HPE Superdome Flex Server User Guide

Part Number: 30-DDC42EAE-001
Published: August 2026
Edition: 14

HPE Superdome Flex Server User Guide

Abstract

This document provides product overview, initial setup, network configuration, and system management instructions.

Part Number: 30-DDC42EAE-001
Published: August 2026
Edition: 14

© Copyright 2017–2026 Hewlett Packard Enterprise Development LP

Notices

The information provided here is subject to change without notice. Hewlett Packard Enterprise's products and services are covered only by the express warranty statements that come with them. This document does not constitute an additional warranty. Hewlett Packard Enterprise is not responsible for any technical or editorial errors or omissions in this document.

Confidential computer software. You must have a valid license from Hewlett Packard Enterprise to possess, use, or copy the software. In accordance with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under the vendor's standard commercial license.

Links to third-party websites will take you outside of the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for the information outside the Hewlett Packard Enterprise website.

Acknowledgments

Adobe, the Adobe logo, Acrobat, and the Adobe PDF logo are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

AMD, the AMD Arrow symbol, ATI, and the ATI logo are trademarks of Advanced Micro Devices, Inc.

Intel Inside®, the Intel Inside logo, Intel®, the Intel logo, Itanium®, Itanium® 2-based, and Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Revision history

Part number	Publication date	Edition	Summary of changes
30-DDC42EAE-001	August 2026	14	Added instructions for removing LDAP group filters
10-200003-Q123	December 2022	13	• Updated release set links in the following sections: ◦ Updating superdome flex firmware ◦ Updating HPE Foundation Software for Linux systems ◦ Updating the I/O firmware and drivers • Updated Set LDAP command information. • Added a note in the SNMP alerts section.
10-200003-Q222	April 2022	12	• Added `custom_cli` option in the following sections: ◦ LDAP configuration ◦ Displaying RMC user information ◦ Changing RMC user passwords ◦ Logging in to the RMC • Added `[connection={ldap,ldaps}]` in the following sections: ◦ Set LDAP command information ◦ Displaying the current LDAP settings ◦ Logging in to the RMC
10-200003-Q122	October 2021	11	Updated password requirements
P06152-007	June 2020	10	Editorial updates.
P06152-006a	May 2020	9	Update published date and information about accessing updates.

Part number	Publication date	Edition	Summary of changes
P06152-006	March 2020	8	• Added password requirements • Added updates for LDAP names • Added Configuring iSCSI boot information • Openstack HTTP boot updates
P06152-005	December 2019	7	• Added HPE Persistent Memory • Updated and clarified JViewer information
P06152-004a	September 2019	6	Updated URL for release sets.
P06152-004	August 2019	5	• Updated safety precautions • Updated several illustrations • Revised configuration content
P06152-003	May 2019	4	• Added section on logging in to SD Flex • Added section on managing user accounts and passwords • Added section on updating SD Flex software • Added section on updating SD Flex firmware • Added section on configuring and using LDAP for user authentication • Updated several illustrations
P06152-002	June 2018	3	Added details about new support for partitionable systems.
P06152-001	March 2018	2	Updated title to HPE Superdome Flex Server User Guide.
007-6489-001	December 2017	1	Published as HPE Superdome Flex Server Getting Started Guide.

Table of contents

HPE Superdome Flex Server overview....8
Superdome Flex Server features....9
Post installation checklist....10
Safety considerations....11
Configuring the HPE Superdome Flex Server....15
Preparing to configure the HPE Superdome Flex Server....15
Information for the RMC and the BMC....17
Supported Superdome Flex Server network ports....18
Connecting the RMC or eRMC to the manageability network....18
Connecting the MGMT LAN port on the BMC to the manageability network....23
Configuring the RMC on the network....25
Connecting the RMC to the network through a USB port....25
Connecting the RMC to the network through an AUX with LAN cable....28
Changing the factory default IPMI command password recommendations....29
Changing the factory-default IPMI password on the RMC....30
Changing the factory-default passwords on the BMC....31
Verifying the HPE Superdome Flex Server is running correctly and can boot....33
Configuring the RMC to forward SNMP alerts....35
SNMP alerts....35
Managing HPE Superdome Flex Server....36
Logging in to HPE Superdome Flex Server....36
Logging in to the RMC with a browser....36
Logging in with JViewer....37
Running JViewer from a privileged account....38
Supported JViewer clients....40
Configuring a virtual folder....40
Configuring a hard disk as virtual media....43
RMC accounts and passwords....46
LDAP user authentication....48
LDAP configuration....48
Configuring LDAP server details....49
Set LDAP command information....50
Clearing LDAP settings....53
Displaying the current LDAP settings....53

