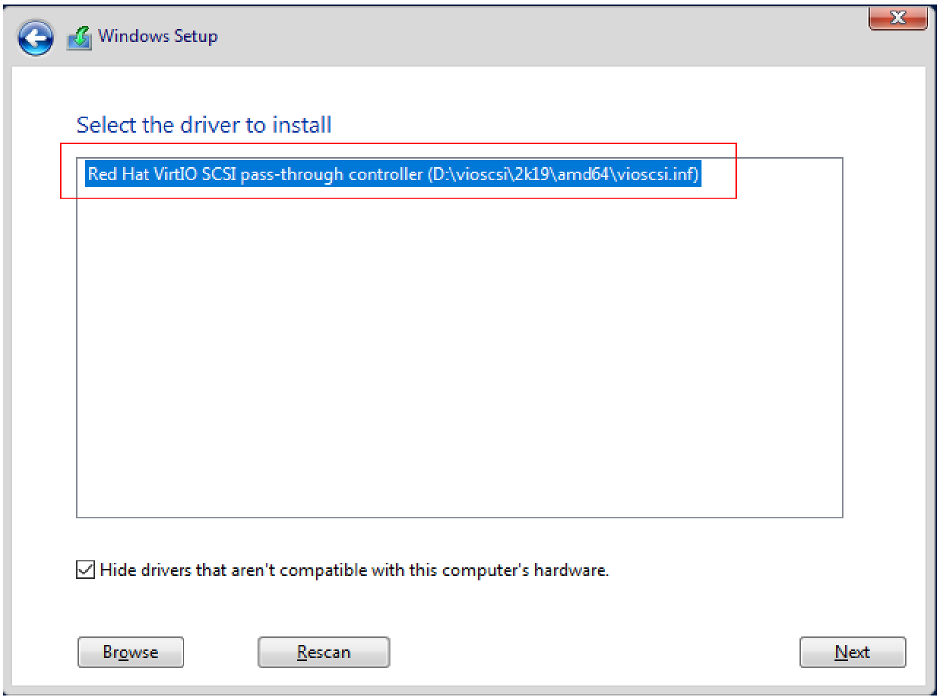
Figure 4-10 Browsing for a folder



9. Select the driver matching the OS and click **Next**.

   The system may provide multiple drivers. Select **VISOTOR.INF** shown in the following figure.

Figure 4-11 Selecting the driver to install

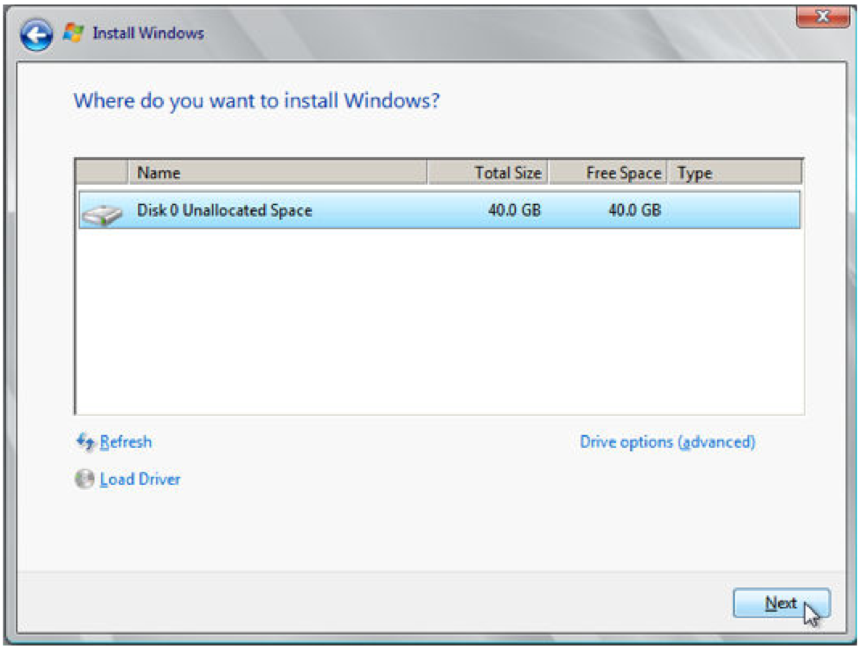


Red Hat VirtIO SCSI pass-through controller (D:\vioscsi\2k19\amd64\vioscsi.inf)

☑ Hide drivers that aren't compatible with this computer's hardware.

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

Figure 4-12 Installation path



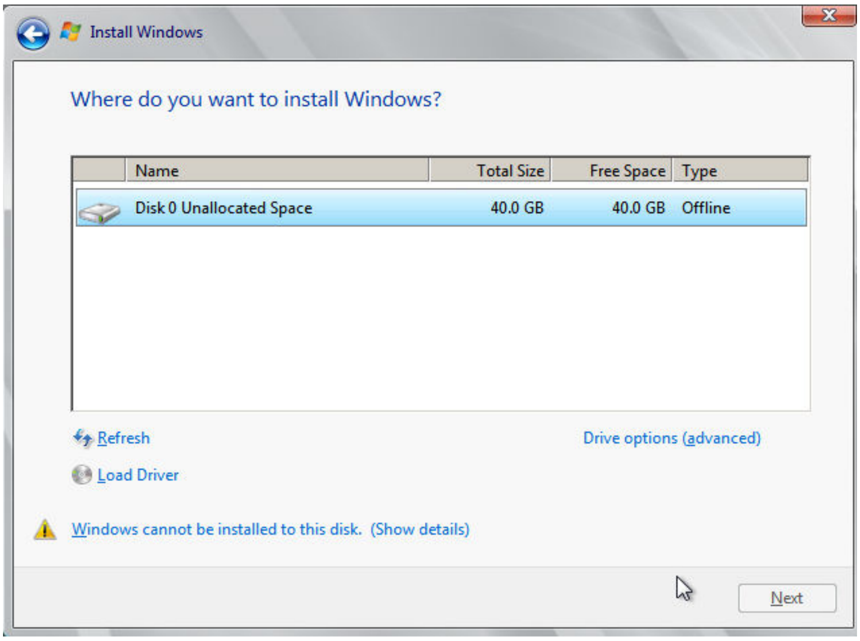
Where do you want to install Windows?

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 4-13 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)

11. The **Installing Windows** window is displayed, and the OS installation starts.

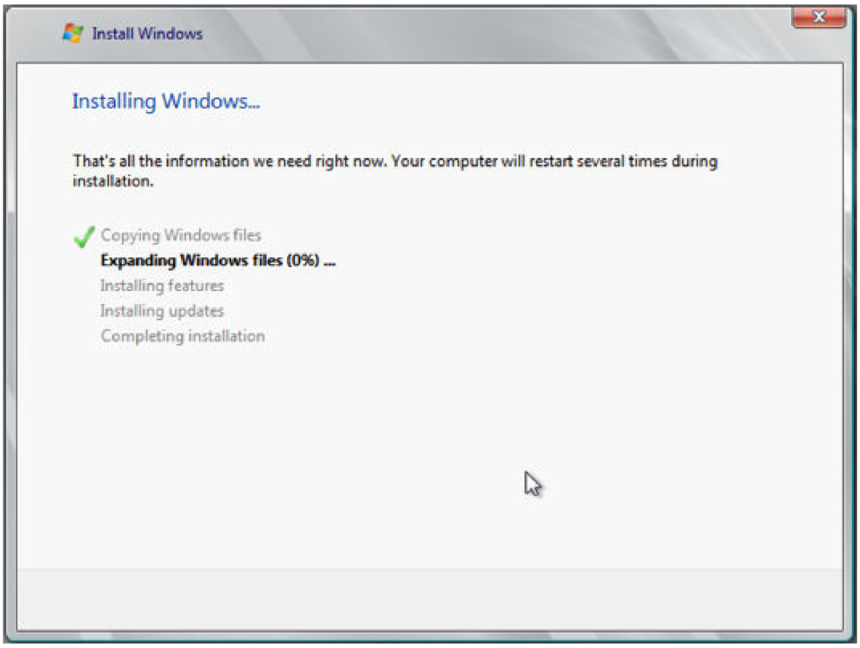
    The installation takes about 50 minutes. The ECS restarts during the installation. After the ECS successfully restarts, log in to it again and configure the OS as prompted.

NOTE

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

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

Figure 4-14 Installation progress



Install Windows

Installing Windows...

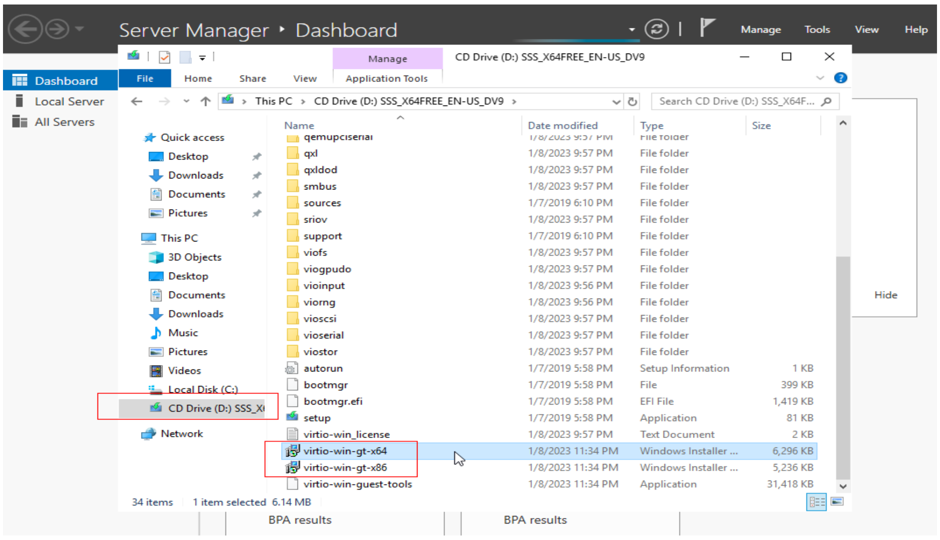
That's all the information we need right now. Your computer will restart several times during installation.

