Hewlett Packard Enterprise

Installing Operating Systems on HPE Superdome Flex 280 Server

Part Number: 10-192004-Q422a
Published: October 2022
Edition: 6

Installing Operating Systems on HPE Superdome Flex 280 Server

Abstract

Operating system software and HPE Foundation Software installation and configuration on HPE Superdome Flex 280 Server

Part Number: 10-192004-Q422a
Published: October 2022
Edition: 6

Notices

Acknowledgments

Revision history

Part number	Publication date	Edition	Summary of changes
10-192004-Q422a	October 2022	6	Updated following sections for OpenStack Zed release:
10-192004-Q422	September 2022	5	Updated Installing HPE Foundation Software on RHEL, Installing HPE Foundation Software on SLES platforms using YaST, and Installing HPE Foundation Software on SLES platforms using Zypper.

10-192004-Q222	April 2022	4	• Added details related to firmware update in the following sections:
			  ◦ HPE Superdome Flex 280 Server I/O Service Pack
			  ◦ I/O firmware update with HPE OneView fails
			• Added a note in the Secure boot section.
			• HPE Foundation Software, Supported operating systems, Supported HFS version with Linux OS versions, and Supported OSs for HPE Persistent Memory on HPE Superdome Flex 280 Server

10-192004-Q321	June 2021	3	• Update list of OS versions supported for the server.

Part number	Publication date	Edition	Summary of changes
1012865453-IOS-1220	December 2020	2	• Update HFS 2.4 support statement and the list of Linux OSs supported for the server. • Minor updates for RHEL tasks.

Table of contents

HPE Superdome Flex 280 Server hardware and firmware setup and configuration

Subtopics

HPE Superdome Flex 280 Server system firmware bundle

The latest firmware recipe bundle for HPE Superdome Flex 280 Server system is available at **www.hpe.com/support/superdomeflex280-software**. Hewlett Packard Enterprise recommends running the latest firmware on your systems.

> **IMPORTANT:**
> Do not stop the firmware update while it is in progress. Doing so can place the system in an unusable state. Make sure that AC power to the system remains in place throughout the update process.

1. On the landing page, search for Firmware Bundle.

   The Manual, OneView, and SUM bundles are listed.

2. Choose either the **Manual** method, Smart Update Manager (**SUM**) method, or HPE OneView method from the firmware TAB under Drivers and Software.

   - **Manual** method: Choose the firmware bundle labeled for manual installation. This bundle can be installed or updated directly from the RMC with the installation instructions in the bundle, under Installation instructions.
   - **SUM** method: Choose the firmware bundle labeled for SUM installation. This bundle can be installed or updated from any system on the same network as the RMC using the included copy of the SUM tool. Follow the instructions in the bundle, under Installation instructions.
   - **HPE OneView** method: Choose the firmware bundle labeled for OneView installation. This bundle can be installed from the HPE OneView application. Follow the instructions in the bundle, under Installation instructions.

> **NOTE:**
> If a firmware mismatch error is displayed after an update, retry the update. If you continue to see failures, contact a support specialist.

For a list of Superdome Flex 280 Server components, see **www.hpe.com/support/superdomeflex280-release-sets**.

HPE Superdome Flex 280 Server I/O Service Pack

Customers can use the HPE Superdome Flex 280 Server I/O Service Pack to update I/O firmware using HPE Smart Update Manager or HPE OneView.

> **NOTE:** HPE OneView update requires to use HPE OneView version 6.6 or later and server firmware version 1.30.x or later.

The HPE Superdome Flex 280 Server I/O Service Pack ISO is available at **www.hpe.com/support/superdomeflex280-software**. This

service pack ISO image can be installed or updated with the install instructions under installation instructions.

Updated I/O drivers for HPE Superdome Flex 280 Server system are available in the I/O Service Pack. Install the I/O drivers after installing the operating system.

More information

- I/O firmware update with HPE OneView fails

Deploying Linux

Linux has multiple deployment options. You can choose the options that best meet the needs of your environment. You can use either an interactive or a scripted installation when installing the software.

Linux installation packages

The Linux operating systems must be obtained from the appropriate Linux vendor. Contact Red Hat, SUSE, or Oracle for instructions to obtain installation packages of the appropriate version of Linux.

HPE Foundation Software

The Linux HPE Foundation Software (HFS) provides updated kernel modules and scripts for use on HPE Foundation Software. It supports Red Hat Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Oracle Linux. HFS consists of software packages designed to ensure the smooth operation of HPE Superdome Flex 280 Server. HFS includes Data Collection Daemon (DCD), an agentless service that proactively monitors the health of hardware components.

Supported versions of HFS and Linux operating systems for Superdome Flex 280 Server are listed at:

https://downloads.linux.hpe.com/SDR/project/hpe-foundation/SD-Flex-LinuxSupportTables.html

HPE Data Collection Daemon

Data Collection Daemon (DCD) is an agentless service for HPE Superdome Flex Family. DCD proactively monitors the health of hardware components that are visible to the running operating system instance. Any errors are reported to management firmware running on the Rack Management Controller (RMC) for the server. The management service running on the RMC uses the data and serves it out of band to client applications like HPE Insight Remote Support (IRS).

DCD is bundled with the HPE Foundation Software and includes the following major features for Linux:

- DCD collects inventory data for the following listed components:
  - SAS/SATA controllers
  - Physical drives— Base Chassis Drives (Internal only)
  - RAID volumes (Logical drives)
  - Fibre Channel devices
  - Ethernet devices
  - NVMe controllers
  - GPU cards
  - Linux Host Operating System
- DCD proactively monitors the health of the host OS, SAS/SATA controllers, attached drives, RAID volumes, Fibre Channel devices,

Ethernet devices, and NVMe controllers. Any state change events are auto-forwarded to the RMC.

- The `dcdcli` command-line utility is provided to test the health of DCD service and its connectivity to the RMC and its clients.
- Logging is supported in DCD to log messages at different logging levels.
- All the data is transferred between DCD and RMC through an in-band IPMI Channel.
- DCD is delivered as an HPE signed and certified package.

Supported operating systems

HPE Superdome Flex 280 Server supports the following Windows and VMware operating systems. The most current list of supported Linux operating systems and HFS versions is available at:

https://downloads.linux.hpe.com/SDR/project/hpe-foundation/SD-Flex-LinuxSupportTables.html

Table 1. OS support for HPE Superdome Flex 280 Server

Operating Systems	Supported versions
Microsoft Windows	Windows 2022
	Windows 2019
	Windows 2016
VMware	VMware vSphere 7.0 U1, U2, U3

For the specific hardware configurations certified, see the OS vendor distribution sites.

- Red Hat Catalog:

  https://catalog.redhat.com/hardware/servers/search

- SUSE Catalog:

  https://www.suse.com/yessearch/

Supported HFS version with Linux OS versions

HPE Foundation Software systems with Linux OS environments require that HPE Foundation Software is also installed.

For information about server hardware supported by each HFS versions, see the HPE Foundation Software download page.

Go to **www.hpe.com/support/superdomeflex280-software** and select `Software (entitlement required)`. Select any bundle and click the Revision History tab to view information about all HFS versions.

The most current supported versions of HFS and Linux operating systems for Superdome Flex 280 Server Superdome Flex 280 servers are available at:

https://downloads.linux.hpe.com/SDR/project/hpe-foundation/SD-Flex-LinuxSupportTables.html

Supported OSs for HPE Persistent Memory on HPE Superdome Flex 280 Server

HPE Superdome Flex 280 Server systems with HPE Persistent Memory require specific OS versions. The following table lists Windows and VMware operating systems supported on HPE Superdome Flex 280 Server and indicates OS versions that can be used on systems with HPE Persistent Memory. A table of the Linux operating systems that support persistent memory on the HPE Superdome Flex 280 Server, along with the minimum kernel version of each Linux operating system is available at:

https://downloads.linux.hpe.com/SDR/project/hpe-foundation/SD-Flex-LinuxSupportTables.html

CAUTION:

When Oracle database is deployed on a standalone server, the persistent memory namespace where the Oracle redo logs reside must be configured with sector mode.

For best reliability, Hewlett Packard Enterprise recommends using sector mode namespaces for Oracle redo logs for both standalone server deployments and high availability solutions such as Oracle Data Guard.

For details about Oracle support of persistent memory, see customer bulletin **a00095559en_us**.

NOTE:

Hewlett Packard Enterprise recommends updating systems to use the latest versions of OS kernels and fixes. For more information, see **https://www.hpe.com/support/superdomeflex280-release-sets**.

Table 1. HPE Persistent Memory support by OSs

Supported OS	Supports HPE Persistent Memory	Kernel version
VMware vSphere 7.0 U3	No	
VMware vSphere 7.0 U2	No	
VMware vSphere 7.0 U1	No	
Windows 2022	Yes	
Windows 2019	Yes	
Windows 2016	No	

NOTE: Intel Optane Persistent Memory 200 series support requires firmware version starting from 1.10.272 or later.

Logging in to the system

Subtopics

Logging in to the RMC Web GUI

Prerequisites

- An Ethernet cable must be connected from the base chassis eRMC port to the manageability network.
- An IP address must be configured for the eRMC.

About this task

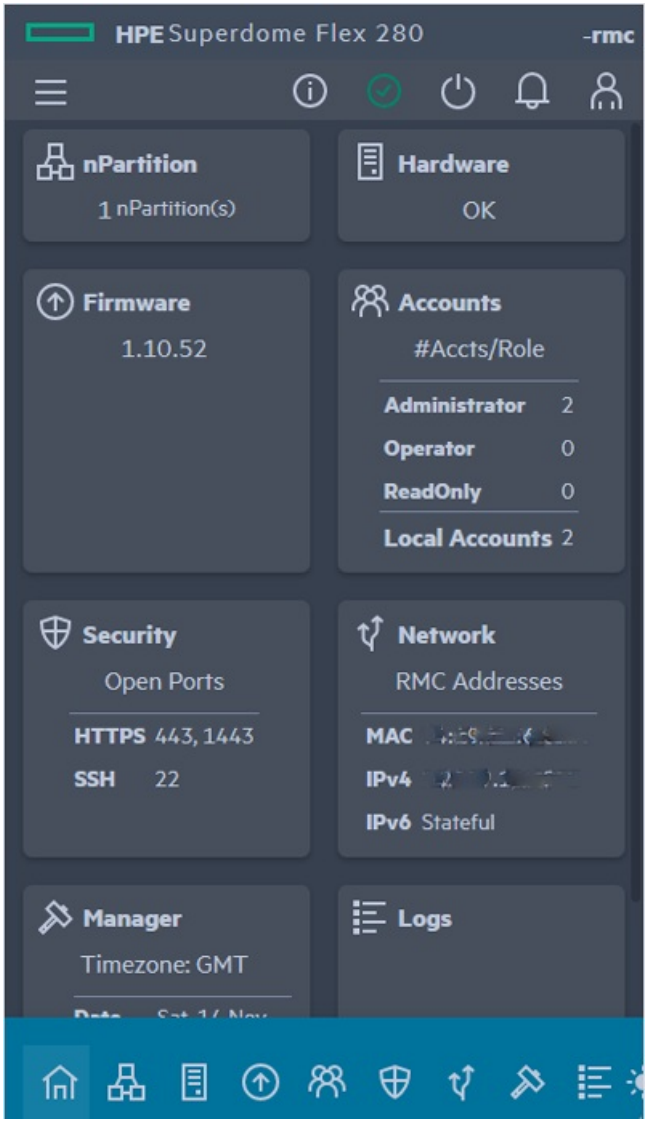
The RMC web GUI provides a management interface accessible by a web browser.

Procedure

1. Use a web browser to access the RMC web GUI at `https://RMC-IP-ADDRESS`.
2. Log in with an RMC user account and password.

   You can operate the RMC web GUI from a phone or desktop browser interface.

Figure 1. RMC web GUI phone view



Logging in to the RMC CLI through the CNSL port (Windows)

Prerequisites

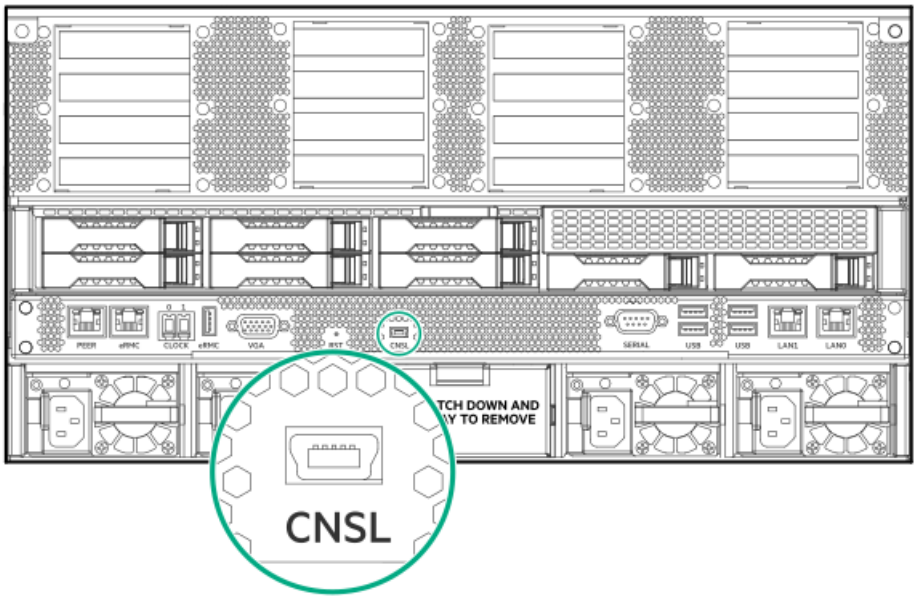
The FT230X device driver must be installed. You can download the device driver and setup instructions from https://www.ftdichip.com/Drivers/D2XX.htm. Windows 10 systems do not have the FT230X driver installed by default.

NOTE: CNSL connection with Windows 7 and Windows 8 are not supported.

Procedure

1. Connect a mini-USB cable between the Windows laptop port and the base chassis CNSL port.

   Figure 1. CNSL port on chassis rear



2. In Windows, use Settings > Device Manager > Ports (COM & LPT) to list the available COM ports.

3. Determine which COM port is assigned to the RMC. The BMC port enables RMC CLI access.

   In Windows, the Superdome Flex 280 Server port numbering can vary.