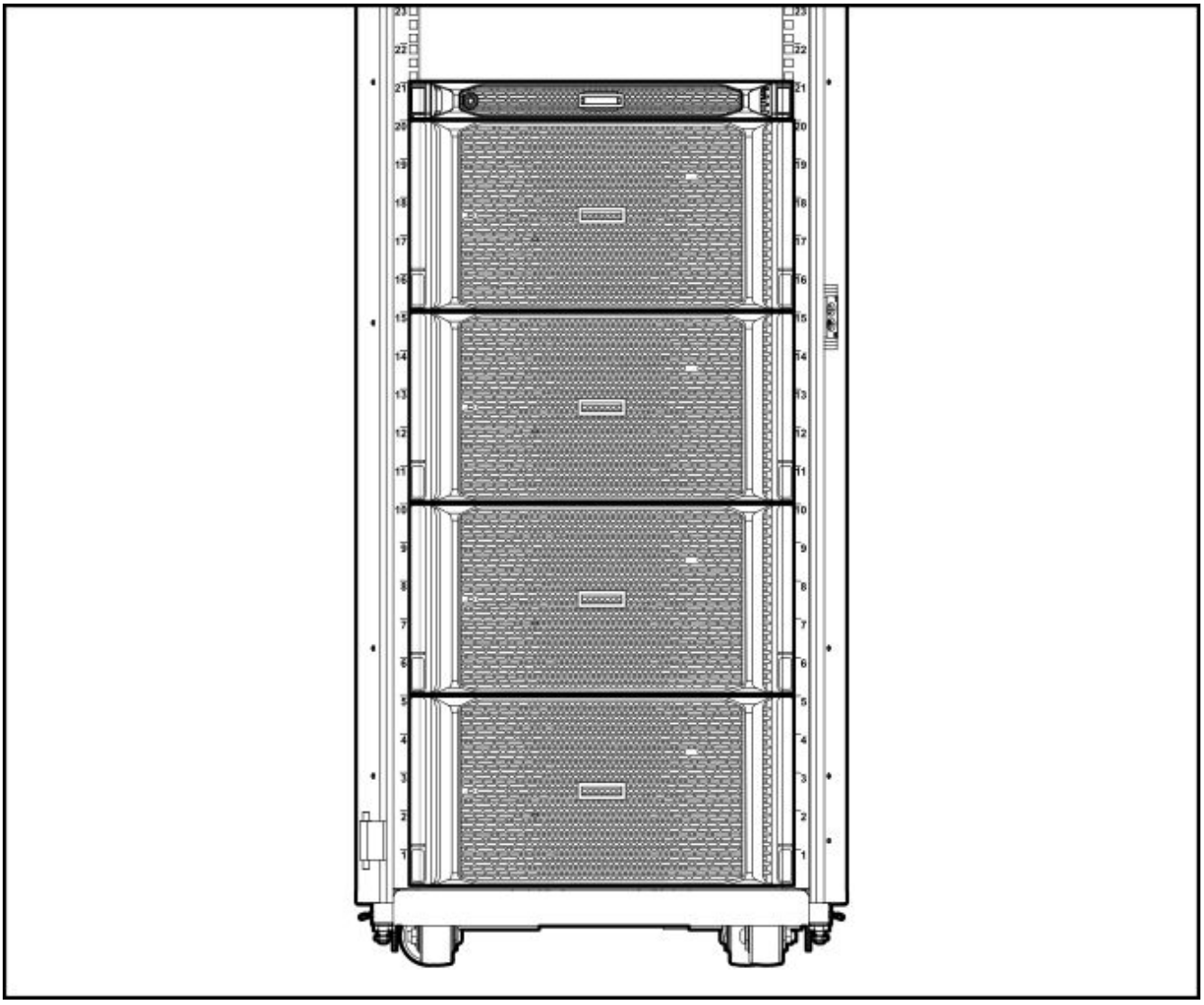
Adding new LDAP groups....54
Modifying LDAP groups....54
Removing LDAP groups and LDAP group filters....54
Displaying the current LDAP groups....55
Enabling LDAP authorization on the RMC....55
Disabling LDAP authorization on the RMC....56
Validating the LDAP configuration....56
User account management with the RMC CLI....58
Logging in to the RMC....58
Displaying RMC user information....59
Adding RMC users....60
Removing RMC users....60
Changing RMC user passwords....61
Changing RMC user roles....61
Resetting the administrator password....62
HPE Superdome Flex Server updates....62
Updating HPE Superdome Flex Server firmware....63
Updating the operating system....64
Updating HPE Foundation Software for Linux systems....65
Updating the I/O firmware and drivers on HPE Superdome Flex Server systems....65
HPE Persistent Memory on HPE Superdome Flex Server....66
Configuring iSCSI boot....66
Secure Boot....67
Secure boot features....68
Default secure boot keys....68
Enabling Secure Boot with CLI....69
Enabling Secure Boot with Boot Manager....70
Disabling Secure Boot with CLI....70
Disabling Secure Boot with Boot Manager....71
Installing or reinstalling default Secure Boot keys....72
Secure Boot Configuration menu....72
Custom Secure Boot Options menu....74
Troubleshooting OS Secure Boot issues....76
Cannot enable the Attempt Secure Boot option....76
OS boot fails from boot manager....77
OS boot fails with security violation message at UEFI Shell....77
OS update may fail on Superdome Flex servers running Linux with Secure Boot enabled....78