✓ Copying Windows files
Expanding Windows files (0%) ...
Installing features
Installing updates
Completing installation

Step 2 Install related drivers.

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

Figure 4-15 Starting the CD drive



CD Drive (D:) SSS_X64FREE_EN-US_DV9

This PC › CD Drive (D:) SSS_X64FREE_EN-US_DV9 ›

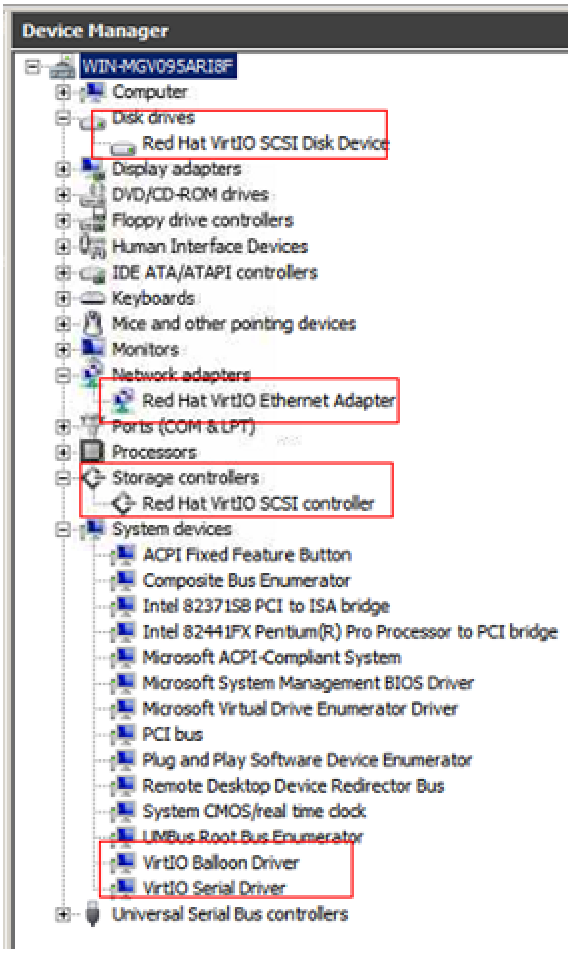
Search CD Drive (D:) SSS_X64F...