   Three COM ports represent the CNSL port. One COM port is the BMC port (RMC CLI), one is the SMC port (unused, no customer or service feature), and the other port also is unused.

4. Use PuTTY or another terminal program to connect to the COM port.

   Establish a serial connection at 115200 baud with 8 data bits, 1 stop bit, no parity, XON/XOFF flow control .

5. Press Enter to access the RMC CLI login prompt.

```
login as:
USER_NAME
```

```
Pre-authentication banner message from server:
| #------------------------------------------------------------------------
| # WARNING: This is a private system.  Do not attempt to login unless you are
| # an authorized user.  Any access and use may be monitored and can result in
| # criminal or civil prosecution under applicable law.
| #------------------------------------------------------------------------
| #
| # Firmware Bundle Version: 1.xx.xxx
| #
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
PASSWORD

End of keyboard-interactive prompts from server

HPE Superdome Flex 280 BMC,  Firmware Rev. 3.xx.xxx-xxxxxxxx_xxxxxx
(C) Copyright 2019-2021 Hewlett Packard Enterprise Development LP


================================================================================

Type "help" to see list of available commands.
Type "help <command>" to learn more about each command.

Enter <tab> to tab-complete a command.
Use cursor keys for command history.

HPE Rack Management Controller
(C) Copyright 2019-2021 Hewlett Packard Enterprise Development LP

================================================================================

example-rmc eRMC:r001u01c cli> help


Commands (type "help <command>" for more information):
=====================================================
acquit   clear       deconfig  generate  ping        remove   show
add      collect     disable   help      ping6       restore  test
apropos  commands    download  indict    power       save     update
backup   connect     enable    ipmi      reallocate  search   upload
cancel   deallocate  exit      modify    reboot      set


example-rmc eRMC:r001u01c cli>
```

Logging in to the RMC through the CNSL port (Linux)

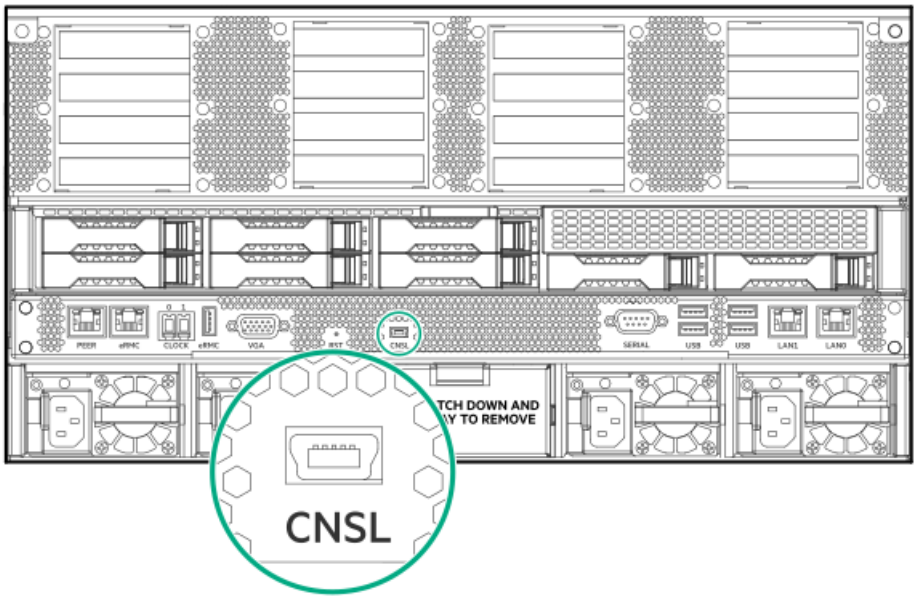
Prerequisites

The FT230X device driver must be installed. You can download the device driver and setup instructions from **https://www.ftdichip.com/Drivers/D2XX.htm**. Linux systems might have the FT230X driver installed by default.

Procedure

1. Connect a mini-USB cable between the laptop and the CNSL port on the base chassis.

   Figure 1. CNSL port on chassis rear



2. Use `cu` or `minicom` to connect to the `/dev/ttyACM1` device.

```
linux#
minicom -D /dev/ttyACM1
```

   Connect at 115200 baud using 8 data bits, 1 stop bit, no parity, XON/XOFF flow control .

3. Press Enter to access the RMC CLI prompt.

Zero configuration networking

The zero configuration feature simplifies the HPE Superdome Flex 280 Server installation or reconfiguration. The RMC serial connection is not required for installation and reconfiguration activities. To use the zero configuration feature, connect a PC or laptop network port directly to the Superdome Flex 280 Server RMC port, or connect a PC or laptop to the same local subnet of the Superdome Flex 280 Server RMC.

Subtopics

Configuring Superdome Flex 280 Server using Windows

Procedure

1. Connect a Windows PC or laptop to the RMC using a LAN cable between the PC and the port labeled RMC. Alternatively, connect the Windows PC or laptop to the same subnet of the RMC.
2. Disable Wi-Fi on the laptop.
3. Start a web browser on the PC or laptop.

   The supported browsers are Google Chrome, Firefox, and Microsoft Edge.

4. Disable the proxy usage during this direct-connect communication.

Table 1. Browser proxy settings

Google Chrome	Firefox	Microsoft Edge

Google Chrome	Firefox	Microsoft Edge
a. Go to Settings > Advanced > Open your computer's proxy settings The Automatic proxy setup page appears. b. Ensure that the setting of the following options are: • Automatically detect settings — Off • Use setup script —Off • Use a proxy server — Off	Go to Options > Network Settings >Settings > No proxy	a. Go to Settings > Advanced > Open Proxy Settings> Open Proxy settings The Automatic proxy setup page appears. b. Ensure that the setting of the following options is: • Automatically detect settings — Off • Use setup script —Off • Use a proxy server — Off

5. Unblock LLLMNR and mDNS ports.

   Ingress port 5355 must be open on the Windows PC or laptop. By default, port 5355 is open on Windows, but corporate IT firewall software can block this port. Check with your IT support personnel for instructions to open port 5355.

Subtopics

Access RMC

Access RMC

Use the RMC name on the factory label and access RMC either:

- Using a web browser

  or

- Using an SSH client

A factory label on the Superdome Flex 280 Server provides the RMC name in the `RMC<RMC MAC address>` format.

For example: RMC9440C9D602D9. The default user name and password is also printed on this label.

Subtopics

Using a web browser
Using an SSH client

Using a web browser

From a web browser on the PC or laptop, enter the `https://RMC<RMC MAC Address>` URL. For example: `https://rmc9440C9D602D9`.

To access the RMC from Windows, user must use `RMC<RMC MAC Address>` as the hostname.

The name resolution is case-insensitive, so lower-case is equivalent to upper case.

When the browser receives the LLMNR or mDNS response from the specified Superdome Flex 280 Server, it begins `https` communication with the Superdome Flex 280 Server using the Link-Local IP address. Log in with the user name and password printed on the pull tab label. The system can be configured using the web GUI and rebooted when complete.

Using an SSH client

You can also use an SSH client from the Windows PC or laptop.

1. SSH to the `RMC<RMC MAC Address>`.
2. Log in with the user name and password printed on the pull tab label.
3. After the Superdome Flex 280 Server has been configured, access the RMC web GUI using the new configured standard routable IP address.

The Zero configuration feature provides a persistent path for the administrator to communicate with the RMC without resorting to serial console access (given the "same local LAN" restrictions that are inherent to dynamic name resolution).

Configuring Superdome Flex 280 Server using Linux

Linux uses mDNS for dynamic name resolution. mDNS uses a domain of `.local`, which must be appended to the RMC name to inform Linux to use dynamic name resolution. The RMC name `RMC<RMC MAC Address>.local` must be used on Linux. For example, `RMC9440C9D602D9.local`. You can access RMC using one of the followings:

- Using the Linux system configured with routable IP address
- Using the Linux system connected to the Superdome Flex 280 Server

Subtopics

Using the Linux system configured with routable IP address

About this task

By default, a Linux system configured with routable IP address sends traffic intended for link local IP address to the gateway assigned to the default route, which does not know how to route link local packets. As a result, link local route must be added to the Linux system.

Procedure

1. Run the following command to add routing information for the link-local network:

   ```
   sudo ip route add 169.254.0.0/16 dev <ethXX>
   ```

   Modify the `ethXX` device. `ethXX` is the Linux network device connected to the same subnet as the RMC.

2. Configure Superdome Flex 280 Server through SSH or a web browser:

   ```
   ssh RMC<RMC MAC Address>.local
   ```

   or

   ```
   https://RMC<RMC MAC Address>.local
   ```

3. Remove the route that was created in step 1:

   ```
   sudo ip route delete 169.254.0.0/16 dev <ethXX>
   ```

Using the Linux system connected to the Superdome Flex 280 Server

About this task

If the laptop is directly connected to the Superdome Flex 280 Server RMC port:

Procedure

1. Change the settings for the Linux LAN interface to `Link-Local Only`.
2. Connect to the RMC through SSH or web browser using `RMC<RMC MAC Address>.local address`.

Gathering installation materials and information

About this task

The following procedure explains how to gather the information you need for the operating system installation session. If you gather the information you need in advance, you can complete the installation more quickly.

Procedure

1. Obtain the operating system software from the operating system vendor and write this software to a DVD or an appropriately formatted USB storage device.
2. Verify your site credentials, site registration status, and other customer data with your operating system vendor.
3. Obtain the HPE Foundation Software.

   Hewlett Packard Enterprise recommends that you read the HFS release notes before you install HFS. The HFS release notes and the software download are at **www.hpe.com/support/superdomeflex280-software**.

   Write the ISO file to a DVD, to a USB storage device, or to a location on your local network.
4. Gather the information that the operating system installer requires.

   The installation requires you to provide information about passwords, your public (or in-house) network, and so on. If you gather the following information from your site network admin before you begin, you can complete the installation more quickly. Be sure to store this data securely and destroy insecure copies.

   - Server fully qualified domain name (FQDN) _____
   - Server hostname _____
   - Server IP address _____
   - Server subnet mask _____
   - Server administrator user password _____
   - Site DNS server IP addresses _____
   - Site search domain _____
   - FQDN of your site network time protocol (NTP) server _____
   - Primary name server IP address _____
   - Secondary name server IP address _____
   - Rack management controller (RMC) fully qualified domain name (FQDN) _____
   - RMC administrator user password _____
5. Connect to the server to enable installing the OS.

Installing Red Hat Enterprise Linux

About this task

This procedure explains how to install and configure the following software.

- The RHEL operating system.
- The HPE Foundation Software (HFS).
  See for versions that support your Linux OS.

Procedure

Installing the OS and HPE Foundation Software

1. Initiating RHEL installation and partitioning the disk
2. Configuring RHEL network and rebooting
3. Completing RHEL installation
4. Installing HPE Foundation Software on RHEL

Subtopics

Initiating RHEL installation and partitioning the disk

Prerequisites

Gather installation materials and information you need for the operating system installation.

> **NOTE:**
>
> HPE Persistent Memory requires supported OS kernels. For more information on supported OS versions, see **HPE Persistent Memory Guide for HPE Superdome Flex Server**.

Procedure

1. On the boot loader menu, complete the following steps:
   a. Use the arrow keys to select Install Red Hat Enterprise Linux *x.x*.
   b. Press **E** (for edit).

      Edit the installer kernel boot line to remove `quiet` and add `erst_disable edac_report=off console=ttyS0,115200 earlyprintk=ttyS0,115200 bau=0 mce=2 nmi_watchdog=0 pci=nobar`

      > **NOTE:**
      >
      > Systems with HPE Persistent Memory might require the following bootline option to boot the distribution installer:
      >
      > `modprobe.blacklist=nfit,dax_pmem,device_dax,libnvdimm,nd_pmem`

   c. Press **Ctrl-X** to start the boot.
2. Wait a few moments while the software loads.
3. On the WELCOME … screen, which asks What language would you like to use during the installation process? , complete the following steps:

a. Select your language.

b. Click Continue.

4. On the INSTALLATION SUMMARY page, click DATE & TIME.
5. On the DATE & TIME page, complete the following steps:
   a. Select your time zone.
   b. Select the date.
   c. Click Done.
6. On the INSTALLATION SUMMARY page, click KEYBOARD.
7. On the KEYBOARD LAYOUT page, complete the following steps:
   a. Select your keyboard layout.
   b. Click Done.
8. On the INSTALLATION SUMMARY page, click SOFTWARE SELECTION.
9. On the SOFTWARE SELECTION page, complete the following steps:
   a. Select Server with GUI.
   b. Click Done.
10. On the INSTALLATION SUMMARY page, complete the following steps:
    a. Click INSTALLATION DESTINATION.
    b. Under Local Standard Disks, click the disk onto which you want to install the operating system.
    c. Under Other Storage Options, click I will configure partitioning.
    d. Click Done.
11. On the MANUAL PARTITIONING page, clean the disk.

    The screen left pane lists the operating system installations that currently reside on the disk. Your goal is to remove all operating system installations, data, and partitions that reside on the disk. You can remove one operating system at a time.

    To remove one operating system, complete the following steps:

    a. Select the operating system name.
    b. Click the minus sign (-) at the bottom of the left pane to delete the operating system.
    c. On the Are you sure … popup, complete the following steps:
       i. Select Delete all other … .
       ii. Click Delete it.
    d. Repeat the preceding steps, as needed, until all operating systems are removed.
12. In the left pane, from the New mount points will use the following partition scheme drop-down list, select Standard Partition.
13. Create mount points.

    Configure the disks according to the following table.

Size	Mount point	Filesystem
512 MB	`/boot/efi`	FAT16
250 GB (256,000 MB)	`/`	XFS
8 GB (8,192 MB)	`swap`	swap
rest of disk	`/data1`	XFS

To create mount points, complete the following steps:

a. In the left pane, click the plus sign (+) to add a mount point.

b. On the ADD A NEW MOUNT POINT popup, complete the following steps:

   i. On the Mount Point drop-down menu, select /boot/efi.

   ii. On the Desired Capacity field, enter `512mb`.

   iii. Click Add mount point.

c. In the left pane, click the plus sign (+) to add a mount point.

d. On the ADD A NEW MOUNT POINT popup, complete the following steps:

   i. On the Mount Point drop-down menu, select /.

   ii. On the Desired Capacity field, enter `250gb`.

   iii. Click Add mount point.

e. In the left pane, click the plus sign (+) to add a mount point.

f. On the ADD A NEW MOUNT POINT popup, complete the following steps:

   i. On the Mount Point drop-down menu, select swap.

   ii. On the Desired Capacity field, enter `8gb`.

   iii. Click Add mount point.

g. In the left pane, click the plus sign (+) to add a mount point.

h. On the ADD A NEW MOUNT POINT popup, complete the following steps:

   i. In the Mount Point field, enter `/data1`.

   ii. Leave the Desired Capacity field blank.

   iii. Click Add mount point.

i. Verify that the Desired Capacity field shows the rest of the disk.

j. Click Done.