Websites....78
Support and other resources....80
Accessing Hewlett Packard Enterprise Support....80
HPE product registration....81
Accessing updates....81
Remote support....82
Warranty information....82
Regulatory information....82
Documentation feedback....83

HPE Superdome Flex Server overview

The HPE Superdome Flex Server is a large-scale system that uses in-memory computing technology to enable real-time transactional and analytical processing for large enterprises. This computing system has the following characteristics.

- The base chassis is the lowest chassis in the rack, carrying the overall system entitlement information.
- The expansion chassis adds on to the system from the base chassis for larger single systems without nPartition support.
- The partitionable chassis adds on to the system from the base chassis and can be used as the monarch boot chassis for nPartitions.
- Any one system has one base chassis.
- Mixing partitionable and expansion chassis is not supported.



Subtopics

Superdome Flex Server features
Post installation checklist

Superdome Flex Server features

- Each chassis supports four sockets of Intel Xeon Scalable processors.
- Each processor supports up to 12 dual in-line memory modules (DIMMs).
- SAP HANA has certified Superdome Flex Server systems.
- 48 DIMM slots of DDR4 memory per chassis provide a large memory footprint for the most demanding applications.

- The three PCIe I/O configuration options per four-socket chassis are as follows:
  - 16 half-height PCIe slots (7 x16 slots and 9 x8 slots)
  - 12 slots with eight full-height slots (4 x16 slots and 4 x8 slots) + 4 half-height slots (1 x16 slot and 3 x8 slots)
  - Compute-only configuration with no PCIe slots (expansion chassis only)
- The BaseIO includes four HDD/SSD drive bays, two 1GbE NIC ports, two 10GbE NIC ports, and four USB ports.
- A built-in DVD is included for system updates.
- The HPE Superdome Flex Server Error Analysis Engine provides system diagnostics and mission-critical reliability.
- HPE nPartitions: 4 socket to 16 socket and multiple nPartition configurations per rack are supported for greater system reliability and licensing optimization.
- Depending on the number of chassis, HPE Superdome Flex Server administration uses either an embedded rack management controller (eRMC) or a 1U rack-mounted RMC (required for partitioned systems).

For more information about features and supported configurations, see the **www.hpe.com/support/superdome-flex-quickspecs**.

Post installation checklist

Prerequisites

NOTE

HPE Foundation Software is required for all operating systems except VMware and Microsoft Windows. See the **HPE Superdome Flex Server OS Installation Guide** for additional information.

About this task

A Hewlett Packard Enterprise representative installs the system in your computer center. When the installation is complete, it is up to you to complete the following tasks.

Procedure

1. Configure the HPE Superdome Flex Server on your site network. This manual, the HPE Superdome Flex Server User Guide, explains how to complete this configuration task.
2. Install an operating system on the server.
3. Install the HPE Foundation Software on the server.