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 4-16 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
```

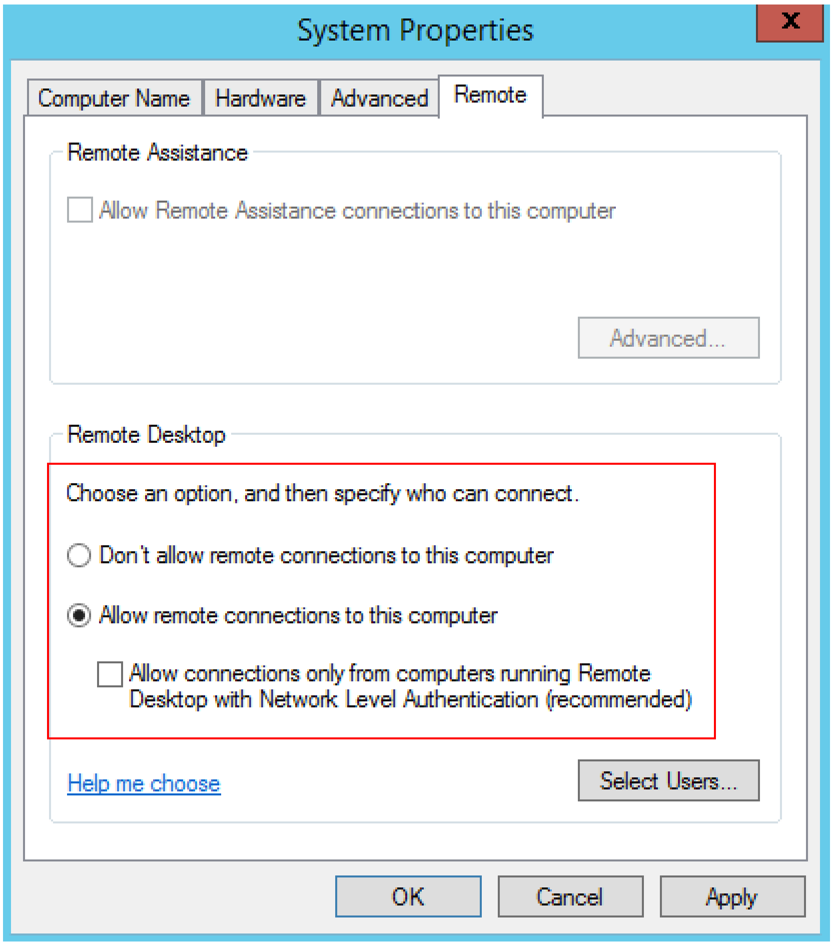
----End

4.6 Configuring the VM Environment

After the Windows OS is installed on the VM, disable the firewall and configure remote desktop.

Procedure

1. Click ⊞ in the lower left corner to start Server Manager.
2. In the navigation pane on the left, choose **Local Server**. In the right pane, click the link following **Windows Firewall**.
3. In the **Windows Firewall** dialog box, choose **Turn Windows Firewall on or off** in the navigation pane on the left.
4. In the **Customize Settings** dialog box, turn off the Windows firewall for the private and public networks.
5. Go back to the **Local Server** page and click the link following **Remote Desktop**.
6. In the **System Properties** window, select the options shown in the red box in the following figure.



Remote Assistance

□ Allow Remote Assistance connections to this computer

Remote Desktop

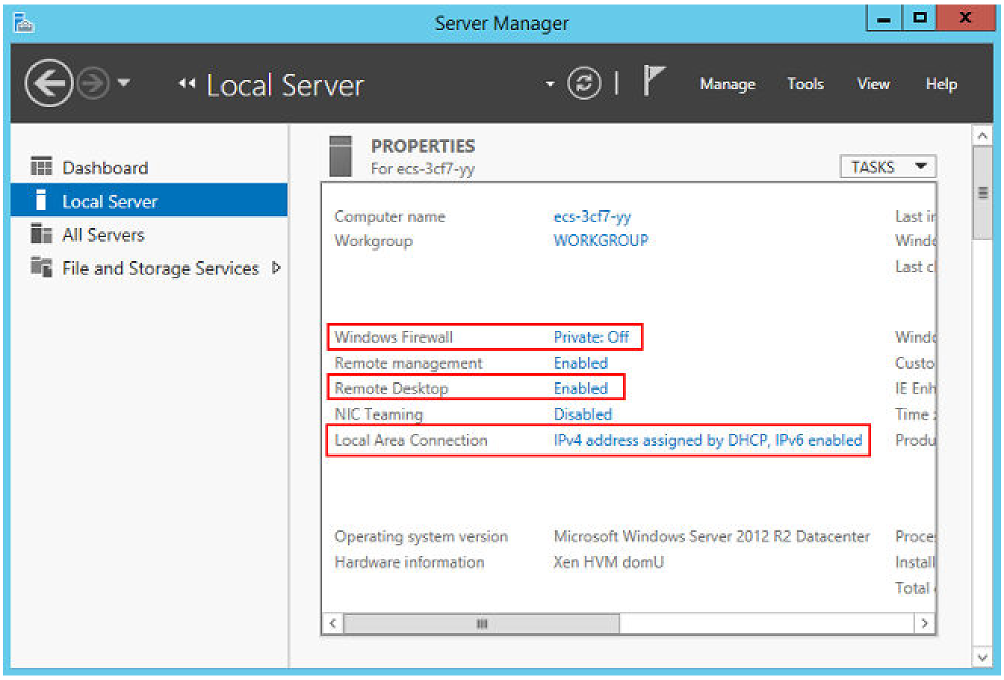
Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

□ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

7. Go back to the **Local Server** page and verify that statuses of the properties are those shown in the red box in the following figure.



PROPERTIES
For ecs-3cf7-yy

Computer name ecs-3cf7-yy
Workgroup WORKGROUP

Windows Firewall Private: Off
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Local Area Connection IPv4 address assigned by DHCP, IPv6 enabled

Operating system version Microsoft Windows Server 2012 R2 Datacenter
Hardware information Xen HVM domU

4.7 Installing Cloudbase-Init

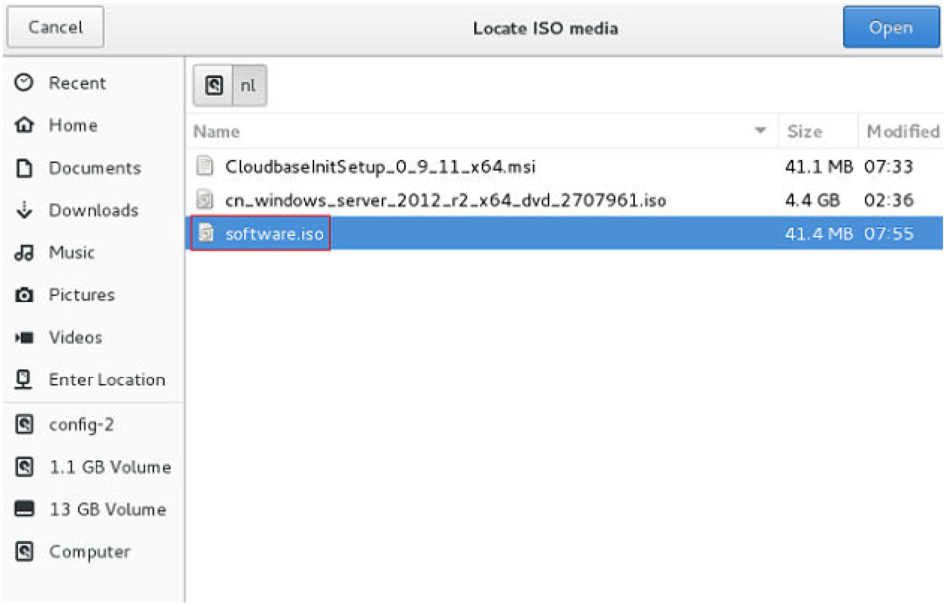
1. Download the Cloudbase-Init software package and SHA256 checksum by referring to **Software** and verify the software package integrity (for details, see**How Do I Verify Software Package Integrity?**).
2. Upload the package to the host and generate an ISO file.

   Upload the installation package to the host.

   ```
   [root@server nl]# ll
   total 4390172
   -rw-r--r--. 1 root root    41070592  Sep 26 07:33 CloudbaseInitSetup_x64.msi
   -rw-r--r--. 1 qemu qemu  4413020160  Sep 26 02:36 cn_windows_server_2012_r2_x64_dvd_2707961.iso
   ```

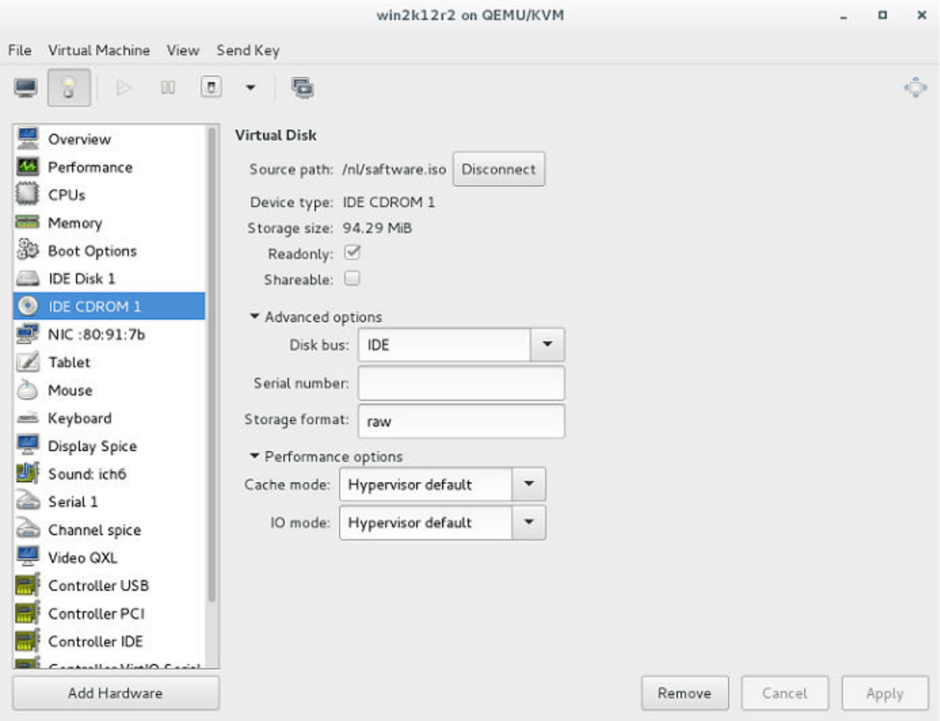
   Run the following command in the directory where the installation package is stored:

   mkisofs -L -R -J -T -V system-sp2 -o *software*.**iso CloudbaseInitSetup_x64.msi**
3. Mount the generated ISO file to the VM and install Cloudbase-Init.
   a. On virt-manager, choose **View** > **Details**.
   b. In the navigation pane on the left, choose **IDE CDROM 1**. In the right pane, click **Disconnect**.
   c. Click **Connect**.
   d. Select the local ISO file and click **Open** in the upper right corner.



Name	Size	Modified
CloudbaseInitSetup_0_9_11_x64.msi	41.1 MB	07:33
cn_windows_server_2012_r2_x64_dvd_2707961.iso	4.4 GB	02:36
software.iso	41.4 MB	07:55

   e. Confirm the settings and click **Apply**.



Virtual Disk

Source path: /nl/saftware.iso

Device type: IDE CDROM 1

Storage size: 94.29 MiB

Readonly: ☑

Shareable: ☐

Advanced options

Disk bus: IDE

Serial number:

Storage format: raw

Performance options

Cache mode: Hypervisor default

IO mode: Hypervisor default

4. Install Cloudbase-Init.

   Double-click the Cloudbase-Init installation package in the CD-ROM drive. The default installation path of Cloudbase-Init is:

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

5. Edit the Cloudbase-Init configuration file **cloudbase-init.conf**.

   Use a text editor (such as Notepad) to open the **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf** file and edit the file as follows:

   a. Create user **Administrator** and add it to a group.

   ```
   username=Administrator
   groups=Administrators
   ```

   b. Configure **hostname** and modify the following parameter (if it does not exist, add it):

   ```
   netbios_host_name_compatibility=false
   ```

   c. Locate and modify **logging_serial_port_settings** as follows:

   ```
   logging_serial_port_settings=COM1,115200,N,8
   ```

   d. Add parameter **metadata_services** and configure the loaded services as follows:

   ```
   metadata_services=cloudbaseinit.metadata.services.httpservice.HttpService,cloudbaseinit.metadat
   a.services.configdrive.ConfigDriveService
   ```

   e. Add parameter **plugins** to configure the plugins that will be loaded. Separate different plugins with commas (,). The information in bold is the keyword of each plugin.

      - Mandatory plugins:

        ```
        plugins=cloudbaseinit.plugins.common.localscripts.LocalScriptsPlugin,cloudbaseinit.plugins
        .common.mtu.MTUPlugin,cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,clou
        dbaseinit.plugins.common.setuserpassword.SetUserPasswordPlugin,cloudbaseinit.plugins.c
        ommon.sshpublickeys.SetUserSSHPublicKeysPlugin,cloudbaseinit.plugins.common.sethost
        name.SetHostNamePlugin,cloudbaseinit.plugins.windows.extendvolumes.ExtendVolumes
        Plugin,cloudbaseinit.plugins.common.userdata.UserDataPlugin,cloudbaseinit.plugins.wind
        ows.licensing.WindowsLicensingPlugin
        ```

        Plugin functions:

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

  - Optional plugins:

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

    Plugin functions:

    - **ConfigWinRMListenerPlugin**: sets listening to remote login.
    - **ConfigWinRMCertificateAuthPlugin**: sets remote login without the password authentication.

⚠ CAUTION

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

4.8 (Optional) Installing bms-network-config

Scenario

network-config works with Cloudbase-Init to configure the BMS network.

Prerequisites

- You have logged in to the VM.
- Cloudbase-Init has been installed.

Procedure

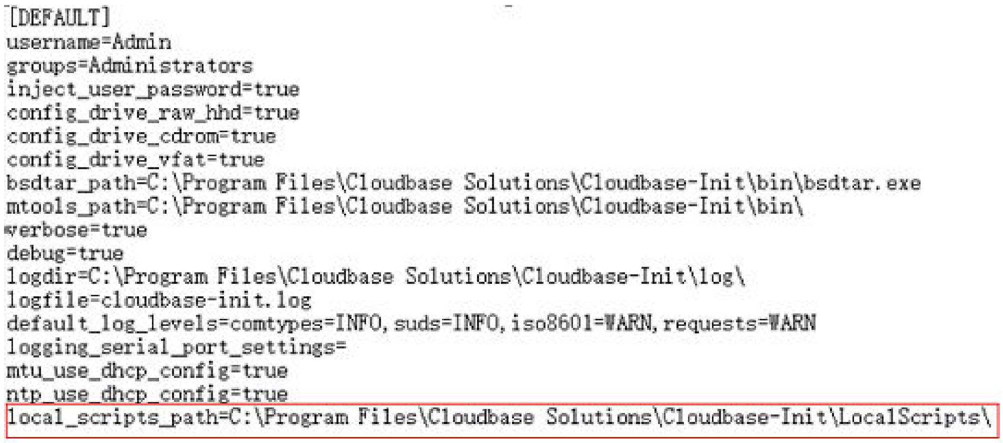
1. Download the bms-network-config software package and SHA256 checksum by referring to **Software** and very the software package integrity (for details, see**How Do I Verify Software Package Integrity?**).

   Decompress the package to the **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts\** directory.

   NOTE

   The value of **bsdtar_path** in the **bms-network-config.conf** file is **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\bsdtar.exe** by default. If Cloudbase-Init is installed in a non-default directory, set this parameter to the directory where **bsdtar.exe** is actually stored.

2. Use a text editor (such as Notepad) to open the Cloudbase-Init configuration file in the **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf** directory and check the path specified by **local_scripts_path**. Cloudbase-Init will execute the scripts from this path.