14. On the SUMMARY OF CHANGES popup, click Accept Changes.
15. On the INSTALLATION SUMMARY page, click KDUMP.
16. On the KDUMP page, complete the following steps:

    a. Next to Kdump Memory Reservation, click Manual.

    b. In the Memory to be Reserved (MB) field, specify `450` MB.

    c. Click Done.

More information

- Installing Red Hat Enterprise Linux
- Configuring RHEL network and rebooting

Configuring RHEL network and rebooting

Procedure

1. On the INSTALLATION SUMMARY page, click NETWORK & HOST NAME.
2. On the NETWORK & HOST NAME page, complete the following steps:

a. Select the Ethernet device that you want to configure.

b. In the right pane, in the upper-right corner of the screen, find the ON/OFF switch, and click the blank box to set the ON/OFF switch to ON.

c. Click Configure.

d. On the Editing *device_name* popup, select IPv4 Settings.

e. Complete this step according to the following table:

To specify dynamic addressing:	To specify static addressing:
1. In the Method: drop-down menu, select Automatic (DHCP).	1. In the Method: drop-down menu, select Manual.
2. On the Editing pop-up, click Save.	2. In the Addresses pane, click Add, and complete the following steps: • Enter the IP address. • Enter the netmask. • Enter the IP address of the default gateway.
	3. In the DNS servers: field, enter the IP address of one or more DNS servers. If you specify more than one, use a comma to separate each IP address.
	4. In the Search domains: field, enter one or more search domains. If you specify more than one, use a comma to separate each domain.
	5. On the Editing pop-up, click Save.

f. In the Host name field, enter the hostname of the system.

g. Click Done.

3. On the INSTALLATION SUMMARY page, click Begin Installation.

4. On the CONFIGURATION page, click ROOT PASSWORD.

5. On the ROOT PASSWORD page, complete the following steps:

a. In the Root Password field, enter the password you want to use on this system.

b. In the Confirm field, enter the password again.

c. Click Done.

If the password is too weak, either specify a stronger password or click Done twice.

6. (Optional) On the CONFIGURATION page, click USER CREATION and follow the prompts.

Complete this optional step if you want to configure additional user accounts.

7. On the CONFIGURATION page, complete the following steps:

a. Wait for the installation to complete.

b. Click Reboot when the installation completes.

c. Wait for the reboot to finish.

The OS auto boots after being rebooted. Wait for the GRUB menu and complete the following step.

d. When the GRUB menu appears, press `e` to edit the top command line.

- (RHEL 7.9 and newer, and Oracle Linux) The top line is highlighted to select the RHEL version. Do **NOT** select the rescue mode version.

8. To reset the boot parameters, complete the following steps:

- (RHEL 7.9 and newer, and Oracle Linux) Complete these steps:

  a. On the boot loader menu, use the arrow keys to select Install Red Hat Enterprise Linux *x.x.*

  b. Press **E** (for edit).

     Edit the installer kernel boot line to remove `quiet` and add `erst_disable edac_report=off console=ttyS0,115200 earlyprintk=ttyS0,115200 bau=0 mce=2 nmi_watchdog=0 pci=nobar`

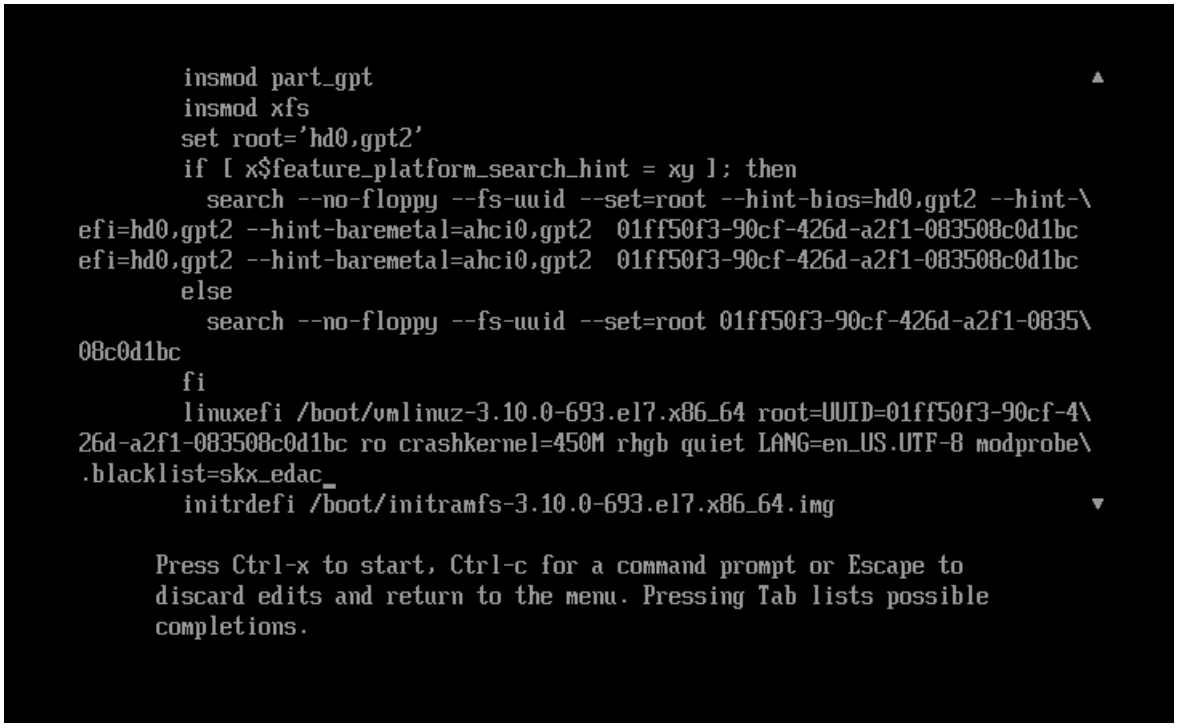
  c. To start the boot, press Ctrl-X.

- (RHEL 7.9 and newer, and Oracle Linux) Complete these steps:

  a. Enter the following string at the end of the `linuxefi` kernel command line:

     ```
     modprobe.blacklist=skx_edac
     ```

     Use a backslash (`\`) character if needed, to continue the line appropriately. The following figure shows the newly edited file and the use of the backslash.

  b. Press CTRL-X to start the boot.

More information

- Installing Red Hat Enterprise Linux
- Completing RHEL installation

Completing RHEL installation

About this task

NOTE:

If a read/write console connection from the RMC is active, Steps 1-5 may appear on the active console connection rather than on the local attached keyboard, monitor, and mouse.

Procedure

1. On the INITIAL SETUP page, click LICENSE INFORMATION.

2. On the LICENSE INFORMATION page, complete the following steps:
   a. Click I accept the license agreement .
   b. Click Done.
3. Perform one of the following:
   - (RHEL 7.9 and newer, and Oracle Linux) On the INITIAL SETUP page, click Subscription Manager.
4. On the Subscription Manager (RHEL 7.9 and newer, and Oracle Linux) page, complete the following steps:
   a. Complete the fields according to your site practices.
   b. Click Done.
5. Click FINISH CONFIGURATION.
6. On the Welcome page, complete the following steps:
   a. Select your language.
   b. Click Next.
7. On the Typing page, complete the following steps:
   a. Select the language you use.
   b. Click Next.
8. Select one of the following:
   - (RHEL 7.9 and newer, and Oracle Linux) On the Privacy page, complete the following steps:
     a. In the right pane, in the upper-right corner of the screen, find the ON/OFF switch. Click the blank box to set Location Services to OFF.
     b. Click Next.
9. On the Time Zone page, complete the following steps:
   a. Type your location, click the magnifying glass search icon, and press Enter.
   b. Click Next.
10. On the Connect Your Online Accounts (RHEL 7.9 and newer, and Oracle Linux) page, click Skip.
11. On the About You page, complete the following steps to create the local user account:
    a. Complete all the fields on this page.
    b. Click Next.
12. On the Set a Password page, complete all fields and click Next.
13. On the You're ready to go page, click Start using Red Hat Enterprise Linux Server .

More information

- Installing Red Hat Enterprise Linux
- Installing HPE Foundation Software on RHEL

Installing HPE Foundation Software on RHEL

About this task

To install the HPE Foundation Software on RHEL platforms, complete the following procedure. Some steps contain platform-specific notes.

NOTE:

The installation of HPE Foundation Software requires additional RHEL packages that were not installed during the initial installation of "Server with GUI" packages. Configure an OS installation repository prior to configuring an HFS repository.

Procedure

1. Insert the HPE Foundation Software X.X media into the DVD drive or navigate to the HFS location on the network.
2. Open a terminal window to the server.

   For example, click Applications > System Tools > Terminal.
3. Make sure that you are logged in as the root user.
4. To create an installation directory for the files from the media, enter the following command:

   ```
   #
   mkdir -p /opt/hpe/Factory-Install/hpe-foundation-X.X/
   ```
5. To mount the media in read-only mode (`-r`), using a loop device, enter one of the following commands:
   - (Oracle Linux platforms) Enter the following command:

     ```
     #
     mount -t iso9660 /dev/cdrom /mnt
     ```
   - (RHEL platforms) Enter the following command:

     ```
     #
     mount -t iso9660 -ro loop /dev/cdrom /mnt
     ```
6. To copy the files from the temporary mount directory to the installation directory, enter the following command:

   ```
   #
   rsync -avHx /mnt/ /opt/hpe/Factory-Install/hpe-foundation-X.X/
   ```
7. To unmount the media from the temporary directory, enter the following command:

   ```
   #
   umount /mnt
   ```
8. Use a text editor to create file `/etc/yum.repos.d/foundation X.X-local.repo` with the following contents:

   ```
   [foundationX.X-repo]
   name=HPE Foundation Software X.X - $basearch
   baseurl=file:///opt/hpe/Factory-Install/hpe-foundation-X.X/RPMS
   enabled=1
   gpgcheck=0
   gpgkey=file:///opt/hpe/Factory-Install/hpe-foundation-X.X/RPM-GPG-KEY-hpe
          file:///opt/hpe/Factory-Install/hpe-foundation-X.X/RPM-GPG-KEY-sgi
   ```
9. To display the list of software that you can install and verify that the list includes the foundation software, enter the following command.

   ```
   #
   yum grouplist | grep HPE
   ```
10. To install the HPE Foundation Software group, enter one of the following commands:
    - (Oracle Linux platforms) Enter the following command:

      ```
      #
      yum groupinstall "HPE Foundation Software for Oracle Linux"
      ```
    - (RHEL platforms) Enter the following command:

      ```
      #
      yum groupinstall "HPE Foundation Software"
      ```

11. To confirm the download size, enter
    ```
    y
    ```
    at the following prompt:
    ```
    Is this ok [y/N]
    ```
12. To accept the package signing, enter
    ```
    y
    ```
    at the following prompt:
    ```
    Is this ok [y/N]
    ```
    The system might prompt you accept one or more `RPM-GPG-KEY-hpe` or `RPM-GPG-KEY-sgi` package signing key. Accept all the keys.
13. Open a terminal window on the booted server.
14. To reboot the server, enter the following command in the terminal window:
    ```
    #
    reboot
    ```

Installing SUSE Linux Enterprise Server

About this task

This procedure explains how to install and configure the following software:

- The SLES operating system.
- The HPE Foundation Software.

  See for versions that support your Linux OS.

Procedure

Installing the OS and HPE Foundation Software

1. Initiating SLES installation
2. Using SLES to partition the disk
3. Configuring SLES network and miscellaneous settings
4. Installing HPE Foundation Software on SLES platforms using YaST

Subtopics

Initiating SLES installation

Prerequisites

- Gather installation materials and information you need for the operating system installation.
- SLES 15 OS installation requires two DVD or ISO images. Use the installation procedure in to install SLES 15.

Procedure

1. On the SUSE Linux Enterprise Server *x* screen, which is the boot loader screen, select Installation.
   a. On the grub menu, select Advanced options for SLES *x*.

      Press E (for edit).
   b. Edit the boot line, adding: `edac_report=off console=ttyS0,115200 earlyprintk=ttyS0,115200 bau=0 mce=2 nmi_watchdog=0 pci=nobar`

      NOTE:

      Systems with HPE Persistent Memory might require the following bootline option to boot the distribution installer:

      `modprobe.blacklist=nfit,dax_pmem,device_dax,libnvdimm,nd_pmem`
   c. Press Ctrl-X to start the boot.
2. Wait a few moments while the software loads.
3. On the Language, Keyboard and License Agreement page, complete the following steps:
   a. Use the pull-down menu to select your language.
   b. Use the pull-down menu to select your keyboard layout.
   c. Check I Agree to the License Terms .
   d. Click Next.
4. On the System Probing ... screen, monitor the progress.
5. On the Registration screen, complete the following steps:
   a. Provide your site credentials.
   b. Click Next.
6. On the Add On Product screen, click Next.
7. On the System Role screen, select Default System, and click Next.
8. On the Suggested Partitioning screen, click Expert Partitioner.

More information

- Using SLES to partition the disk
- Installing SUSE Linux Enterprise Server

Using SLES to partition the disk

About this task

This topic explains how to partition the disk and how to monitor a reboot.

Configure the disks according to the following table.

Table 1. Disk partitions

Size	Mount Point	Filesystem
512 MB	`/boot/efi`	FAT16
250 GB (256,000 MB)	`/`	XFS
8 GB (8,192 MB)	`swap`	Swap
rest of disk	`/data1`	XFS

Procedure

1. On the Expert Partitioner screen, complete the following steps to clean the disk:
   a. Expand Hard Disks.
   b. Select the disk you want to use.