   For information on installing an operating system and the HPE Foundation Software, see **HPE Superdome Flex Server OS Installation Guide**.

Safety considerations

> **WARNING**
> Be sure to observe all Electrostatic Discharge (ESD) and safety requirements when you install or service Superdome Flex Server and RMC.

General safety

- Follow all warnings and instructions marked on the product and noted in the documentation included with this product.
- Unplug this product before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
- Do not use this product near water.
- Do not place this product, or components of this product, on an unstable cart, stand, or table. The product can fall and become seriously damaged.
- Slots and openings in the system are provided for ventilation. The slots and openings ensure reliable operation of the product and protect it from overheating. Do not block or cover these openings. Do not place this product near or over a radiator. Do not place this product near or over a heat register. Do not place this product in a built-in installation unless proper ventilation is provided.
- Never push objects of any kind into this product through cabinet slots. Such actions can touch dangerous voltage points or short out parts that could result in a fire or electric shock. Never spill liquid of any kind on the product.
- Use caution when opening or removing covers of node and switch internal components. Removing the covers can expose you to dangerous voltage points or other risks.

- Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:
  - When the power cord or plug is damaged or frayed.
  - If liquid has been spilled into the product.
  - If the product has been exposed to rain or water.
  - If the product does not operate as expected when the operating instructions are followed. Adjust only those controls that are covered by the operating instructions. Improper adjustment of other controls can result in damage and can require extensive work by a qualified technician to restore the product to normal condition.
  - The product has been dropped or the cabinet has been damaged.
  - If the product exhibits a distinct change in performance. This behavior indicates a need for service.
- Keep all system cables neatly organized in the cable management system. Loose cables are a tripping hazard that can cause injury or can damage the system.

> **CAUTION**
> Power off the system only after the system software has been shut down in an orderly manner. If you power off the system before you halt the operating system, data can be corrupted.

ESD safety

To eliminate possible ESD damage to equipment, wear ESD protection when you handle any ESD-sensitive device. When using a grounding wrist strap, connect the wrist strap cord directly to the earth ground connection provided in the rack enclosure.

Hearing safety

Wear proper hearing protection when you install or service a system.

Chassis and system weight safety

- A fully loaded chassis weighs approximately 110 lbs (50 kg). Use one of the following methods to move Superdome Flex Server safely:
  - Use a mechanical lift.

- Team lift the chassis with a partner.

> **CAUTION**
> Do not apply floor plating over open floor tiles. Unsupported floor plating can collapse under heavy equipment and result in damage to the computer equipment.

Power safety

- Operate this product only from the type of power indicated on the marketing label. If you are not sure of the type of power available, consult your dealer or local power company.
- Use only the proper type of power supply cord set (provided with the system) for this unit.
- Do not allow anything to rest on the power cord. Do not locate this product where people will walk on the cord.

Chassis movement safety

- Do not attempt to move the system alone. Moving a rack requires at least two people.
- To slide out the chassis in either direction, complete the following steps:
  - Confirm that the rack does not move. The rack feet should be down or the rack wheels should be locked.
  - Locate the release latches. The latches are on the left and right sides and in the center of the rail mounts.
  - Push in the two release latches, towards the center of the chassis.
  - Pull the chassis out using the handles. The chassis latches at the 20” limit.
  - To slide the chassis back in, press the two release latches near the rail and slide it back in.

> **CAUTION**
> Make sure that only **one** person moves the chassis in the rack at any given time. It is possible to get your fingers caught in the latches when two people attempt to move a chassis at the same time. This action can trap your finger between the metal edges of the rail mount and the rack, potentially resulting in injury.

- Slide/rail mounted equipment is not to be used as a shelf or a workspace. The following figure shows the label that appears on all hardware that has slide/rail mounted equipment:



Stepladder safety

Installing Superdome Flex Grid cables or accessing components located near the top of a rack might require using a stepladder. To properly use a stepladder:

WARNING

Always exercise caution when using a stepladder. Failure to do so may result in serious personal injury.