```
[DEFAULT]
username=Admin
groups=Administrators
inject_user_password=true
config_drive_raw_hhd=true
config_drive_cdrom=true
config_drive_vfat=true
bsdtar_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\bsdtar.exe
mtools_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\
verbose=true
debug=true
logdir=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\log\
logfile=cloudbase-init.log
default_log_levels=comtypes=INFO,suds=INFO,iso8601=WARN,requests=WARN
logging_serial_port_settings=
mtu_use_dhcp_config=true
ntp_use_dhcp_config=true
local_scripts_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts\
```

3. Copy **bms-network-config.py** to the **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts** directory based on the value of parameter **local_scripts_path** in the Cloudbase-Init configuration file.

   The default path of Cloudbase-Init is recommended. If you store the script file in another directory, change the value of parameter **local_scripts_path** in the Cloudbase-Init configuration file.

4.9 (Optional) Installing the SDI Driver

With the SDI driver, EVS disks can be attached to BMSs. The EVS disks can be used as system disks from which the BMSs are booted. This facilitates quick BMS provisioning. If you do not need to use EVS disks or your BMS does not have SD1 cards, skip this section.

Prerequisites

- You have logged in to the VM.
- You have downloaded the SDI driver (scsi_ep_front) as instructed in **Software** and have uploaded it to the VM.

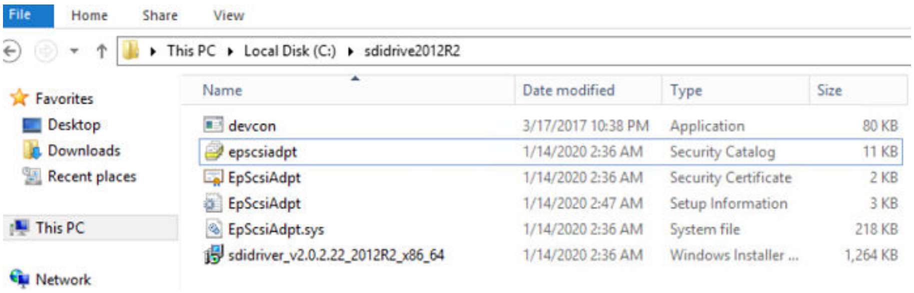
  NOTE

  The scsi_ep_front version must be 2.0.2.12 or later.
- WDK has been installed.

  Download WDK from **http://download.microsoft.com/download/4/E/0/4E07EAAD-E394-4EA8-B2B8-D46E46A409C5/wdk/wdksetup.exe**.

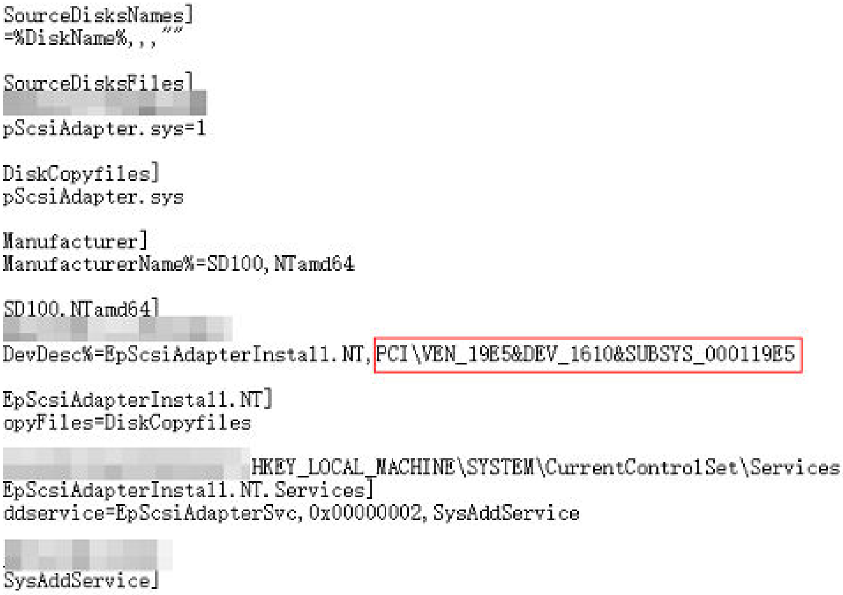
Procedure

1. Obtain the device management tool **devcon.exe** from the WDK directory **C:\Program Files (x86)\Windows Kits\10\Tools\x64**, and place **devcon.exe** in the same directory as the SDI driver.



Name	Date modified	Type	Size
devcon	3/17/2017 10:38 PM	Application	80 KB
epscsiadpt	1/14/2020 2:36 AM	Security Catalog	11 KB
EpScsiAdpt	1/14/2020 2:36 AM	Security Certificate	2 KB
EpScsiAdpt	1/14/2020 2:47 AM	Setup Information	3 KB
EpScsiAdpt.sys	1/14/2020 2:36 AM	System file	218 KB
sdidriver_v2.0.2.22_2012R2_x86_64	1/14/2020 2:36 AM	Windows Installer ...	1,264 KB

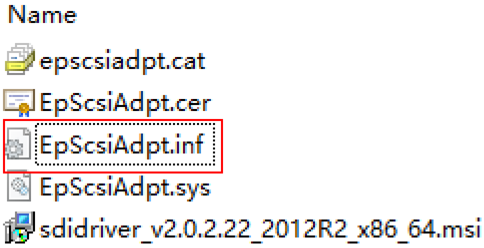
2. Find the EpScsiAdpt installation file and view the PCI ID.



```
SourceDisksNames]
=%DiskName%,,,""

SourceDisksFiles]
[redacted]
pScsiAdapter.sys=1

DiskCopyfiles]
pScsiAdapter.sys

Manufacturer]
ManufacturerName%=SD100,NTamd64

SD100.NTamd64]
[redacted]
DevDesc%=EpScsiAdapterInstall.NT,PCI\VEN_19E5&DEV_1610&SUBSYS_000119E5

EpScsiAdapterInstall.NT]
opyFiles=DiskCopyfiles

[redacted] HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
EpScsiAdapterInstall.NT.Services]
ddservice=EpScsiAdapterSvc,0x00000002,SysAddService

[redacted]
SysAddService]
```

3. Open the CLI, go to the directory where the SDI driver and device management tool are located, and run the following command:

   devcon install EpScsiAdpt.inf "*PCI|VEN_19E5&DEV_1610&SUBSYS_000119E5*"

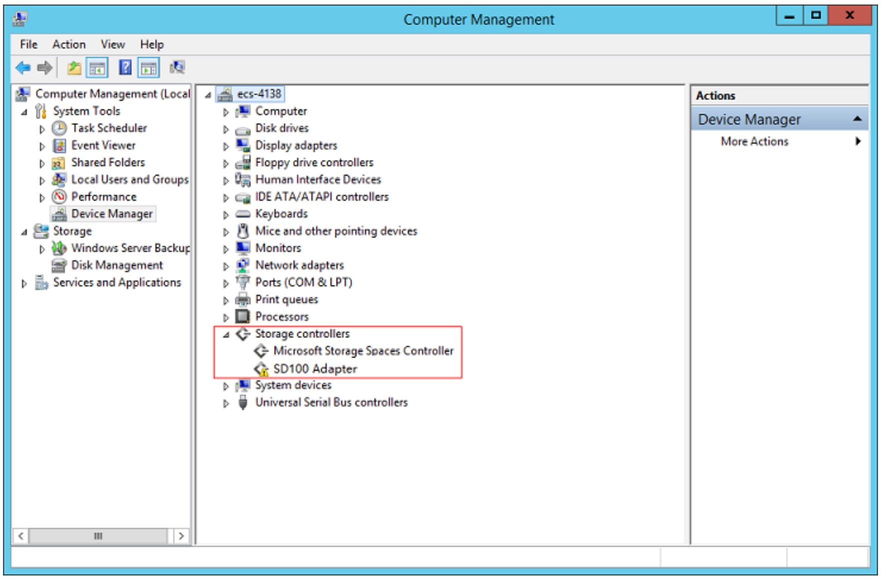


Name
epscsiadpt.cat
EpScsiAdpt.cer
EpScsiAdpt.inf
EpScsiAdpt.sys
sdidriver_v2.0.2.22_2012R2_x86_64.msi

   The PCI ID is an example only.

4. (Optional) Delete device nodes.

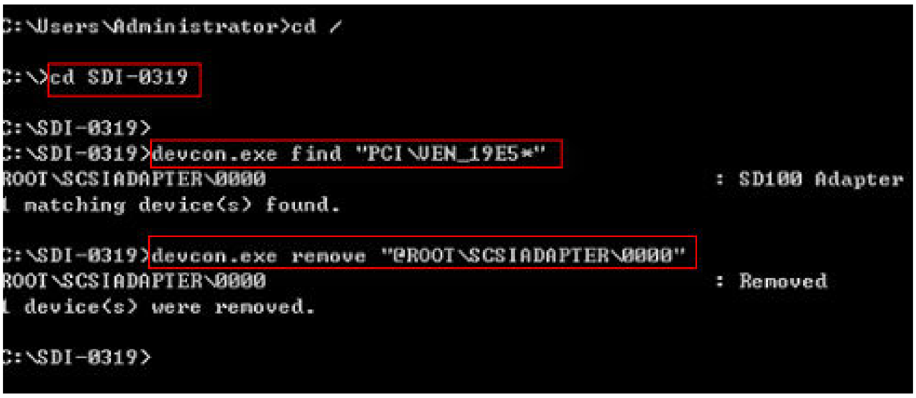
   a. If the environment where you create an image does not have SDI hardware, the storage controller in the device manager has exceptions.



b. Open the CLI, go to the directory where the SDI driver and devcon installation tool are stored, and delete the abnormal device nodes.

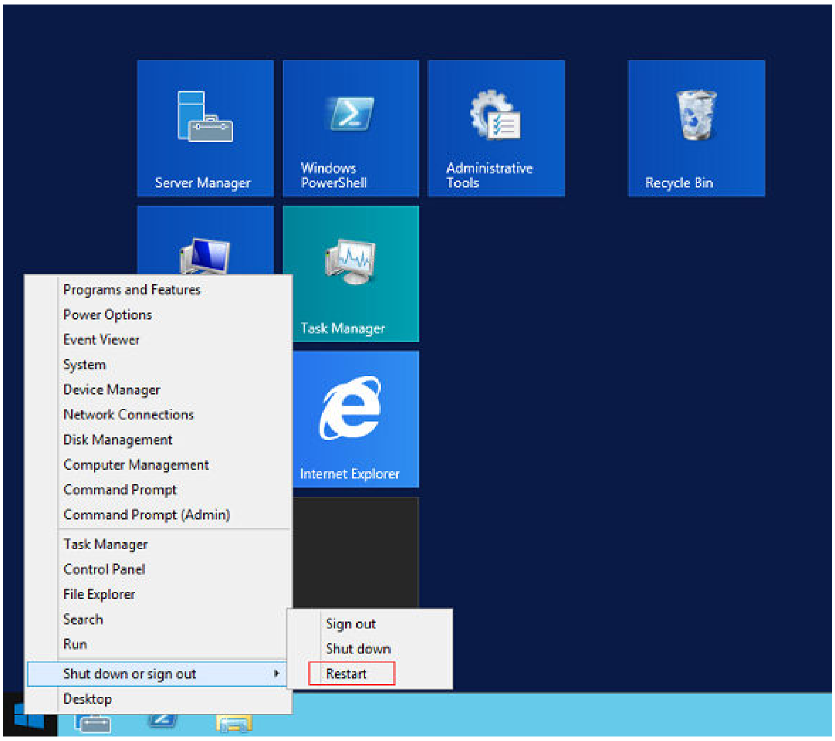
Run the **devcon.exe find "PCI\VEN_19E5*"** command to locate abnormal device nodes.

Run the **devcon.exe remove "@ROOT\SCSIADAPTER\0000"** command to delete the nodes.