      For example, select sda.
   c. On the Expert ... drop-down in the lower right part of the screen, select Create New Partition Table.
   d. On the YaST2 pop-up with the message Really create a new partition table ... , click Yes.
   e. Expand Hard Disks.
   f. Select the hard disks you want to use.
   g. Click Add.
2. Complete the following steps on the Add Partition on /dev/*disk* screen to configure the boot partition:
   a. Under New Partition Size, click Custom Size.
   b. Enter `512 MB` in the Size field.
   c. Click Next.
   d. Under the Role list, complete the following steps:
      i. Select Operating System.
      ii. Click Next.
   e. Under Formatting Options, select Format partition.
   f. Under File system, use the pull-down menu to select `FAT`.
   g. Under Mounting Options, select Mount Partition.
   h. Under Mount point, use the pull-down menu to select `/boot/efi`.
   i. Select Finish.
3. On the Expert Partitioner screen, click Add.
4. Complete the following steps on the Add Partition on /dev/*disk* screen to configure the root partition:
   a. Under New Partition Size, click Custom Size.
   b. Enter `250 GB` in the Size field.
   c. Click Next.
   d. Under the Role list, complete the following steps:
      - Select Operating System.
      - Click Next.
   e. Under Formatting Options, select Format partition.
   f. Under File system, use the pull-down menu to select `XFS`.
   g. Under Mounting Options, select Mount Partition.
   h. Under Mount point, use the pull-down menu to select `/`.
   i. Select Finish.
5. On the Expert Partitioner screen, click Add.
6. Complete the following steps on the Add Partition on /dev/*disk* screen to configure the swap partition:
   a. Under New Partition Size, click Custom Size.

b. Specify `8 GB` in the Size field.

c. Click Next.

d. Under the Role list, complete the following steps:

- Select Swap.
- Click Next.

e. Under Formatting Options, select Format partition.

f. Under File system, use the pull-down menu to select `Swap`.

g. Under Mounting Options, select Mount Partition.

h. Under Mount point, use the pull-down menu to select `swap`.

i. Select Finish.

7. On the Expert Partitioner screen, click Add.
8. Complete the following steps on the Add Partition on /dev/*disk* screen to configure the data partition:

a. Under New Partition Size, click Maximum Size.

b. Click Next.

c. Under the Role list, complete the following steps:

i. Select Data and ISV Applications.

ii. Click Next.

d. Under Formatting Options, select Format partition.

e. Under File system, use the pull-down menu to select `XFS`.

f. Under Mounting Options, select Mount Partition.

g. Under Mount point, enter `/data1`.

h. Select Finish.

9. On the Expert Partitioner screen, in the Partitions tab, examine the disk partitions.

   If the partitions match the disk partitions in Disk partitions, click Accept.

   If the partitions are incorrect, correct the partition specifications.
10. On the Suggested Partitioning screen, click Next.
11. On the Clock and Time Zone screen, complete the following steps:

a. Select your region.

b. Select your time zone.

c. Check the box next to Hardware Clock Set To UTC.

d. Click Next.

12. On the Local Users screen, click Create New User.

    Complete the following steps:

a. Complete the following fields:

- User's Full Name
- Username
- Password
- Confirm Password

b. Click Next.

13. On the Password for the System Administrator “root” screen, complete the following steps:

    a. In the Password for root User field, enter the root user password.

    b. In the Confirm password field, re-enter the root user password.

    c. Enter a few characters in the Test Keyboard Layout field.

       For example, if you specified a language that includes non-English characters and you include these characters in passwords, enter these characters into this field. This field is a plain text field. You assure yourself that the operating system can recognize these characters when you enter them.

    d. Click Next.

14. On the Installation Settings screen, configure additional features as needed and click Install.

15. On the Confirm Installation pop-up, click Install.

16. Monitor the installation and, if you are using hard media, be prepared to remove the installation software media before the boot.

    The installation itself can take several minutes. At the end of the installation, the system boots. The installation software notifies you of this boot. If you can, remove the installation DVD before the system boots.

    If you fail to remove the installation DVD before the final boot, the machine boots from the DVD. In this case, complete the following steps:

    a. Remove the DVD after the boot.

    b. Press CTRL-ALT-DEL to boot the machine again.

    c. Allow the machine to boot from the hard disk to finish the installation.

    If you are installing over the network, the JViewer software manages the disk.

More information

- Configuring SLES network and miscellaneous settings
- Installing SUSE Linux Enterprise Server

Configuring SLES network and miscellaneous settings

Procedure

1. Log into the server as the root user.
2. Click Applications > System Tools > YaST.
3. On the Administrator Settings screen, click Network Settings.
4. On the YaST2 -- Network Settings screen, highlight the network card you want to configure, and click Edit.
5. On the Network Card Setup screen, specify dynamic or static addressing, as follows:

To specify dynamic addressing:	To specify static addressing:
1. Select the type of dynamic addressing that you want.	1. Verify that eth0 appears in the Configuration Name field, and click Statically assigned IP Address.

To specify dynamic addressing:	To specify static addressing:
2. Click Next to accept the default of DHCP.	2. Configure the first NIC (`eth0`) for your house (public) network. On the Address tab, specify the following: • The IP Address • The Subnet Mask • The Hostname
	3. Click Next.

6. On the Network Settings screen, click the Hostname/DNS tab and complete the following steps:
   a. Enter the hostname.
   b. Enter the domain name.
   c. Verify that Change Hostname via DHCP is set correctly.

      To assign a static IP address, clear the check box to the left of the Change Hostname via DHCP label. A later step saves the hostname to the `/etc/hosts` file. Consult your network administrator if you have questions regarding the use of DHCP.

      NOTE: This procedure explains how to configure a static address on a network card. If you want a different network configuration, for example if you want to configure DHCP, ensure that the check box in this step is checked before you click Next. You can use this procedure as a guide and consult the SLES documentation for more specific steps.

   d. The IP address for Name Server 1.
   e. (Optional) The IP address for Name Server 2.
   f. (Optional) The IP address for Name Server 3.
   g. (Optional) In the Domain Search field, add additional domains.
   h. Click the Routing tab.
   i. On the Routing tab, enter the Default Gateway, and click OK.

More information

- Installing HPE Foundation Software on SLES platforms using YaST
- Installing SUSE Linux Enterprise Server

Installing HPE Foundation Software on SLES platforms using YaST

Procedure

1. Insert the HPE Foundation Software X.X media into the DVD drive or make a network connection to the HPE Foundation Software repository.
2. Log into the server as the root user.
3. To start the YaST interface, click Applications > System Tools > YaST.
4. Under Software, click Software Repositories to start the SLES repository manager.
5. On the Configured Software Repositories screen, click Add.
6. On the Add On Product screen, select DVD, and click Next.
7. On the YaST pop-up, complete the following steps:

a. Select the correct DVD.

b. Click Continue.

8. On the Import Untrusted GnuPG Key, follow this procedure to import a trusted key.

> **NOTE:**
>
> Perform this step if you are going through this process for the first time and you must confirm the security of the Hewlett Packard Enterprise digital key.

a. Download the keys.

Copy the compressed tar file (`HPE-GPG-Public-Keys.tar.gz`) from this link to your local directory and extract the public keys.

https://downloads.hpe.com/pub/keys/HPE-GPG-Publick-Keys.tar.gz

b. Import the keys for GPG.

For each key that you have unzipped, install the public key using the `gpg --import` command.

```
#
gpg --import /path_to_the_key/file_name_of_the_key
```

For example:

```
gpg --import /path_to_the_key/B1275EA3.pub
```

c. Verify using GPG.

Use the `gpg --verify` command to validate and verify the digital signature of the signed file. The output from the command indicates the validity of the signature. Specify the `.sig` (detached signature) file and the corresponding input file in the command.

```
#
gpg --verify filename.sig filename
```

If the level of trust on the key has not been set, you will see a trust level warning similar to the following:

```
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
```

Because you have downloaded the key from an SSL secured site by Hewlett Packard Enterprise Company, you can ultimately trust that this public key is indeed from Hewlett Packard Enterprise Company. Therefore edit the key to set the trust level of the key for proper verification.

d. Find the "*key_name*" of the key.

Type the following command and select the key that you must trust:

```
#
gpg --list-keys
```

Example of a "*key_name*": `"Hewlett Packard Enterprise Company RSA 2048 1"`

e. Edit the key.

```
#
gpg --edit-key "key_name"
```

Type the command "

```
trust
```

" and select "5" for trusting the key ultimately.

f. Confirm and enter

```
quit
```

to exit.

In the future, you will not see the warning about an untrusted identity when verifying the signature. Example verification:

```
#
gpg --verify test.bin.sig test.bin

gpg: Signature made Thu 03 Jan 2013 04:48:47 PM UTC using RSA key ID
5CE2D476
gpg: Good signature from "Hewlett Packard Enterprise Company RSA 2048 1"
```

9. On the Configured Software Repositories screen, click OK.
10. On the YaST Control Center screen, click Software Management.
11. Select View > Patterns.
12. Scroll down to HPE Foundation.
13. Check the box to the left of HPE Foundation Libraries, Software, and Drivers, and click Accept.
14. On the Changed Packages pop-up, click Continue.
15. Insert the media into the DVD drive as directed by the prompts on the Perform Installation screen.

    If necessary, click Eject on the YaST2 pop-up to open the DVD drive. In the YaST pop-up, you might need to click Retry more than once to read a new media.
16. On the Installation Report screen, click Finish.
17. Close the YaST session.
18. Open a terminal window on the booted system.
19. Log into the server as the root user.
20. Configure items in `/etc/sysconfig/hpe-auto-config`.
21. In the terminal window, enter the following command to reboot the system.

```
#
reboot
```

Installing HPE Foundation Software on SLES platforms using Zypper

About this task

You can install HPE Foundation Software using Zypper:

1.
```
# zypper install -t pattern HPE-Foundation
```

Installing Microsoft Windows Server operating system

For installation instructions for Windows Server 2016 Standard and Datacenter Editions and Windows Server 2019 and 2022 Standard and Datacenter Editions, see **Deploying Microsoft Windows Server on HPE Superdome Flex 280 Server**.

Installing VMware vSphere operating system

About this task

For VMware vSphere installation instructions, see Running VMware vSphere on HPE Superdome Flex Family at **www.hpe.com/support/superdomeflex280-vmware**.

Updating HPE Foundation Software using online Software Delivery Repository

Prerequisites

- An active warranty or support contract is required to access HPE Foundation Software product updates.
- The email associated with the HPE Passport account must be supplied as the username.
- A user-generated token must be supplied as the HTTP password to access the repository.

About this task

HPE Foundation Software is available from the HPE Software Delivery Repository at **https://downloads.linux.hpe.com/SDR/project/hpe-foundation/**.

The SDR provides a way to install software packages on a Linux system by using `yum` or `zypper`.

Procedure

1. Go to the HPE Foundation Software page.

   https://downloads.linux.hpe.com/SDR/project/hpe-foundation/
2. Generate your user token following the instructions on the site.
3. Access the HPE Foundation Software repository with a web browser, `yum`, or `zypper`.

   Use the following URL syntax: `https://EMAIL:TOKEN@update1.linux.hpe.com/repo/hpe-foundation`
4. The first time accessing the SDR from a system, you may subscribe the system by following the instructions on the SDR site.
5. For specific `yum` and `zypper` command options for package installation, see the examples at **https://downloads.linux.hpe.com/SDR/project/hpe-foundation/**.

Updating HPE Foundation Software on RHEL

About this task

To update the HPE Foundation Software on RHEL platforms, complete the following procedure. Some steps contain platform-specific notes.

> **NOTE:**
> The installation of HPE Foundation Software requires additional RHEL packages that were not installed during the initial installation of "Server with GUI" packages. Configure an OS installation repository prior to configuring an HFS repository.

Procedure

1. Insert the HPE Foundation Software X.X media into the DVD drive or navigate to the HFS location on the network.
2. Open a terminal window to the server.

   For example, click Applications > System Tools > Terminal.
3. Make sure that you are logged in as the root user.
4. To create an installation directory for the files from the media, enter the following command:

   ```
   #
   mkdir -p /opt/hpe/Factory-Install/hpe-foundation-X.X/
   ```
5. To mount the media in read-only mode (`-r`), using a loop device, enter one of the following commands:

   - (Oracle Linux platforms) Enter the following command:

```
#
mount -t iso9660 /dev/cdrom /mnt
```

- (RHEL platforms) Enter the following command:

```
#
mount -t iso9660 -ro loop /dev/cdrom /mnt
```

6. To copy the files from the temporary mount directory to the installation directory, enter the following command:

```
#
rsync -avHx /mnt/ /opt/hpe/Factory-Install/hpe-foundation-X.X/
```

7. To unmount the media from the temporary directory, enter the following command:

```
#
umount /mnt
```

8. Use a text editor to create file `/etc/yum.repos.d/foundation X.X-local.repo` with the following contents:

```
[foundationX.X-repo]
name=HPE Foundation Software X.X - $basearch
baseurl=file:///opt/hpe/Factory-Install/hpe-foundation-X.X/RPMS
enabled=1
gpgcheck=0
gpgkey=file:///opt/hpe/Factory-Install/hpe-foundation-X.X/RPM-GPG-KEY-hpe
       file:///opt/hpe/Factory-Install/hpe-foundation-X.X/RPM-GPG-KEY-sgi
```

9. To display the list of software that you can install and verify that the list includes the foundation software, enter the following command.

```
#
yum grouplist | grep HPE
```

10. To install the HPE Foundation Software group, enter one of the following commands:

- (Oracle Linux platforms) Enter the following command:

```
#
yum update "HPE Foundation Software for Oracle Linux"
```

- (RHEL platforms) Enter the following command:

```
#
yum update "HPE Foundation Software"
```

11. To confirm the download size, enter

```
y
```

at the following prompt:

```
Is this ok [y/N]
```

12. To accept the license keys, enter

```
y
```

at the following prompt:

```
Is this ok [y/N]
```

The system might prompt you accept one or more `RPM-GPG-KEY-hpe` or `RPM-GPG-KEY-sgi` license key. Accept all the keys.

13. Run `hpe-auto-config` to set the bootline options and other settings.

14. To reboot the server, enter the following command in the terminal window:

```
#
reboot
```

Updating HPE Foundation Software on SLES platforms

About this task

To update the HPE Foundation Software on SLES platforms, complete the following procedure.