- Visually inspect the stepladder to make sure that the feet and steps are clean and in good repair prior to use. Do not use a stepladder that is in disrepair.
- Place the stepladder on a stable and level surface.
- Position the stepladder side-on to the rack, rather than straight on, to reduce reaching as you install components.
- Use the ladder handhold while climbing the stepladder.
- Be aware that tools and equipment that you carry up the ladder could fall from the top of the rack 2 m (6 ft.). Falling tools could cause personal injury to personnel in the work area.
- Do not rely on the slip-resistant feet to stabilize the ladder and prevent it from moving. Always stand in a stable position on the ladder in case it moves unexpectedly.
- Do not move the stepladder when someone is on it.
- Do not carry objects or loads that could cause you to lose your balance and fall.
- Do not reach too far when installing components.
- Store the ladder in a safe place that limits use by unauthorized personnel and reduces the likelihood that someone will trip on it.

Configuring the HPE Superdome Flex Server

Procedure

1. Prepare to configure the HPE Superdome Flex Server.
2. Connect the RMC or eRMC to the manageability network.
3. Connect the MGMT LAN port on the BMC to the manageability network.
4. Configuring the RMC on the network
5. Changing the factory-default IPMI password on the RMC.
6. Verify the HPE Superdome Flex Server is running correctly and can boot.
7. Configure the RMC to forward SNMP alerts.

Subtopics

Preparing to configure the HPE Superdome Flex Server
Connecting the RMC or eRMC to the manageability network
Connecting the MGMT LAN port on the BMC to the manageability network
Configuring the RMC on the network
Changing the factory default IPMI command password recommendations
Verifying the HPE Superdome Flex Server is running correctly and can boot
Configuring the RMC to forward SNMP alerts

Preparing to configure the HPE Superdome Flex Server

About this task

Hewlett Packard Enterprise recommends that you gather the information and equipment you need before you configure the HPE Superdome Flex Server.

Procedure

1. Verify the height of the rack and the doorways at your site.

   The system resides in a 42 U rack, which is 200 cm, or 78.75 inches, high.

   For more information about the physical specifications, see the HPE Superdome Flex QuickSpecs at **www.hpe.com/support/superdome-flex-quickspecs**.

2. Coordinate with the site network administrator to connect the HPE Superdome Flex Server to a private server management network within your corporate LAN.

Hewlett Packard Enterprise strongly recommends using a management network that is separate from the normal corporate LAN. Make sure to limit and restrict access to the rack management controller (RMC) management interfaces using a firewall, access control lists (ACLs), or VPN. These precautions greatly reduce many security risks.

3. Determine the configuration that the Hewlett Packard Enterprise customer engineer has performed for you.
4. Gather information for the rack management controller (RMC) and the baseboard management controller (BMC).

   Your site network administrator can help you gather the information in the following table.

If you have a 1U RMC and want to set it up using the RMC AUX port and LAN cable, go directly to step 7. Otherwise continue with step 5.

5. Locate or obtain the following equipment:
   - A system that you can connect to the RMC.
   - A terminal emulation program installed on the laptop. For example, Minicom, HyperTerminal, or PuTTY.
   - The RMC cable, which was included in the shipping crate. This cable is a USB-A to micro USB-B cable, and it bears one of the following part numbers:
     - 018-1667-001
     - P0005521-001
   - Ethernet cables. You, the customer, must provide cables to connect each HPE Superdome Flex Server chassis to your network. Make sure that the cables are long enough to extend from each chassis to your LAN ports. For example, if you have two chassis, you need two Ethernet cables.
6. (Optional) Install drivers on your Windows laptop.
   a. If necessary, download the Windows shim for PuTTY and install the shim on your laptop.
   b. Different drivers are required for systems with an RMC or an eRMC. Download and install one of the following drivers on your laptop.
      - A driver shim for the RMC serial port
      - A driver for the eRMC serial port

   For details on installing the Windows drivers, see **Accessing HPE Superdome Flex Server RMC or eRMC from Windows**.
7. (Optional) Use this step only if you have a 1U RMC and want to set it up using the RMC AUX port and LAN cable.

The RMC AUX port is preconfigured with zero-conf IP address 169.254.0.254. This AUX port is not available on systems with eRMC.

a. Connect a laptop/PC supporting zero-conf IP address in the subnet 169.254.0.0/16 directly to the RMC AUX port with a LAN cable.

b. SSH from the laptop to the RMC address 169.254.0.254 and finish setting up the system.