```
C:\Users\Administrator>cd /

C:\>cd SDI-0319

C:\SDI-0319>
C:\SDI-0319>devcon.exe find "PCI\VEN_19E5*"
ROOT\SCSIADAPTER\0000                                       : SD100 Adapter
1 matching device(s) found.

C:\SDI-0319>devcon.exe remove "@ROOT\SCSIADAPTER\0000"
ROOT\SCSIADAPTER\0000                                       : Removed
1 device(s) were removed.

C:\SDI-0319>
```

c. Restart the VM.



d. Check whether the exceptions in the storage controller are cleared.

4.10 Setting the Windows Time Zone

Linux uses the time of the motherboard CMOS chip as the Coordinated Universal Time (UTC) and determines the system time based on the configured time zone. However, Windows uses the CMOS time as the system time directly without converting it based on the time zone. You need to perform the following steps:

1. Log in to the Windows VM.
2. Click ⊞ in the lower left corner, choose **Windows PowerShell**, and enter **regedit.exe** to open the registry.
3. In the displayed **Registry Editor** window, choose **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **TimeZoneInformation**.
4. In the right pane, right-click a blank area and choose **New** > **DWORD (32-bit) Value** to add a REG_DWORD code. Set its name to **RealTimeIsUniversal** and value to **1**.

   NOTE

   If the operations cannot be performed by using a mouse, you can use the keyboard instead.

4.11 Setting the Windows Virtual Memory

NOTE

You need to set virtual memory only for Windows Server 2012 R2 and Windows Server 2016.

BMS memory is large. Therefore, the automatically allocated virtual memory will take up a lot of system disk space. You are advised to disable the virtual memory or set an upper limit for it.

1. Log in to the Windows VM.
2. Click ⊞ in the lower left corner, right-click **This PC**, and choose **Properties** from the shortcut menu.

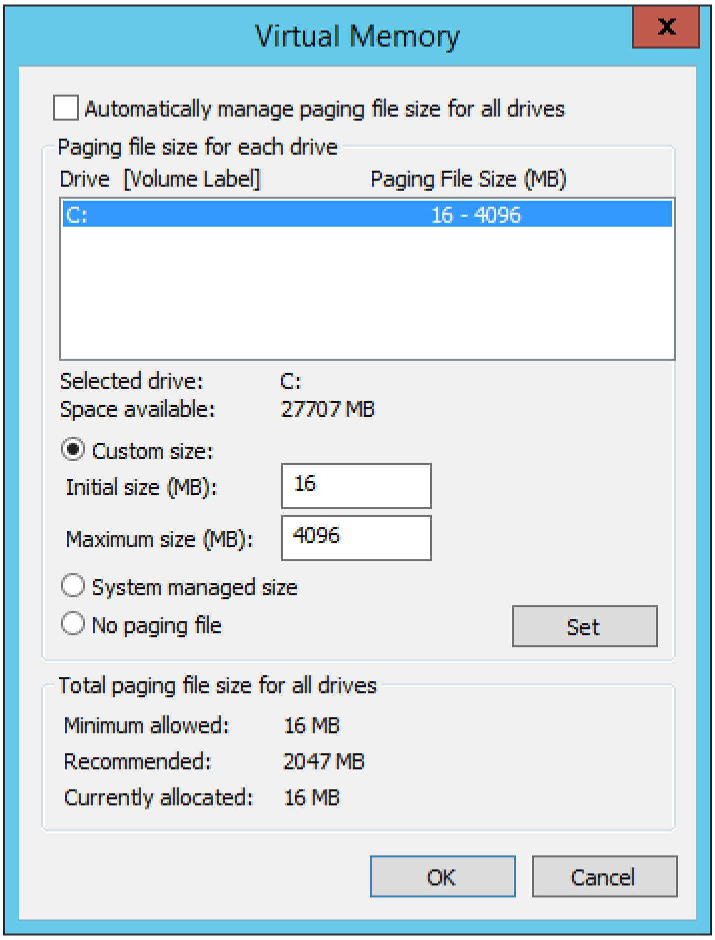
   The **System** page is displayed.
3. In the navigation pane on the left, choose **Advanced system settings**.

   The **System Properties** dialog box is displayed. By default, the **Advanced** tab is active.
4. In the **Performance** area, click **Settings**.

   The **Performance Options** dialog box is displayed.
5. Click the **Advanced** tab, and click **Change** in the **Virtual memory** area.

   The **Virtual Memory** dialog box is displayed.

Figure 4-17 Virtual Memory dialog box



Virtual Memory

□ Automatically manage paging file size for all drives

Paging file size for each drive

Drive [Volume Label]	Paging File Size (MB)
C:	16 - 4096

Selected drive: C:
Space available: 27707 MB

● Custom size:
Initial size (MB): 16
Maximum size (MB): 4096

○ System managed size
○ No paging file

Total paging file size for all drives

Minimum allowed: 16 MB
Recommended: 2047 MB
Currently allocated: 16 MB

6. Deselect **Automatically manage paging file size for all drives**.
7. To disable the virtual memory, select **No paging file**. To set an upper limit for the virtual memory, select **Custom size**. You are advised to set the maximum virtual memory to less than 2 GB.

8. Click **Set**, In the displayed dialog box, select **Yes**.
9. Click **OK**.
10. Restart the VM to complete the virtual memory settings.

4.12 (Optional) Configuring Automatic Windows Update

You can manually configure Windows Server so that you will be reminded about important Windows updates.

Procedure

The following procedure is for reference only. For detailed operations, see the procedure provided by the Windows official website.

1. Log in to the Windows VM.
2. Click ⊞ in the lower left corner to start Server Manager.
3. In the navigation pane on the left, choose **Local Server**. In the right pane, locate **Windows Update** and click the link that follows it.
4. On the **Windows Update** page, click **Install updates automatically**.

   NOTE

   Determine whether to enable automatic Windows update based on the site requirements. Do not interrupt the update until it is finished.

4.13 Configuring the SID

NOTICE

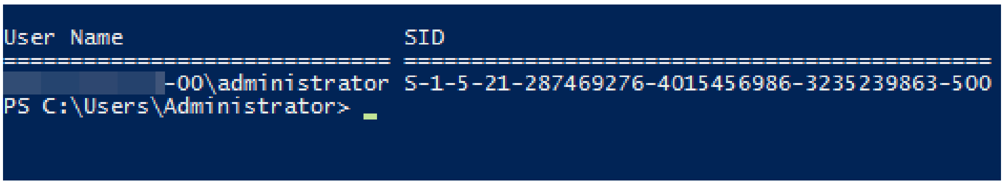
This is the last step for VM configuration. Due to the Cloudbase-Init mechanism, after the VM used to create an image is restarted, a random password is generated, and the VM cannot be logged in. Therefore, confirm the VM configuration before performing operations in this section.

A Security Identifier (SID) is a unique value that identifies a user, group, or computer account.

Only Windows Server 2016 requires SID configuration during image creation. For how to configure a SID for Windows Server 2012 R2, see **Bare Metal Server User Guide**.

1. Log in to the Windows VM.
2. Click ⊞ in the lower left corner, choose **Windows PowerShell**, and run the **whoami /user** command to check the SID.

Figure 4-18 Querying the original SID



```
User Name                    SID
============================ =============================================
[redacted]-00\administrator S-1-5-21-287469276-4015456986-3235239863-500
PS C:\Users\Administrator> _
```

3. Modify the Cloudbase-Init configuration files.

   a. Open the **cloudbase-init.conf** and **cloudbase-init-unattend.con** files.

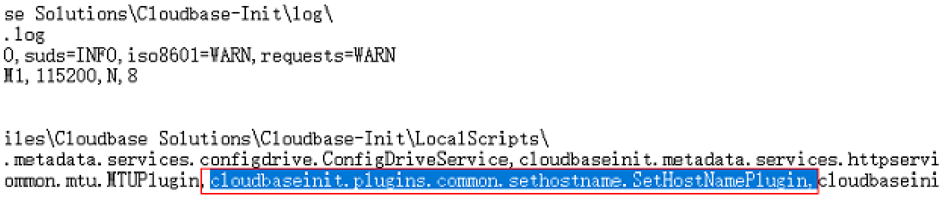
      File directory: **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf**

   b. Add **first_logon_behaviour=no** to both files.