Procedure

1. Insert the HPE Foundation Software media into the DVD drive or make a network connection to the HPE Foundation Software repository.
2. Log into the server as the root user.
3. To start the YaST interface, click Applications > System Tools > YaST.
4. Under Software, click Software Repositories to start the SLES repository manager.
5. On the Configured Software Repositories screen, click Add.
6. On the Add On Product screen, select DVD, and click Next.
7. On the YaST pop-up, complete the following steps:
   a. Select the correct DVD.
   b. Click Continue.
8. On the Import Untrusted GnuPG Key, follow this procedure to import a trusted key.

   NOTE:

   Perform this step if you are going through this process for the first time and you must confirm the security of the Hewlett Packard Enterprise digital key.

   a. Download the keys.

      Copy the compressed tar file (`HPE-GPG-Public-Keys.tar.gz`) from this link to your local directory and extract the public keys.

      https://downloads.hpe.com/pub/keys/HPE-GPG-Publick-Keys.tar.gz

   b. Import the keys for GPG.

      For each key that you have unzipped, install the public key using the `gpg --import` command.

      ```
      #
      gpg --import /path_to_the_key/file_name_of_the_key
      ```

      For example:

      ```
      gpg --import /path_to_the_key/B1275EA3.pub
      ```

   c. Verify using GPG.

      Use the `gpg --verify` command to validate and verify the digital signature of the signed file. The output from the command indicates the validity of the signature. Specify the `.sig` (detached signature) file and the corresponding input file in the command.

      ```
      #
      gpg --verify filename.sig filename
      ```

      If the level of trust on the key has not been set, you will see a trust level warning similar to the following:

      ```
      gpg: WARNING: This key is not certified with a trusted signature!
      gpg: There is no indication that the signature belongs to the owner.
      ```

      Because you have downloaded the key from an SSL secured site by Hewlett Packard Enterprise Company, you can ultimately trust that this public key is indeed from Hewlett Packard Enterprise Company. Therefore edit the key to set the trust level of the key for proper verification.

d. Find the "*key_name*" of the key.

   Type the following command and select the key that you must trust:

   ```
   #
   gpg --list-keys
   ```

   Example of a "*key_name*": `"Hewlett Packard Enterprise Company RSA 2048 1"`

e. Edit the key.

   ```
   #
   gpg --edit-key "key_name"
   ```

   Type the command "
   ```
   trust
   ```
   " and select "5" for trusting the key ultimately.

f. Confirm and enter
   ```
   quit
   ```
   to exit.

In the future, you will not see the warning about an untrusted identity when verifying the signature. Example verification:

```
#
gpg --verify test.bin.sig test.bin

gpg: Signature made Thu 03 Jan 2013 04:48:47 PM UTC using RSA key ID
5CE2D476
gpg: Good signature from "Hewlett Packard Enterprise Company RSA 2048 1"
```

9. On the Configured Software Repositories screen, click OK.
10. On the YaST Control Center screen, click Software Management.
11. Select View > Patterns.
12. Scroll down to HPE Foundation.
13. Check the box to the left of HPE Foundation Libraries, Software, and Drivers, and click Accept.
14. On the Changed Packages pop-up, click Continue.
15. Insert the media into the DVD drive as directed by the prompts on the Perform Installation screen.

    If necessary, click Eject on the YaST2 pop-up to open the DVD drive. In the YaST pop-up, you might need to click Retry more than once to read a new media.
16. On the Installation Report screen, click Finish.
17. Close the YaST session.
18. Open a terminal window on the booted system.
19. Log into the server as the root user.
20. Configure items in /etc/sysconfig/hpe-auto-config.
21. Run `hpe-auto-config` to configure the bootline options and other settings.

    ```
    #
    hpe-auto-config
    ```

OS installation using multiple ISO files

Prerequisites

- System administrator login has been completed.
- Launching JViewer from a macOS client is not supported.

About this task

OS installation from ISO file on a PC requires using virtual media to simulate a local CD/DVD drive on the server. Some OSs require more than one DVD for a complete installation.

When using more than one DVD ISO, it is necessary to download a separate Java Application to mount the Virtual Media.

In this example, the SLES 15 OS is installed using two DVD ISO files.

Procedure

1. On the home page, navigate to nPartition > Remote Console & Media.
2. Click Download Application on the Remote Media Application section.

   `JViewer.jar` file downloads on you default download location on your PC.
3. Click the `JViewer.jar` to install the application.
4. Alternatively, on your PC, open a command window (`cmd` or `PowerShell` in Windows) and navigate to the location where the `jviewer-sa.jar` file was downloaded. Run the `jviewer-sa.jar` file using the following syntax:

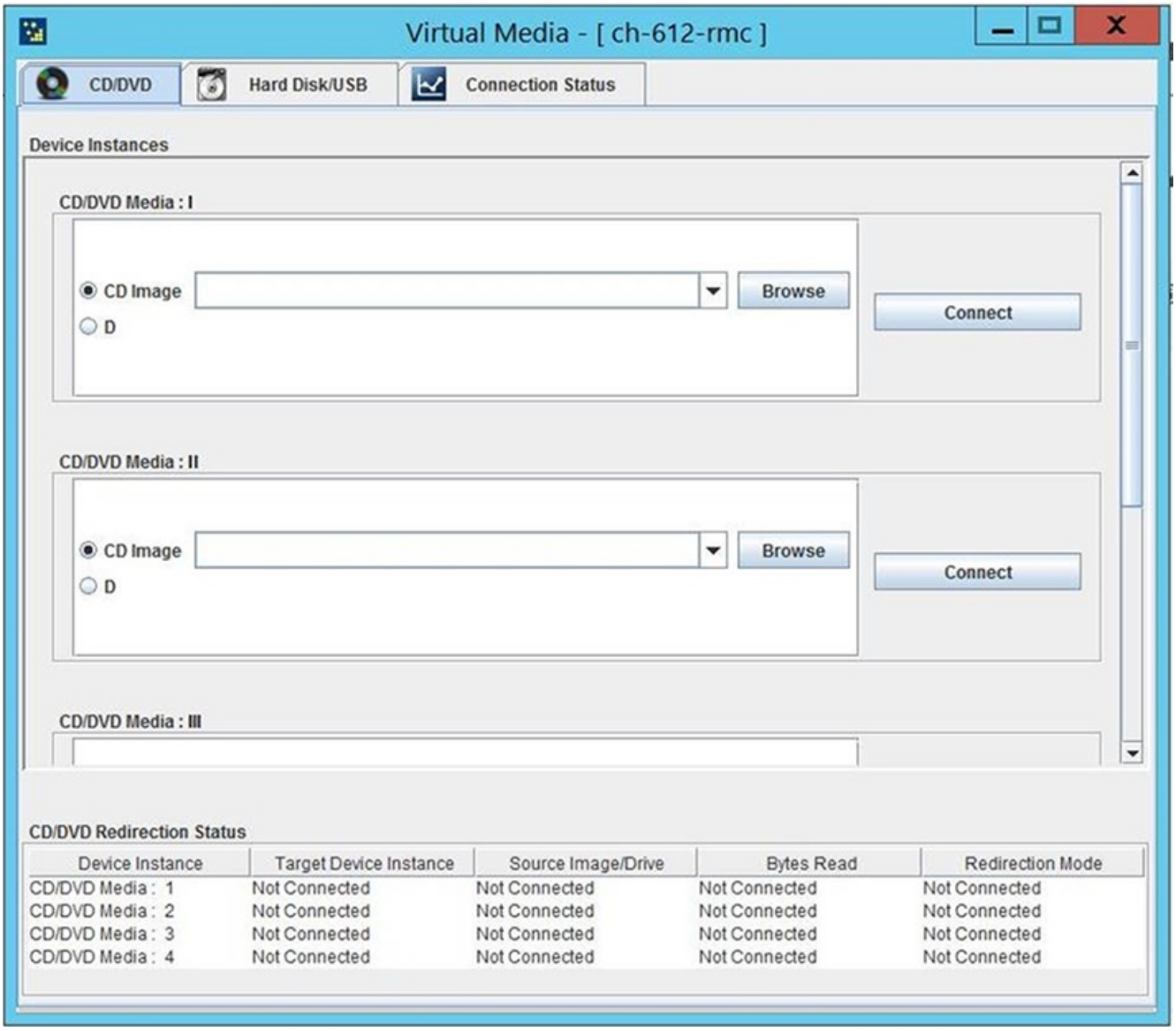
   `java -jar jviewer-sa.jar [-hostname <bmc_hostname>] [-u <username>] [-p <password>]`

   where *bmc_hostname* is the name of the monarch BMC in the partition.

   NOTE:

   `java` must be in your `PATH`, otherwise specify the full path to your installed `java.exe` file.
5. Fill in the form with your system details and credentials and click Launch.

6. Browse to each of the DVD ISO files that are required for the OS installation and click Connect.



Once connected, JViewer will show information about each media device.

7. Return to the RMC CLI and enter the following command to power On the system:

```
RMC cli> power on npar pnum=1
```

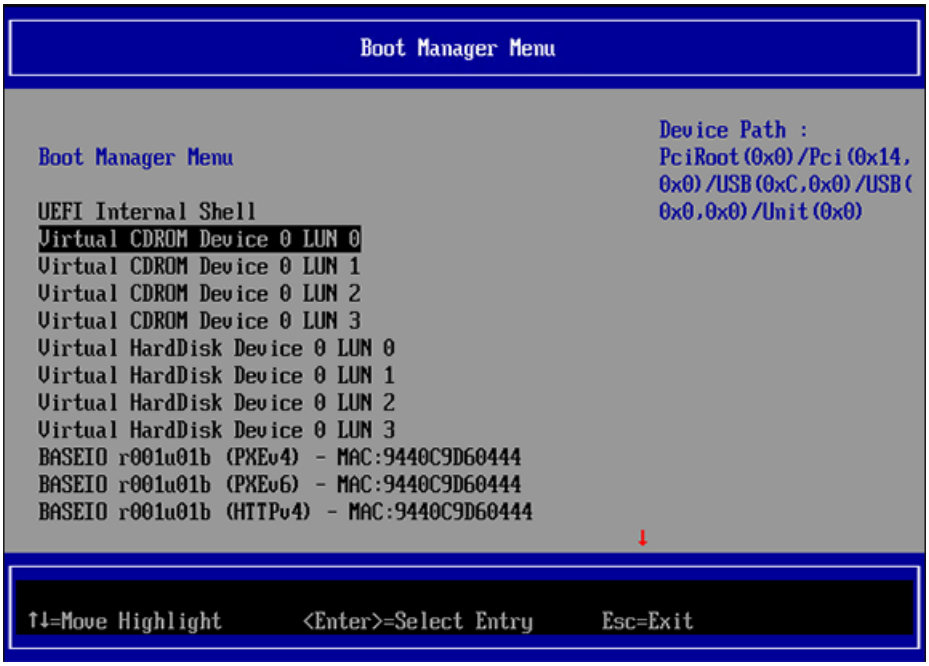
As the system powers up, the console will display the progress. You can view the console with the RMC text interface or the KVM interface. To view the system from the RMC text interface use:

```
RMC cli> connect npar pnum=p1
```

8. When the system has booted to the UEFI Shell, exit to the Boot Options screen with the `exit` command and press Enter.

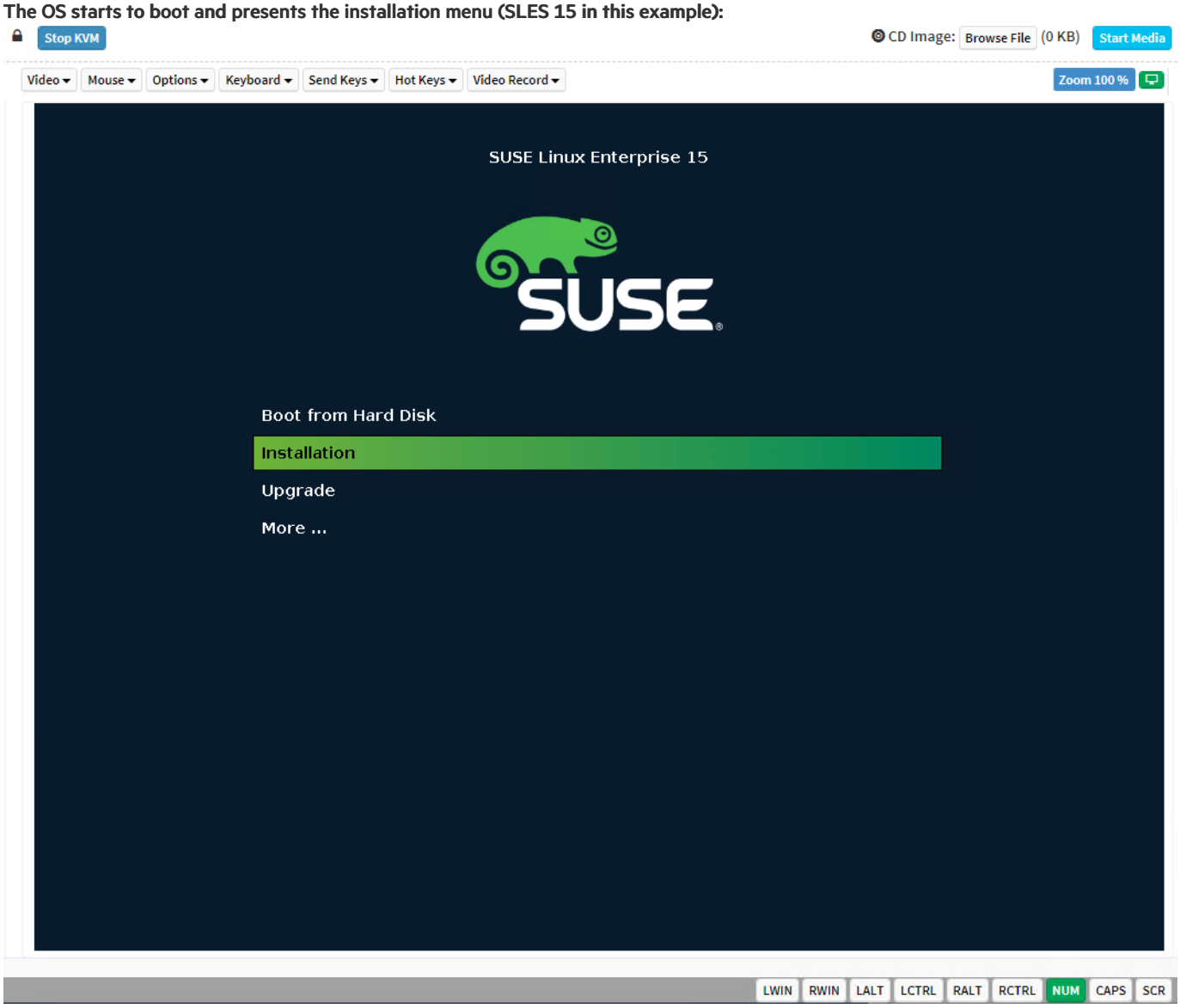
```
Shell> exit
```

9. On the Boot Options screen, use the arrow keys to select Boot Manager Menu and press Enter.
10. On the Boot Manager Menu screen, use the arrow keys to scroll through the list of devices and select `Virtual CDROM Device 0 LUN 0`. Press Enter to start booting from that device.