```
[DEFAULT]
username=Administrator
groups=Administrators
first_logon_behaviour=no
netbios_host_name_compatibility=false
metadata_services=cloudbaseinit.metadata.services.httpser
inject_user_password=true
...
```

   c. Delete **cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin** from the **cloudbase-init-unattend.conf** configuration file.

Figure 4-19 Modifying the configuration file



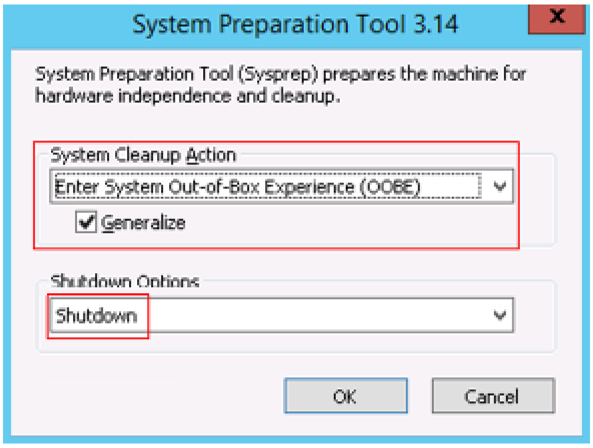
```
se Solutions\Cloudbase-Init\log\
.log
0,suds=INFO,iso8601=WARN,requests=WARN
M1,115200,N,8


iles\Cloudbase Solutions\Cloudbase-Init\LocalScripts\
.metadata.services.configdrive.ConfigDriveService,cloudbaseinit.metadata.services.httpservi
ommon.mtu.MTUPlugin,cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin,cloudbaseini
```

4. Open the CLI and run the following command to open the Sysprep window:

```
C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf>
C:\Windows\System32\Sysprep\sysprep.exe /unattend:Unattend.xml
```

5. Configure the parameters shown in the following figure.

Figure 4-20 System Preparation Tool settings



System Preparation Tool 3.14

System Preparation Tool (Sysprep) prepares the machine for hardware independence and cleanup.

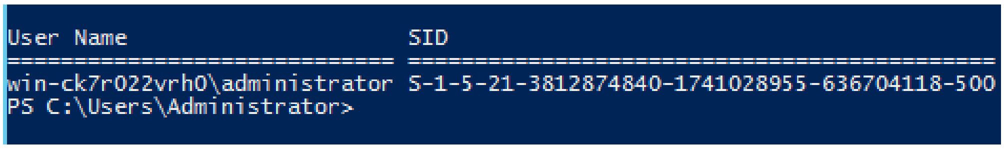
System Cleanup Action: Enter System Out-of-Box Experience (OOBE)

☑ Generalize

Shutdown Options: Shutdown

6. After the configuration is complete, the BMS automatically restarts. You need to encapsulate and decompress the system again. Log in to the VM and query the SID as instructed in 2.

Figure 4-21 Viewing the new SID



```
User Name                    SID
============================ ============================================
win-ck7r022vrh0\administrator S-1-5-21-3812874840-1741028955-636704118-500
PS C:\Users\Administrator>
```

As shown in the preceding figure, the SID has been changed successfully.

5 Stopping the VM and Obtaining the Image

Stopping the VM

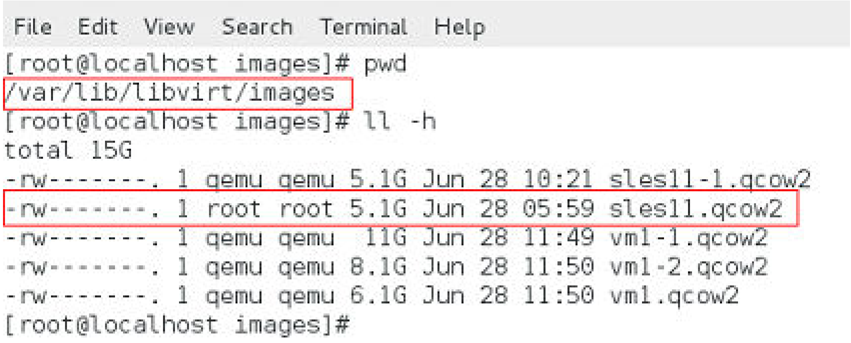
You can run the **sudo poweroff** command in the VM to stop it. If it cannot be stopped, on virt-manager, click **Virtual Machine Manager**, select the VM and right-click **Shut Down**.

If the VM still cannot be stopped, you are advised to click **Force Off** to forcibly stop it.

Generating an Image File

If you choose to automatically create the image, the .qcow2 or .img image file is stored in the **/var/lib/libvirt/images** directory on the host.

Figure 5-1 Image file (Linux)



```
[root@localhost images]# pwd
/var/lib/libvirt/images
[root@localhost images]# ll -h
total 15G
-rw-------. 1 qemu qemu 5.1G Jun 28 10:21 sles11-1.qcow2
-rw-------. 1 root root 5.1G Jun 28 05:59 sles11.qcow2
-rw-------. 1 qemu qemu  11G Jun 28 11:49 vm1-1.qcow2
-rw-------. 1 qemu qemu 8.1G Jun 28 11:50 vm1-2.qcow2
-rw-------. 1 qemu qemu 6.1G Jun 28 11:50 vm1.qcow2
[root@localhost images]#
```

If you choose to manually create the image, obtain the image file from your specified directory.

Compressing the Image File

If the generated image file is too large, run the following command to compress it:

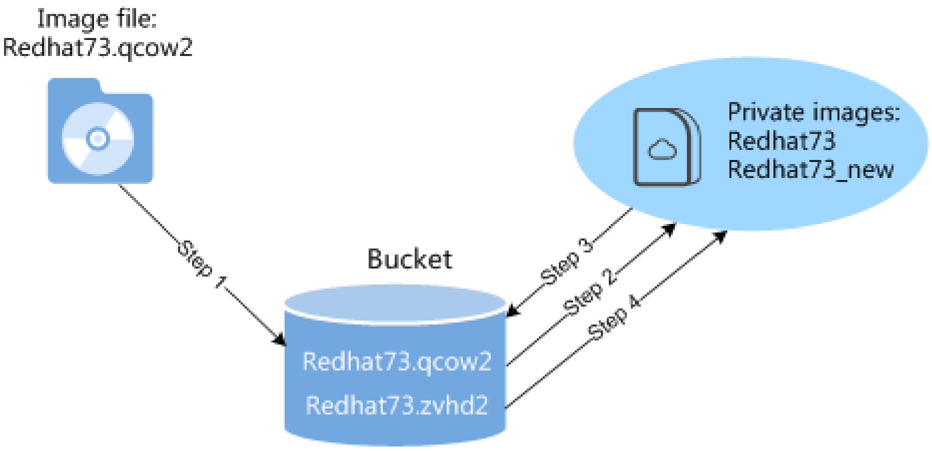
qemu-img convert -f raw -O qcow2 *SourceFile FinallyFile.qcow2*

SourceFile can be in .img or .qcow2 format.

6 Converting the Image Format

For BMS, the image format can only be ZVHD2. After obtaining an image file, convert its format to ZVHD2.

Figure 6-1 Converting the image format



Step 1: Upload the image file (for example, **Redhat73.qcow2**) to an OBS bucket.

Step 2: Register the image file as a private image (for example, **Redhat73**). For details, see "Creating a Private Image from an External Image File" in *Bare Metal Server User Guide*.

Step 3: Export the private image to an OBS bucket in ZVHD2 format, for example, **Redhat73.zvhd2**. For details, see "Exporting Images" in *Image Management Service User Guide*.

Step 4: Register the image file in ZVHD2 format in the OBS bucket as a private image (for example, **Redhat73_new**).

NOTE

The image format has been converted to ZVHD2 in Step 3. If you want to use the private image to create a BMS, you need to register the private image as instructed in Step 4.

7 FAQ

7.1 What Can I Do If Packets from the VLAN Subinterface of bond0 of a Linux BMS Use the MAC Address of bond0 as the Source MAC Address?

This is a known Linux kernel issue that will result in ping failures from BMS extension NICs to the gateway. This issue is known in the OSs listed in **Table 7-1**. Obtain a patch based on the kernel version from the OS vendor to rectify this issue.

Table 7-1 OS type and kernel version

OS	Kernel Version
Red Hat 7.2	3.10.0-327
Red Hat 7.3	3.10.0-514
Red Hat 7.4	3.10.0-693
CenOS 7.0	3.10.0-514
CentOS 7.2	3.10.0-327
CentOS 7.3	3.10.0-514
CentOS 7.4	3.10..0-693
EulerOS 2.2	3.10.0-327
Ubuntu 14.04	3.13.0-24

7.2 What Can I Do If IP Links Are Disconnected Due to the Incorrect Bond Port Mode Configured by the Wicked Module of SUSE 12 SP1?

This is a known Wicked issue. You are advised to upgrade Wicked to 0.6.40.28 for rectifying this issue. Download wicked from the official website **https://software.opensuse.org/package/wicked**.

7.3 How Do I Set the BMS CPU Frequency Governor?

Generally, CPU frequency governors include **performance**, **powersave**, and **ondemand**. You can select a one based on service requirements.

Assume that you want to set the CPU frequency governor to **performance**.

- Red Hat 6

  Make the following modification in the **/etc/sysconfig/cpuspeed** file:

  ```
  GOVERNOR=performance
  ```

- Red Hat 7

  Make the following modification in the **/etc/sysconfig/cpupower** file:

  ```
  CPUPOWER_START_OPTS="frequency-set -g performance"
  ```

- Debian Gnu/Linux 8

  Make the following modification in the **/etc/init.d/cpufrequtils** file:

  ```
  GOVERNOR="performance"
  ```

NOTE

- You can run the **yum install** *Software name* command to install the software you need, or download the software (.rpm package) from the official website and install it.
- You can configure a script for Red Hat 6 to automatically load the intel_pstate driver and make the preceding configurations take effect upon OS startup.
  1. Run the following command to create the **intel_pstate.modules** file:

     vi /etc/sysconfig/modules/intel_pstate.modules
  2. Add the following information into the file:
     ```
     /sbin/modprobe intel_pstate > /dev/null 2>&1
     ```
  3. Press **Esc** and enter **:wq!** to save the configuration.
  4. Run the following commands to modify the file permission:

     chmod 755 /etc/sysconfig/modules/intel_pstate.modules

7.4 What Do I Do If Cloudbase-Init Is Stopped on a Provisioned Windows BMS?

NOTE

If you cannot log in to or perform operations on BMC, contact Huawei technical support.

Symptom

If Cloudbase-Init is stopped after a Windows BMS is provisioned, and information "Failed to find trace ID description from Cloudbase-Init because the component triggering the trace is not installed or has been damaged. You can install or recover the component." is displayed, you need to reinstall Cloudbase-Init.

Solution

1. Log in to the BMS using BMC and back up the .conf files in the **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\** directory and all the files in the **LocalScripts** directory.
2. Download Cloudbase-Init from the official website.

   https://cloudbase.it/cloudbase-init/#download
3. Click **Remote Control** on the BMC host management page.

   The remote control window is displayed.
4. Click 💿 in the upper toolbar. Select **Directory** and click **Browse**.

   A dialog box is displayed.
5. Select the Cloudbase-Init package and click **Connect** to upload it to the BMS. The CD-ROM drive read and install the Cloudbase-Init.
6. Copy the files you backed up in step **1** to the new Cloudbase-Init directory.
7. Restart the BMS and check whether Cloudbase-Init runs properly.

7.5 What Can I Do If Data Cannot Be Injected into BMSs Due to cloud-init-local Failures?

Symptom

For Red Hat 7 or CentOS 7, cloud-init-local may fail to start up. As a result, BMS failed to inject data correctly. When you run the **systemctl status cloud-init-local.service** command, the message "OSError: [Errno 2] No such file or directory" is displayed.

Solution

For Red Hat 7 and CentOS 7, if the libselinux version is earlier than 2.5.7, cloud-init-local may fail to start up. This is a known issue and has been fixed in libselinux 2.5.7. For details, see **https://bugzilla.redhat.com/show_bug.cgi?id=1406520**. If you are creating a Red Hat 7 or CentOS 7 image, upgrade libselinux to 2.5.7 or later after you configure the yum source in section "Installing Cloud-Init > SUSE/Red Hat/CentOS/Oracle Linux/Ubuntu/Debian > CentOS".

7.6 How Do I Activate a Windows BMS?

Windows BMSs need to be activated manually.

1. Log in to the BMS.

2. Click **Start**, enter **cmd** in the **Type here to search** box to open the command-line interface (CLI).
3. Run the following command to configure the IP address of the Key Management Service (KMS) server:

   slmgr -skms 100.125.1.2
4. Run the following command to restart the BMS:

   slmgr -ato
   - The BMS is activated if a message similar to "Activated the product" is displayed, and no further action is required.
   - The BMS is not activated if the error 0xC004F074 (with description "The Key Management Server (KMS) is unavailable") occurs. Go to **5**.
5. Check whether the BMS system time is synchronized with the standard time. If it is not, synchronize it with the standard time.
6. Run the following command to check whether the BMS can connect to the KMS server port:

   telnet 100.125.1.2 1688

   If the connection fails, disable the firewall or enable TCP port 1688 on the firewall. Stop security software such as safedog if any.
7. Run the following command to check whether the BMS has been activated:

   slmgr -ato

7.7 How Do I Improve the UDP Packet Performance for x86 EulerOS 2.3?

Scenario

The iperf3 tool is used to test the maximum UDP bandwidth (1440-byte packets) and PPS (64-byte packets) with 0% packets lost. To acquire more UDP bandwidth and PPS, perform operations in this section.

Procedure

1. Log in to x86 EulerOS 2.3 in SSH mode and switch to user **root**.
2. Run the following command to back up **/etc/sysctl.conf**:

   cp /etc/sysctl.conf /root/sysctl.conf_bak
3. Use vim to append the following content to **/etc/sysctl.conf**:

   ```
   net.core.wmem_default =21299200
   net.core.rmem_default=21299200
   ```
4. Run the following command to make the configuration take effect:

   /sbin/sysctl -p

7.8 How Do I Verify Software Package Integrity?

Prerequisites

- A BMS has been created.
- You have obtained the software package and its SHA256 checksum.

Verifying Software Package Integrity (Linux)

1. Log in to the BMS as the **root** user.
2. Obtain the hash value of the software.

   sha256sum *{Local directory of the software package}***/***{Software package name}*

   Replace *{Local directory of the software package}* with the actual download directory.

   Replace *{Software package name}* with the actual name of the downloaded software package. For example, the name can be **qemu-img-hw.zip**.
3. Check whether the SHA256 hash value obtained in **Prerequisites** is consistent with that obtained in step **2**.
   - If they are consistent, the verification is successful.
   - If they are inconsistent, download the software package again and repeat steps **2** and **3** to verify it.

Verifying Software Package Integrity (Windows)

1. Log in to the BMS.
2. Open the cmd window as an administrator and run the following command to obtain the hash value of the software:

   certutil –hashfile *{Local directory of the software package}\{Software package name}* **SHA256**

   Replace *{Local directory of the software package}* with the actual download directory.

   Replace *{Software package name}* with the actual name of the downloaded software package. For example, the name can be **qemu-img-hw.zip**.
3. Check whether the SHA256 hash value obtained in **Prerequisites** is consistent with that obtained in step **2**.
   - If they are consistent, the verification is successful.
   - If they are inconsistent, download the software package again and repeat steps **2** and **3** to verify it.

A Appendix

A.1 Configuring the SSH Service

1. After Linux is installed on the host, open the Linux terminal and run the following command to check the SSH service status:

   service sshd status

   Check whether the SSH service is enabled and whether its status is **active**.

   – If the SSH service is not enabled, run the **service enable sshd** command.

   – If the status is not **active**, run the **service sshd start** command.

2. Modify the SSH service configuration file to enable user **root** to log in to the host using SSH.

   Configuration file path: **/etc/ssh/sshd_config**

   Set the value of **PermitRootLogin** to **yes**.

3. Run the following command to restart the SSH service after the configuration is complete:

   service sshd restart

A.2 Configuring the vsftpd Service

After Linux is installed on the host, open the Linux terminal and run the following command to check the vsftpd service status:

service vsftpd status

Check whether the vsftpd service is enabled and whether its status is **active**.

- If the vsftpd service is not enabled, run the **service enable vsftpd** command.
- If the vsftpd service status is not **active**, run the **service vsftpd start** command.

A.3 Configuring the VNC Service

1. Run the following command to check whether VNC Server has been installed on the host:

   rpm -qa | grep tigervnc-server

   Command output:

   ```
   tigervnc-server-1.1.0-5.e16.x86_64
   ```

   – If no command output is displayed or the command output shows that VNC Server is not installed, go to 2.

   – If the command output shows that VNC Server has been installed, go to 3.

2. (Optional) Install tigervnc-server.

   a. Run the **lsblk** command (the OS ISO file must have been mounted to the BMC virtual CD-ROM drive. If not, mount the ISO file in the same way as you mount it during OS installation).

      NOTE

      If you cannot log in to or perform operations on BMC, contact Huawei technical support.

   b. Locate the block device whose **name** is **sr0** and **type** is **rom**, and check whether any directories are mounted to the mount point. If no, run the following command:

      mount /dev/sr0 /mnt

   c. Enter the **/etc/yum.repos.d** directory where the configuration is stored and back up all **.repo** files. Use vim to create a **.repo** file, for example **tiger.repo**. The file content is as follows:

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

      Save the file and run the following commands:

      yum repolist

      yum install tigervnc-server

3. Run the following command to start the VNC service:

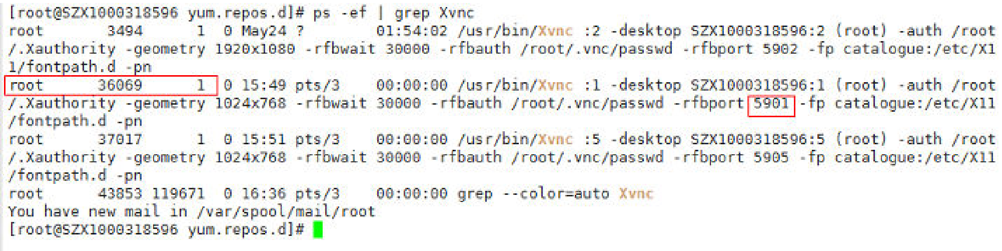
   vncserver

   Configure the VNC login password of user **root** as prompted.

   The command output contains **Log file is /root/.vnc/rhel:1.log**. **1** indicates that the first VNC virtual desktop is allocated to you.

4. Run the following command to check whether the Xvnc process exists:

   ps -ef | grep Xvnc

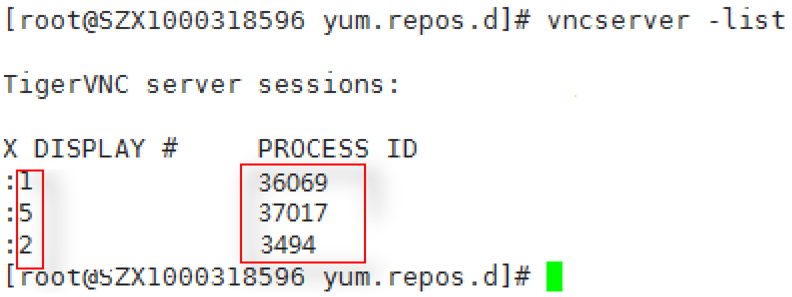