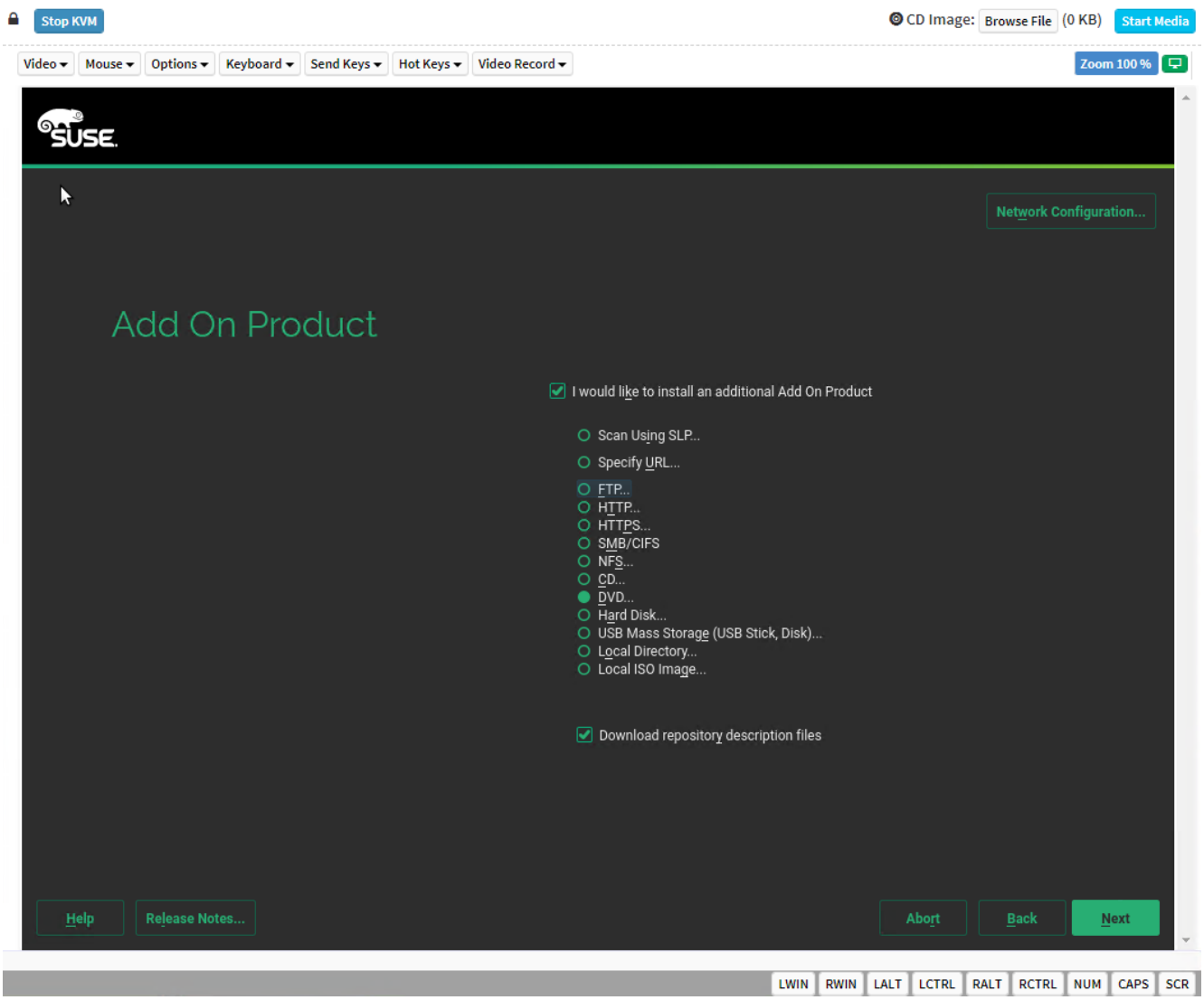


This virtual device named "Virtual CDROM Device 0 LUN 0", is the first "CD/DVD Image" that was mounted earlier. Notice that a second instance called "Virtual CDROM Device 0 LUN 1" is also displayed. This corresponds to the second DVD ISO file that was mounted earlier.

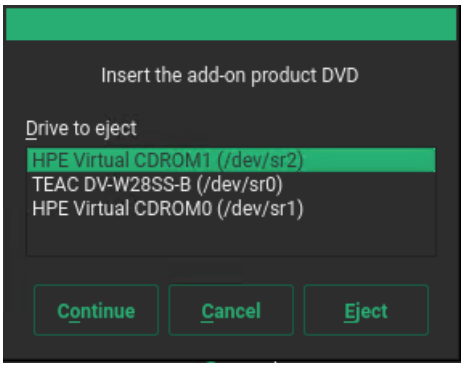
The OS starts to boot and presents the installation menu (SLES 15 in this example):



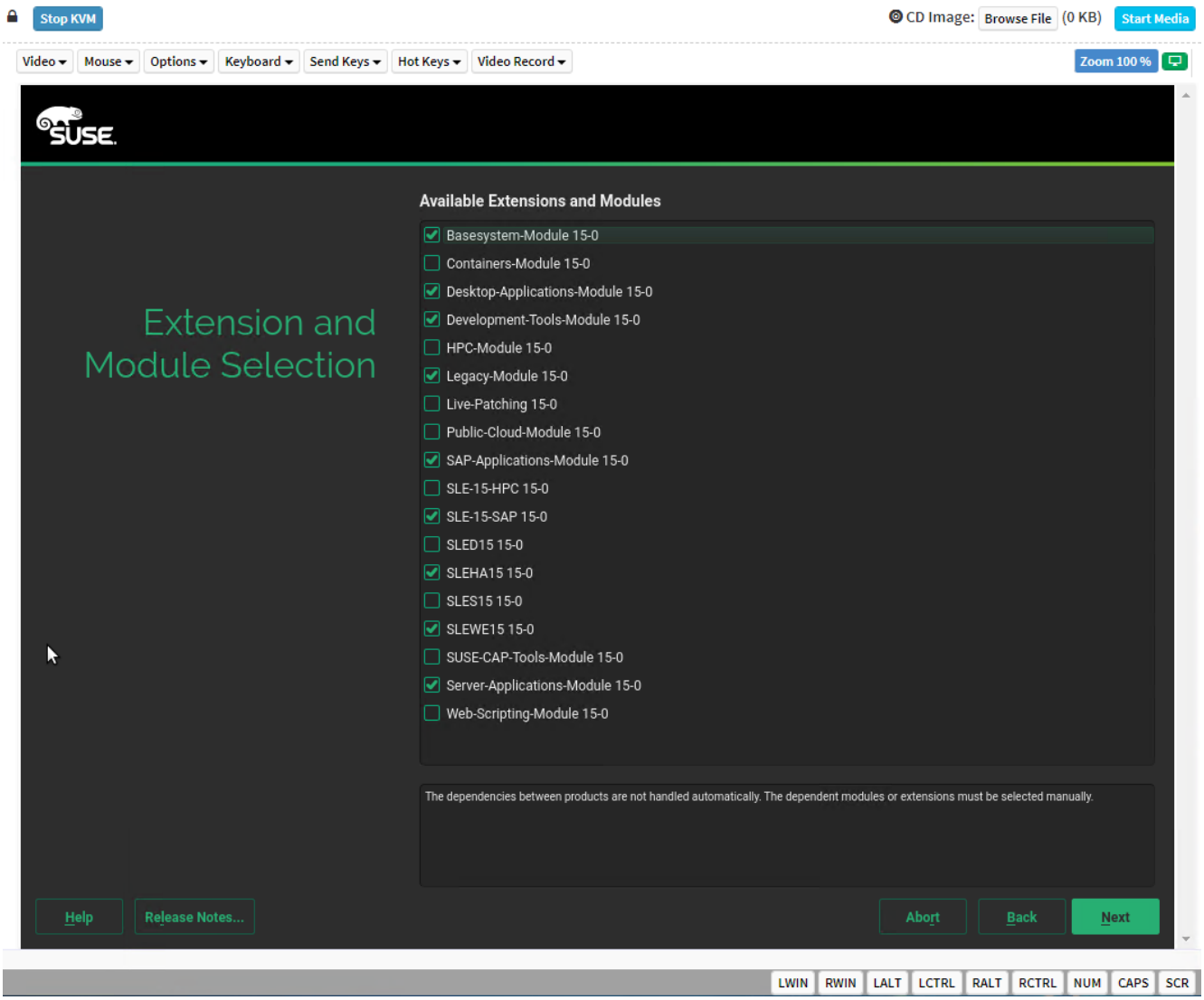
11. Follow the installation process until you reach the Add on Product screen. This will install content from the second Virtual CD/DVD. Select the following options:



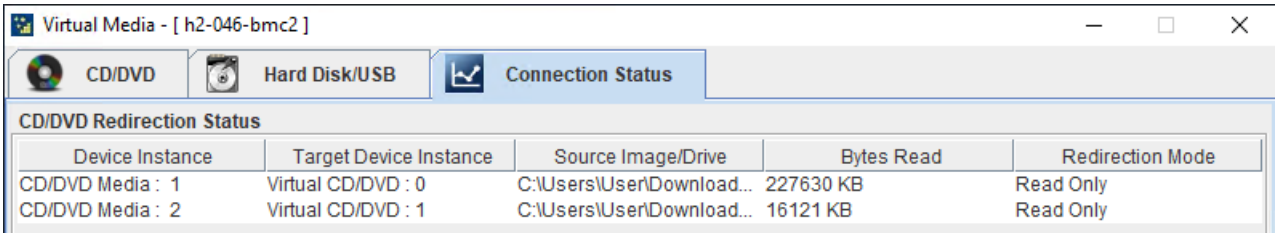
12. Select the HPE Virtual CDROM1 to install content from the second DVD ISO.



13. Select from the list of available extensions:



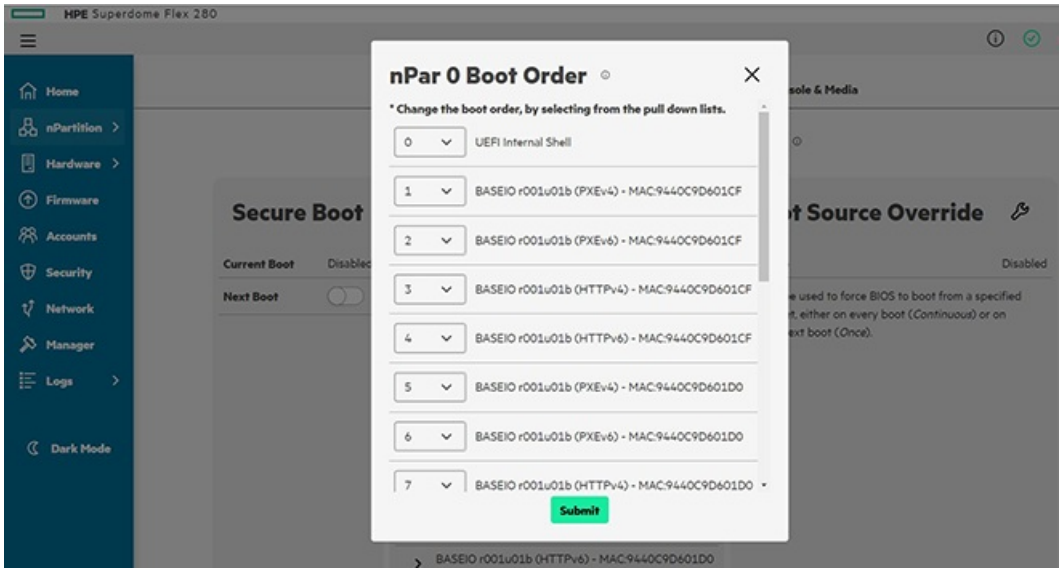
14. Continue with the OS installation. You can monitor the Virtual Media with the "Connection Status" tab.



Setting up boot order with the RMC web GUI

Procedure

1. Log in to the RMC web GUI.
2. Click nPartition on the main screen or the menu bar on the left.
3. Click the Boot Options tab.
4. To verify the system boot order, check the Boot Order heading.
5. Change the boot order.
   a. Click the  icon under the Boot Order heading.



b. Choose the boot option you want to change and click the pull-down list.

c. Select the position for the boot option from the list.

d. To confirm the changes, click Submit.

6. Reverify the system boot order. The system uses the listed boot order during the next system boot.

Specifying boot options using the RMC CLI

About this task

The Superdome Flex 280 Server can be booted from multiple sources using RMC commands. The boot options can be specified during power on, power reset, or during reboot.

Procedure

1. Log in to the RMC CLI.
2. Verify the boot option required.

   The following boot options are available:

   - *None* - No boot option specified. Boots from default source.
   - *BiosSetup* - Boot to BIOS setup.
   - *Cd* - Boot from existing UEFI boot option entries that correspond to CD/DVD drives of any connection type (such as SATA and USB).
   - *Hdd* - Boot from existing UEFI boot option entries that correspond to local hard disk drives, excluding USB drives.
   - *Pxe* - Boot from existing UEFI boot option entries that correspond to PXE.
   - *RemoteDrive* - Boot from existing UEFI boot option entries that correspond to remote (FibreChannel or iSCSI) hard disk drives.
   - *SDCard* - Boot from existing UEFI boot option entries that correspond to SD cards.
   - *UefiShell* - Boot to UEFI Shell.
   - *UefiHttp* - Boot from existing UEFI boot option entries that correspond to HTTP boot.
   - *Usb* - Boot from existing UEFI boot option entries that correspond to USB disk drives.