```
[root@SZX1000318596 yum.repos.d]# ps -ef | grep Xvnc
root      3494      1  0 May24 ?        01:54:02 /usr/bin/Xvnc :2 -desktop SZX1000318596:2 (root) -auth /root
/.Xauthority -geometry 1920x1080 -rfbwait 30000 -rfbauth /root/.vnc/passwd -rfbport 5902 -fp catalogue:/etc/X1
1/fontpath.d -pn
root     36069      1  0 15:49 pts/3    00:00:00 /usr/bin/Xvnc :1 -desktop SZX1000318596:1 (root) -auth /root
/.Xauthority -geometry 1024x768 -rfbwait 30000 -rfbauth /root/.vnc/passwd -rfbport 5901 -fp catalogue:/etc/X11
/fontpath.d -pn
root     37017      1  0 15:51 pts/3    00:00:00 /usr/bin/Xvnc :5 -desktop SZX1000318596:5 (root) -auth /root
/.Xauthority -geometry 1024x768 -rfbwait 30000 -rfbauth /root/.vnc/passwd -rfbport 5905 -fp catalogue:/etc/X11
/fontpath.d -pn
root     43853 119671  0 16:36 pts/3    00:00:00 grep --color=auto Xvnc
You have new mail in /var/spool/mail/root
[root@SZX1000318596 yum.repos.d]#
```

The process ID is **36069**, port number is **5901**, and virtual desktop number is **1**.

5. Run the following command to check the VNC virtual desktop of the current user:

   vncserver -list



```
[root@SZX1000318596 yum.repos.d]# vncserver -list

TigerVNC server sessions:

X DISPLAY #     PROCESS ID
:1              36069
:5              37017
:2              3494
[root@SZX1000318596 yum.repos.d]#
```

   The current user has three virtual desktops, 1, 5, and 2.

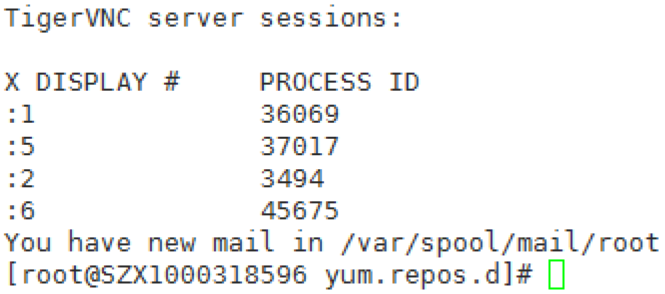
6. Connect VNC Viewer on the local Windows with VNC Server on the host to remotely log in to the host.

   Choose **Options** > **Expert** > **ColorLevel** to set **ColorLevel** to **rgb222** if the version of VNC Viewer is 5.3.2 when you install it for the first time.

7. Run the following command to add a virtual desktop for the current user:

   vncserver :*6*

   Run the **vncserver -list** command to check whether the virtual desktop is added successfully. As shown in the following figure, the virtual desktop 6 is added successfully.



```
TigerVNC server sessions:

X DISPLAY #     PROCESS ID
:1              36069
:5              37017
:2              3494
:6              45675
You have new mail in /var/spool/mail/root
[root@SZX1000318596 yum.repos.d]#
```

A.4 Mapping Between BMS Specifications and Drivers

NOTE

"-" in the tables indicates that this parameter is not required.

- **Table A-2** lists the OSs supported by x86 V4 BMSs with Intel Broadwell CPU.
- **Table A-2** lists the OSs supported by x86 V5 BMSs with Intel Skylake CPU.
- **Table A-4** lists the OSs supported by x86 V6 BMSs with Intel Cascade Lake CPU.
- **Table A-4** lists the OSs supported by BMSs with Kunpeng CPU.

Table A-1 Mapping between BMS specifications and drivers

BMS		Driver							
BMS Type	OS	Server Driver	SDI Driver	Hi1822 Normal NIC Driver / Management Component	Hi1822 Offloading NIC Driver	IB Driver	GPU Driver	Multipath Software	bms-network-config
s4	Windows	x86 V5 BMS driver	Required	-	-	-	-	Required by BMSs with HBA cards	Required
	CentOS/EulerOS/RedHat/Oracle	x86 V5 BMS driver	Required	-	-	-	-	Required by BMSs with HBA cards	Required
	Ubuntu	x86 V5 BMS driver	Required	-	-	-	-	Required by BMSs with HBA cards	Required
	SLES	x86 V5 BMS driver	Required	-	-	-	-	Required by BMSs with HBA cards	Required
	Debian	x86 V5 BMS driver	Required	-	-	-	-	Required by BMSs with HBA cards	Required

BMS		Driver								
d2 or io2	Windows	x86 V5 BMS driver	-	-	-	-	-	-	Required
	CentOS/EulerOS/RedHat/Oracle	x86 V5 BMS driver	-	-	-	-	-	-	Required
	Ubuntu	x86 V5 BMS driver	-	-	-	-	-	-	Required
	SLES	x86 V5 BMS driver	-	-	-	-	-	-	Required
	Debian	x86 V5 BMS driver	-	-	-	-	-	-	Required
h2	CentOS/EulerOS/RedHat/Oracle	x86 V5 BMS driver	Required	-	-	Required	-	-	Required
	Ubuntu	x86 V5 BMS driver	Required	-	-	Required	-	-	Required
p3	CentOS/EulerOS/RedHat/Oracle	x86 V5 BMS driver	Required	Required	-	Required	Required	-	Required

BMS		Driver							
	Ubuntu	x86 V5 BMS driver	Required	Required	-	Required	Required	-	Required
a/r/k (Kunpeng)	CentOS/ EulerOS/ Ubuntu	TaiShan BMS driver	-	Required	Required by BMSs with SDI cards	-	-	-	Required by BMSs without SDI cards

Table A-2 Mapping between x86 V4 BMS specifications and drivers

BMS Type	OS	Server Driver	SDI Driver	Hi1822 Driver / Management Component	IB Driver	GPU Driver	Multipath Software	bms-network-config
s4	Windows	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required
	CentOS/ EulerOS/ RedHat/ Oracle	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required
	Ubuntu	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required

BMS Type	OS	Server Driver	SDI Driver	Hi1822 Driver / Management Component	IB Driver	GPU Driver	Multipath Software	bms-network-config
	SLES	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required
	Debian	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required

Table A-3 Mapping between x86 V5 BMS specifications and drivers

BMS Type	OS	Server Driver	SDI Driver	Hi1822 Driver / Management Component	IB Driver	GPU Driver	Multipath Software	bms-network-config
s4	Windows	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required
	CentOS/ EulerOS/ RedHat/ Oracle	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required

BMS Type	OS	Server Driver	SDI Driver	Hi1822 Driver / Management Component	IB Driver	GPU Driver	Multipath Software	bms-network-config
	Ubuntu	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required
	SLES	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required
	Debian	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required

Table A-4 Mapping between x86 V6 BMS specifications and drivers

BMS Type	OS	Server Driver	SDI Driver	Hi1822 Driver / Management Component	IB Driver	GPU Driver	Multipath Software	bms-network-config
s4	Windows	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required

BMS Type	OS	Server Driver	SDI Driver	Hi1822 Driver/Management Component	IB Driver	GPU Driver	Multipath Software	bms-network-config
	CentOS/EulerOS/RedHat/Oracle	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required
	Ubuntu	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required
	SLES	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required
	Debian	x86 V5 BMS driver	Required	-	-	-	Required by BMSs with HBA cards	Required

Table A-5 Mapping between Kunpeng BMS specifications and drivers

BMS Type	OS	Server Driver	Hi1822 Normal NIC Driver / Management Component	Hi1822 Offloading NIC Driver	IB Driver	GPU Driver	Multipath Software	bms-network-config
a/r/k (Kunpeng)	CentOS/ EulerOS/ Ubuntu	TaiShan BMS driver	Required by BMSs with Hi1822 normal NIC	Required by BMSs with SDI cards	-	-	Required by BMSs with HBA cards	Required by BMSs without SDI cards

B Change History

Released On	Description
2023-09-04	This issue is the second official release. Added the links for downloading SHA256 checksums and described how to verify software package integrity with SHA256 checksums. For details, see: **Software**, **Tools**, **Installing bms-network-config**, **Preparing Hardware and Software**, **Installing Cloudbase-Init**, **(Optional) Installing bms-network-config**, and **How Do I Verify Software Package Integrity?**
2022-09-30	This issue is the first official release.