3. Verify if you are powering on the server, resetting the power, or rebooting the server.

   - If you are powering on the server, enter the `power on` command.

     ```
     power on npar pnum=0 [bootopt=BOOTOPT]
     ```

- If you are resetting the power or rebooting, enter the `power reset` or `reboot` command.

  ```
  power reset npar pnum=0 [bootopt=BOOTOPT] [force]
  ```

  ```
  reboot npar pnum=0 [bootopt=BOOTOPT] [force]
  ```

  - If power is on, the `power reset` or `reboot` commands perform a graceful OS shutdown then restart the server.
  - If `force` is specified, the commands perform an OS immediate (non-graceful) shutdown instead.

Setting up boot order with UEFI

Procedure

1. Interrupt the boot process and access UEFI.

   Press F2 to access the UEFI Boot Manager.
2. Select the Boot Maintenance Manager menu.
3. Select the Change Boot Order menu.
4. To select the boot options, press Enter.
5. Change the boot order.
   a. Use the up and down arrow keys to select a boot option.
   b. To move the boot option up, press +. To move the boot option down, press -.
   c. To finish setting the boot order, press Esc.
   d. To commit the changes and exit, press the down arrow and select Commit Changes and Exit. The changes take effect immediately and are applied on the next system boot.

Secure boot

HPE Superdome Flex 280 Server systems support features that secure the boot process. When enabled, Secure Boot prevents execution of OS loaders, drivers, and UEFI applications that are not signed with an acceptable digital signature.

Secure boot features

When secure boot is enabled on Superdome Flex 280 Server, system firmware verifies OS loader, driver, and UEFI application signatures before executing them.

By default, secure boot is disabled. This default applies to systems shipped from the factory.

Many secure boot configuration changes require resetting the system before booting an OS or accessing the UEFI Shell.

Secure boot protection applies both at the Boot Manager menu and at the UEFI Shell. In secure boot mode, the UEFI Shell disables the `mm`, `hexedit`, and `setvar` commands, and restricts the `dmpstore` command.

System logs record changes to the secure boot mode. Secure boot checks performed during firmware verification also are logged.

> **NOTE:**
> Secure boot keys are restored to defaults when 'set npar default all' or equivalent operations are executed. This means that any customizations to the Secure Boot settings such as update DBX settings are lost and must be reapplied.

Subtopics

Default secure boot keys

The default keys include signatures for supported operating systems.

The Superdome Flex 280 Server default secure keys permit execution of images signed by the following certificates.

- HPE KEK 2016
- Microsoft Corporation KEK CA 2011
- SUSE Linux Enterprise Secure Boot CA
- HPE DB 2016
- HP DB 2013
- Microsoft Corporation UEFI CA 2011
- Microsoft Windows Production PCA 2011
- SUSE Linux Enterprise Secure Boot Signkey
- VMware certificate 2017

Configuring Secure Boot on HPE Superdome Flex 280 Server

About this task

Secure Boot can be configured on Superdome Flex 280 Server through the RMC web GUI, the RMC CLI, or through UEFI.

Procedure

- Configure Secure Boot with the RMC web GUI
- Configure Secure Boot with the RMC CLI
- Configure Secure Boot with UEFI Boot Manager

Subtopics

Configuring Secure Boot with the RMC web GUI

Procedure

1. Log in to the RMC web GUI.
2. Click nPartition from the main screen or the menu bar on the left.
3. Click the Boot Options tab.
4. To verify the status of Secure Boot, check the Next Boot entry under the Secure Boot heading.
5. Under the Secure Boot heading, toggle the Next Boot control to either enable or disable Secure Boot on the next system boot.
6. To apply the changes, reboot the system.

Configuring Secure Boot with the RMC CLI

Prerequisites

- System must be powered off.

About this task

Secure Boot can be enabled and disabled with RMC CLI commands.

Procedure

To enable Secure Boot:

1. Log in to the RMC CLI.
2. Verify if the system is powered off. If not, enter the `power off npar` command.
3. Enter the `modify npar` command.
   - To enable Secure boot, enter the following command.

     ```
     modify npar secure_boot=on
     ```

   - To disable Secure boot, enter the following command.

     ```
     modify npar secure_boot=off
     ```

4. Verify the Secure Boot state using the `show` command.

   ```
   show npar verbose
   ```

5. Power on the system.

   ```
   power on npar
   ```

Configuring Secure Boot with UEFI Boot Manager

Procedure

1. Access UEFI Boot Manager from the nPartition console.
2. Access the Secure Boot Configuration menu.

   At Boot Manager, select the Device Manager menu, then select the Secure Boot Configuration menu.
3. Enable or disable secure boot.

   To enable secure boot:

   You can either enable with default keys, or install a custom set of keys.

   a. Enable Secure Boot with the default keys.

      Select the Attempt Secure Boot option.

   b. Install custom keys.

      Enable the Custom Secure Boot Options menu by changing the Secure Boot Mode setting to Custom Mode. After installing custom keys, verify that the Attempt Secure Boot option is selected to enable secure boot.

   To disable secure boot, clear the Attempt Secure Boot option.
4. To apply the changes, reset the system.

   The system must be reset before you can load an OS or access the UEFI Shell. If you select "Continue" at the Boot Manager or attempt to use the Boot Manager to boot any option, a pop-up window will display:

```
Configuration changed. Reset to apply it now. Press ENTER to reset.
```

Press Enter to reset the system.

More information

- Default secure boot keys

Installing or reinstalling default Secure Boot keys

Prerequisites

The system automatically installs default keys if all Secure Boot keys have been deleted.

About this task

When installing default keys, all secure boot data is written with a default set for supported operating systems.

Procedure

1. Access UEFI Boot Manager from the nPartition console.
2. Access the Secure Boot Configuration menu.

   At Boot Manager select the Device Manager menu, then select the Secure Boot Configuration menu.
3. Select the Custom Secure Boot Options menu.

   Change the Secure Boot Mode option to Custom Mode, then select the Custom Secure Boot Options menu.
4. Delete all KEK keys.

   Select the KEK Options menu, then select the Delete KEK menu. For each key displayed, toggle the corresponding checkbox to delete the key.
5. Delete all DB keys.

   Select the DB Options menu, then select the Delete Signature menu. For each key displayed, toggle the corresponding checkbox to delete the key.
6. Delete all DBX keys.

   Select the DBX Options menu, then select the Delete Signature menu. Select the Delete All Signature List option and press Y to confirm.
7. Delete the PK key.

   Select the PK Options menu, then select the Delete Pk checkbox. Press Y to confirm.
8. Reset the system to apply the changes.

   You must reset the system before you can load an OS or access the UEFI Shell.

More information

- Default secure boot keys

Setting up remote media files with the RMC web GUI

Prerequisites

- A file server configured on the local network using CIFS or NFS.
- Network address details for the file server.
- Credentials to access the file server.

About this task

HPE Superdome Flex 280 Server can access up to two ISO or image files on a remote file server.

Procedure

1. Log in to the RMC web GUI.
2. Click nPartition from the main screen or the menu bar on the left.
3. Click the Remote Console & Media tab.
4. Enable Remote Media by clicking Remote Media.
5. Under the File Server heading, click the configure icon ().

   This enables you to configure the file server options, IP address, media path, and login credentials.
6. Connect to the file server by clicking Connect.
7. Select the image files.

   Two image files can be selected and inserted.

   To remove an image file, click Eject.

   a. Click the Select Media Files drop-down list under the Media Files heading.

   b. Select an image file in the specified file path.

   c. Click Insert. The selected image file is inserted.

Provisioning an OS with OpenStack Ironic

About this task

Following is the procedure to provision an OS using OpenStack Ironic:

Procedure

1. Install OpenStack Ironic.
2. Configure OpenStack Ironic.
3. Create cloud format images and upload to Glance.

   a. Build an OS partition image in cloud format.

   b. Upload partition images to Glance.

   c. Upload wholedisk images to Glance.
4. Install OS.

   a. Install OS using OpenStack Ironic.

   b. Install OS onto an FC volume.

   For more information on OpenStack Ironic features, see:

   - `redfish` driver.
   - `sdflex-redfish` driver and `sdflexutils` library.

Installing OpenStack Ironic

Procedure

Download and install OpenStack Ironic (Bare Metal Service) version Zed from the following location:

https://docs.openstack.org/ironic/zed/install/

Configuring OpenStack Ironic

Procedure

1. Configure OpenStack Ironic for `redfish` driver and `pxe`.
   a. Configure PXE and PXE-UEFI.

      Refer https://docs.openstack.org/ironic/zed/install/configure-pxe.html link for setup steps.

      NOTE: The tftproot directory may not be configured at /.

   b. Install `sudo pip install sushy`.
   c. Make the following changes in /etc/ironic/ironic.conf for Redfish enablement and **`pxe`**

      .

```
[DEFAULT]
enabled_hardware_types = ipmi,redfish
enabled_power_interfaces = ipmitool,redfish
enabled_management_interfaces = ipmitool,redfish
enabled_boot_interfaces = pxe
enabled_drivers = pxe_ipmitool

[pxe]
pxe_append_params = earlyprintk=ttyS0,115200 console=ttyS0,115200
erst_disabletftp_master_path = <”absolute path of tftpboot folder”/master_images>
#Example tftp_master_path = /opt/stack/data/ironic/tftpboot/master_images
tftp_root = <absolute path of tftpboot folder>
#Example tftp_root = /var/lib/ironic/tftpboot
tftp_server = <tftp server IP>
uefi_pxe_config_template = $pybasedir/drivers/modules/pxe_grub_config.template
uefi_pxe_bootfile_name = bootx64.efi
```

   d. Restart the ironic conductor service.
2. Configure PXE in Ironic Inspector.

   This configuration is required for the Ironic hardware inspection feature which fetches the Superdome Flex Server Hardware resource details and populates automatically to the Ironic node properties.

   a. Refer https://docs.openstack.org/ironic-inspector/zed/install/index.html link for steps.

      NOTE: Add `dhcp-boot=bootx64.efidhcp-match=set:efi-x86_64,option:client-arch,7dhcp-boot=tag:efi-x86_64,grubx64.efi` parameter and values in /etc/ironic-inspector/dnsmasq.conf as the server is a UEFI system only.

   b. Set `enabled_inspect_interfaces = inspector` parameter value in/etc/ironic/ironic.conf and restart the ironic conductor service.
3. Build or download deploy images (Ramdisk and kernel) and upload to Glance.
   a. Build deploy images which includes Ironic Python Agent from the respective release or download pre-built deploy images if available.

      Zed based pre-built Centos deploy images can be downloaded from the following links.

      - Centos deploy Ramdisk: https://tarballs.opendev.org/openstack/ironic-python-agent/dib/files/ipa-centos9-stable-

zed.initramfs

- Centos deploy kernel: https://tarballs.opendev.org/openstack/ironic-python-agent/dib/files/ipa-centos9-stable-zed.kernel

b. Upload Deploy images to Glance.

- Use the following command to upload the deploy Ramdisk image:

```
glance image-create --name ipa-centos9-stable-zed.initramfs --visibility public --
disk-format ari --container-format ari < ipa-centos9-stable-zed.initramfs
```

Use the following command to upload the deploy kernel image:

```
glance image-create --name ipa-centos9-stable-zed.kernel --visibility public --disk-
format aki --container-format aki < ipa-centos9-stable-zed.kernel
```

Create Cloud Format Images and Upload to Glance

Subtopics

Building an OS Partition Image in Cloud Format
Uploading partition images to Glance
Uploading Wholedisk Images to Glance

Building an OS Partition Image in Cloud Format

Prerequisites

This procedure applies to RHEL operating systems.

Procedure

1. Install `diskimage-builder` on any Linux system using `sudo pip install diskimage-builder` command.
2. Set RHEL Image as DIB_LOCAL_IMAGE.

   To download the RHEL cloud image procedure, see https://docs.openstack.org/diskimage-builder/latest/elements/rhel/README.html
3. Build the RHEL partition image using the command:
   `disk-image-create rhel baremetal dhcp-all-interfaces grub2 -o rhel_partition`
   .

   This command generates three images:

   - Ramdisk image: `rhel_partition.initrd`
   - Kernel image: `rhel_partition.vmlinuz`
   - User image: `rhel_partition.qcow2`
   - Enter the command:
     `mkdir mount_dir`

a. Enter the command:
`mkdir mount_dir`

b. Enter the command:
`sudo modprobe nbd`

c. Enter the command:
`sudo qemu-nbd -c /dev/nbd0 rhel-partition.qcow2`

d. Enter the command:
`sudo mount /dev/nbd0 mount_dir/`

e. Enter the command:
```
cd mount_dir
```

f. Add `console=ttyS0,115200n8 erst_disable` to the `GRUB_CMDLINE_LINUX` parameter in `etc/default/grub` file which is present inside the `mount_dir`

g. Recheck the modified file by this command:
```
cat /etc/default/grub
```

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto no_timer_check net.ifnames=0
console=ttyS0,115200n8 erst_disable"
GRUB_DISABLE_RECOVERY="true"
```

h. Enter the command:
```
sudo umount -l mount_dir/
```

i. Enter the command:
```
sudo qemu-nbd -d /dev/nbd0
```

Uploading partition images to Glance

About this task

Use the following procedure to upload RHEL partition images into Glance. The same procedure applies to upload all supported operating system partition images.

Procedure

1. RHEL 7.*x* Ramdisk:

   ```
   glance image-create --name rhel_partition.initrd --visibility public --disk-format ari --
   container-format ari < rhel_partition.initrd
   ```

2. RHEL 7.*x* kernel:

   ```
   glance image-create --name rhel_partition.vmlinuz --visibility public --disk-format aki --
   container-format aki < rhel_partition.vmlinuz
   ```

3. RHEL 7.*x* partition image:

   ```
   glance image-create --name PARTITION-IMAGE-NAME --property kernel_id=GLANCE-ID-KERNEL --
   property ramdisk_id=GLANCE-ID-RHEL-RAMDISK --visibility public --disk-format qcow2 --
   container-format bare GLANCE-ID-PARTITION.qcow2
   ```

   For example:

   ```
   glance image-create --name rhel7.9_partition.qcow2 --property kernel_id=789fbeec-ef7c-43a3-
   b89f-4f34100a9453 --property ramdisk_id=c4f0c6c4-b52a-4038-8f93-dcdd8f6c784d --visibility
   public --disk-format qcow2 --container-format bare < rhel7.9_partition.qcow2
   ```

Uploading Wholedisk Images to Glance

About this task

After the wholedisk images are created, Use the following procedure to upload the wholedisk images into Glance. The same procedure applies to upload all supported operating system wholedisk images.

Procedure

Upload wholedisk image

```
glance image-create --name WHOLEDISK-IMAGE-NAME --visibility public --disk-format qcow2 --
container-format bare <WHOLEDISK-IMAGE-NAME
```

For example, to upload RHEL 8 wholedisk image:

```
glance image-create --name rhel8-wholedisk-image.qcow2 --visibility public --disk-format qcow2
--container-format bare <rhel8-wholedisk-image.qcow2
```

Install Operating System

Subtopics

Installing OS using OpenStack Ironic

Prerequisites

This procedure applies to all supported versions of RHEL, SLES, Oracle Linux, Oracle Virtual Server, Windows 2022, Windows 2019, and Windows 2016 operating systems.

Procedure

1. Register the ironic node using the command:
   ```
   openstack baremetal node create --driver redfish --driver-info redfish_address=https://RMC-
   IP --driver-info redfish_system_id=/redfish/v1/Systems/PARTITION-ID --driver-info
   redfish_username=ADMIN-USER --driver-info redfish_password=PASSWORD
   ```
2. Obtain the node UUID using the command:
   ```
   openstack baremetal node list
   ```
3. Set `redfish_verify_ca` to `False` using the command:
   ```
   openstack baremetal set NODE-UUID --driver-info redfish_verify_ca="False"
   ```
4. Create the Ironic port using the command:
   ```
   openstack baremetal port create --node NODE-UUID MAC-ADDRESS-CHASSIS-NIC
   ```
   for OS provisioning with OpenStack Ironic 71.

   > **NOTE:** Provide the address for the chassis NIC that is not connected to the network.

   For example, `openstack baremetal port create --node e15d658a-8dcb-42a1-b1d4-dcad8be5188c 08:00:69:11:22:33`
5. Create a network port using the command:
   ```
   openstack port create --mac-address MAC-ADDRESS-CHASSIS-NIC --network NETWORK-NAME PORT-
   NAME
   ```

   > **NOTE:** Provide the address for the chassis NIC that is not connected to the network.

   For example: `openstack port create --mac-address 08:00:69:11:22:33 --network NETWORKNAME VIFport`
6. Associate the neutron port (VIFport) to the ironic port using the following commands:
   ```
   openstack baremetal node vif attach --port-uuid IRONIC-PORT NODE-UUID NEUTRON-PORT
   ```

   For example: `Openstack baremetal node vif attach --port-uuid 9415296c-a25e-4d18-8f88-0d9f4d0eab34 e15d658a-8dcb-42a1-b1d4-dcad8be5188c 734efc0c-bad2-4fa6-b1c0-`

`644d1b63a501`

7. Set the `boot_mode` to `uefi` using `openstack baremetal node set NODE-UUID --property capabilities='boot_mode:uefi'` command.

8. Set the hardware details to Ironic node properties using the command:
   `openstack baremetal node set NODE-UUID --property cpus=NUMBER-CPUs --property memory_mb=MEMORY-SIZE --property local_gb=LOCAL-STORAGE-SIZE --property cpu_arch=CPU-ARCHITECTURE`

   `openstack baremetal node set 138ded88-6d10-4d05-8a97-0e2875d7377e --property cpus=4 --property memory_mb=761408 --property local_gb=20 --property cpu_arch=x86_64`

   > **NOTE:** Ironic Inspector can be configured automatically to fetch hardware details and populate in ironic node properties. If the ironic inspector is configured, use `openstack baremetalnode inspect NODE-UUID` command.

9. Set the Glance IDs of deploy images (Ramdisk and kernel) using the command:
   `openstack baremetal node set NODE-UUID --driver-info deploy_ramdisk=RAMDISK-GLANCE-ID --driver-info deploy_kernel=KERNEL-GLANCE-ID`

   `openstack baremetal node set 138ded88-6d10-4d05-8a97-0e2875d7377e --driver-info deploy_ramdisk=b28e2d32-806e-46ad-8c1b-1f5e1b764bad --driver-info deploy_kernel=a9a82fc6-85e7-4b23-b54c-fcb022ef5c9a`

10. Set the user OS image details.

11. Set the `image_source` value with the respective OS image glance ID in the `instance_info` of the node. Use `openstack baremetal node set NODE-UUID --instance-info image_source=GLANCE-ID-USER-OS-IMAGE --instance-info root_gb=SIZE` command for OS provisioning with OpenStack Ironic.

    For example: `openstack baremetal node set 138ded88-6d10-4d05-8a97-0e2875d7377e --instance-info image_source=93d99e9d-80ec-4612-81b7-a53224c5584d --instance-info root_gb=25`

12. Perform the node validate using the command:
    `openstack baremetal node validate NODE-UUID`

13. Move the ironic node provision state to manage using the command:
    `openstack baremetal node manage NODE-UUID`

14. Move the ironic node provision state to provide using the command:
    `openstack baremetal node provide NODE-UUID`

    > **NOTE:** If `automated_clean` is set to `true` in /etc/ironic/ironic.conf, an automated clean is performed.

15. Provision OS using the command:
    `openstack baremetal node deploy NODE-UUID`

    > **NOTE:** Once the OS provisioning is complete, it moves the ironic node provision state to active and initiates the OS boot.
    >
    > Post OS installation tasks are performed when `configdrive` is configured.

Installing OS onto an FC volume

Procedure

1. Setup FC volume.
   a. Have an FC card on the Superdome Flex chassis belongs to the nPartition being enrolled as abaremetal node to OpenStack.
   b. Have the FC card connected to the same FC switch where the OpenStack FC card is connected.
   c. Install `sysfsutils` on the OpenStack using `sudo apt-get install sysfsutils` command.

d. Have the FC card on the OpenStack system in which cinder is configured.

e. Have the FC card to have a connection to an FC switch that can access SAN storage.

2. Use case 1: Install the OS to an empty FC volume (noncinder volume).

   a. Create an FC volume in the SAN storage and attach it to the Superdome Flex nPartition.

   b. Perform the steps in installing an OS with Netboot as a boot option.

      After the provisioning is complete, the OS boots from FC volume.

3. Use case 2: Install the OS to the FC volume using OpenStack Cinder.

   a. Configure SAN storage as a backend for OpenStack Cinder.

      To configure MSA as backend make the following changes in `cinder.conf`:

      ```
      [MSA]
      hpmsa_backend_name = A
      volume_backend_name = hpmsa-array
      volume_driver = cinder.volume.drivers.san.hp.hpmsa_fc.HPMSAFCDriver
      san_ip = <IP address of SAN storage>
      san_login = <SAN storage user name>
      san_password = <SAN storage password>
      hpmsa_backend_type = virtual
      hpmsa_api_protocol=https
      hpmsa_verify_certificate = False
      ```

   b. Restart the cinder service.

   c. Create cinder type using the command:
      `cinder type-create --description MSA MSA`
      .

   d. Create volume using the command:
      `cinder create --name cinder_fc --volume-type MSA size`
      .

   e. Set the storage interface as cinder in `ironic.conf` and restart the ironic services using the command:
      `enabled_storage_interfaces = cinder,noop`
      .

OpenStack Ironic Features with `redfish` Driver

The following features of OpenStack Ironic with `redfish` driver are qualified on HPE Superdome Flex Server.

For more details on OpenStack Ironic, see **https://docs.openstack.org/ironic/latest/**.

- Power operations – Power on, power off, graceful shutdown, and graceful restart.
- Automated cleaning – Performs automated cleaning (delete neutron port, removed disk metadata, and shred-baseddisk erase) during node provision and node tear down. To enable automated cleaning, set `automated_clean =True` in /etc/ironic/ironic.conf.
- Ironic inspector – Fetches Superdome Flex Server Hardware resource details and populates automatically to the ironic node properties.
- OS provisioning
  - Provisioning using wholedisk image with local boot for supported versions of RHEL 7, RHEL 8, RHEL 9, SLES 15, Oracle Linux 7, Oracle Linux8, Oracel Linux 9, Windows 2022, Windows 2019, and Windows 2016.
  - Provisioning using partition image with Localboot for supported versions of RHEL 7, RHEL 8, RHEL 9, SLES 15, Oracle Linux 7 and Oracle Linux 8, Oracle Linux 9.

- Configdrive – Performs post OS installation tasks.

  > **NOTE:** (Optional) For the procedure, see **https://docs.openstack.org/ironic/latest/install/configdrive.html** and follow the steps.

- Cinder volume attach – Provides additional storage capacity to ironic node.
- Node Rescue - Rescue operation can be used to boot nodes into a rescue Ramdisk so that the rescue user can access the node in case access to OS is not possible. For example, if there is a need to perform manual password reset or data recovery after some failure, rescue operation can be used. For more information on node rescue feature, see **https://github.com/openstack/ironic/blob/stable/zed/doc/source/admin/rescue.rst**
- Provisioning OS on to FC volume - Install OS on to FC volume and boot the OS from it.

OpenStack Ironic Features with `sdflex-redfish` Driver and `sdflexutils` Library

OpenStack Ironic with the Ironic hardware type sdflex-redfish enables the following additional features.

- Secure boot - enables configuring secure boot on the node, OS provisioning, and boot OS in secure boot mode.
- Directed LAN boot - an alternative to regular LAN boot, and is more secure as it enables baremetal to connect and boot from the specified TFTP boot file URL only.
- BIOS settings - provides mechanism to set the specified values for the BIOS parameters.
- Firmware update - provides a utility to update the complex firmware and nPar firmware.
- RAID configuration - provides an in-band RAID configuration functionality for both create and delete logical volumes.
- Hardware disk erase - provides an in-band disk erase functionality with the specified pattern using the respective storage controller utility.
- UEFI-HTTP boot - an alternative to LAN boot, and is more secure as it enables baremetal to connect and boot from the specified http boot file URL only.
- Boot from preprovisioned FC volume (SAN boot).
- Virtual Media based OS provisioning: an alternative to the regular LAN boot. It is a PXE less OS provisioning.
- IO firmware update using SUM: provides mechanism to update the IO firmware using SUM.
- DHCP less OS provisioning: to provision the OS without any dependency on DHCP setup in the network.
- Deploy-steps based OS provisioning: enables to combine some of the system configuration steps (RAID configuration, BIOS settings and SUM based IO firmware update) along with OS provisioning by onetime service OS boot for both deploy steps as well as provisioning the OS. Previously these system configuration steps were run as clean steps which results in one additional Service OS boot to perform these configuration steps and after that again boot the Service OS to provision the actual OS.

> **NOTE:** For more detailed steps on `sdflex-redfish` driver, see **https://github.com/HewlettPackard/sdflex-ironic-driver/wiki**

Troubleshooting

Subtopics

I/O firmware update with HPE OneView fails

I/O firmware update with HPE OneView fails

Symptom

If you are using HPE OneView, the I/O firmware update can fail with the following error:

```
Unable to reach out Rack Management Controller (RMC) to
clean up the configuration
```

Action

If you are using a tool such as SUM to retry, the cleanup step is required. If you retry the operation using HPE OneView, the cleanup step is not required.

Before retrying the I/O firmware update, run the following command using any Redfish client:

```
POST  https://<RMC IPaddress>/redfish/v1/Systems/Partition0/Oem/Hpe/OV/State

Content-Type: application/json
X-Auth-Token: <Auth token>
Accept: application/json
{
  "Configuration": {},
  "Deployment": {
    "Mode": "Offline",
    "StartTime": "",
    "StopTime": "",
    "Baseline": "",
    "Status": "Aborted",
    "UpdatePolicy":1
  }
}
```

More information

- HPE Superdome Flex 280 Server I/O Service Pack

Websites

HPE Superdome Flex 280 Server websites

- Product page

  www.hpe.com/support/superdomeflex280-product

- Customer documentation

  www.hpe.com/support/superdomeflex280-docs

- Software

  www.hpe.com/support/superdomeflex280-software

- HPE Foundation Software

  https://downloads.linux.hpe.com/SDR/project/hpe-foundation/

- Hewlett Packard Enterprise server operating systems and virtualization software

  www.hpe.com/us/en/servers/server-operating-systems.html

- HPE Superdome Flex 280 Server QuickSpecs

  www.hpe.com/support/superdomeflex280-quickspecs

- HPE Foundation Software (HFS) and Linux version support matrix

  https://downloads.linux.hpe.com/SDR/project/hpe-foundation/SD-Flex-LinuxSupportTables.html

- Customer advisories

  www.hpe.com/support/superdomeflex280-customer-advisories

- Spare parts list

  www.hpe.com/support/superdomeflex280-spareparts

- Release sets (support matrix)

  www.hpe.com/support/superdomeflex280-release-sets

- Safety and regulatory information

  www.hpe.com/support/Safety-Compliance-EnterpriseProducts

- Recycling information

  www.hpe.com/recycle

- Visio templates

  www.visiocafe.com/hpe.htm

  The `HPE-Integrity-MC` stencil includes HPE Superdome Flex 280 Server front and rear physical shapes.

- Supported browsers

  Google Chrome, Mozilla Firefox, and Microsoft Edge (based on chromimum)

HPE Superdome Flex 280 Server support documentation

HPE Superdome Flex 280 Server documentation for support specialists is available at **www.hpe.com/support/superdomeflex280-docs-restricted** by signing in to **Hewlett Packard Enterprise Support Center** with an entitled account.

Support and other resources

Subtopics

Accessing Hewlett Packard Enterprise Support
Accessing updates
Remote support
Customer self repair
Warranty information
Regulatory information
Documentation feedback

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  https://www.hpe.com/info/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  https://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version

- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  https://www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  https://www.hpe.com/support/downloads

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter
- To subscribe to eNewsletters and alerts:

  https://www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

  https://www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Onepass set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which initiates a fast and accurate resolution based on the service level of your product. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

HPE Get Connected

https://www.hpe.com/services/getconnected

HPE Pointnext Tech Care

https://www.hpe.com/services/techcare

HPE Complete Care

https://www.hpe.com/services/completecare

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider.

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

https://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

https://www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

https://www.hpe.com/support/Storage-Warranties

HPE Networking Products

https://www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

https://www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

https://www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

https://www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the Feedback button and icons (located at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**) to send any errors, suggestions, or comments. All document information is captured by the process.