Subtopics

Information for the RMC and the BMC
Supported Superdome Flex Server network ports

More information

Information for the RMC and the BMC

Information for the RMC and the BMC

Table 1. Information for the RMC and the BMC

Information	Value
A site-specific RMC `administrator` user password and an `ipmi` command password. [1]	
RMC configuration	
Static IP address or DHCP	
Hostname or DHCP	
Subnetwork mask or DHCP	
BMC configuration	
Static IP address or DHCP	
Hostname or DHCP	
Subnetwork mask or DHCP	
Common configuration	
NTP Server IP address	

Information	Value
Nameserver IP addresses (up to two)	
Resolver domain search list (optional) - Hewlett Packard Enterprise recommends keeping it short to avoid lengthy name resolution for unknown names.	

[1] Hewlett Packard Enterprise configures a default RMC user password at the factory. The configuration process directs you to define a site-specific password.
By default the `ipmi` command password is the same as the factory-configured RMC user password. The configuration process directs you to define a site-specific `ipmi` command password.

> **NOTE**
>
> A site-specific IPMI password is only necessary if IPMI over LAN is turned on. If you are not using IPMI over LAN, then there is no need to change the default IPMI password.

Hewlett Packard Enterprise recommends that you configure the same password for both the RMC `administrator` user and `ipmi` user.
The BMC Superdome Flex chassis running FW 3.0.512 or later will use the RMC/eRMC local account to authenticate JViewer, KVM, and Virtual Media.

Supported Superdome Flex Server network ports

Superdome Flex servers use the following network ports:

- 443: RMC Redfish and web server traffic
- 636: LDAP traffic
- 1443: JViewer and BMC traffic

Connecting the RMC or eRMC to the manageability network

Prerequisites

HPE recommends that the management network is separated from the other networks at a customer site.

About this task

An external, self-contained rack management controller is called an **RMC**. A rack management controller embedded within the base chassis is called an **eRMC**.

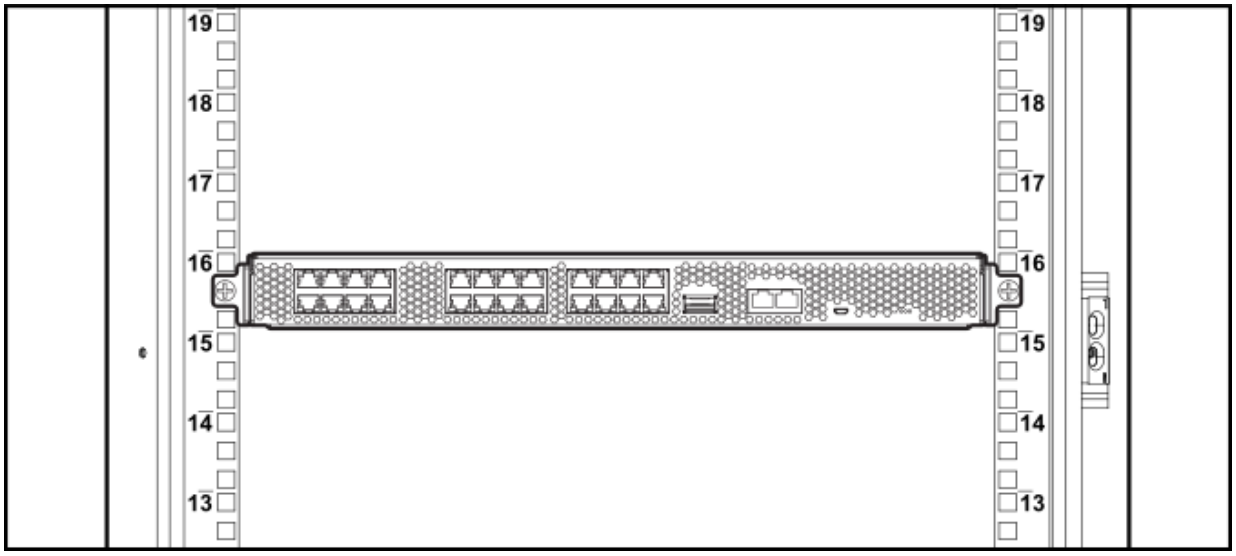
The RMC or eRMC is the administrative node for the HPE Superdome Flex Server that includes one network port for administrative access to the system console.

Procedure

The following procedure explains how to connect the RMC to a private server management network within a corporate LAN.

1. Locate the RMC at the back of the HPE Superdome Flex Server.

   - An RMC is a 1U rackmounted component.

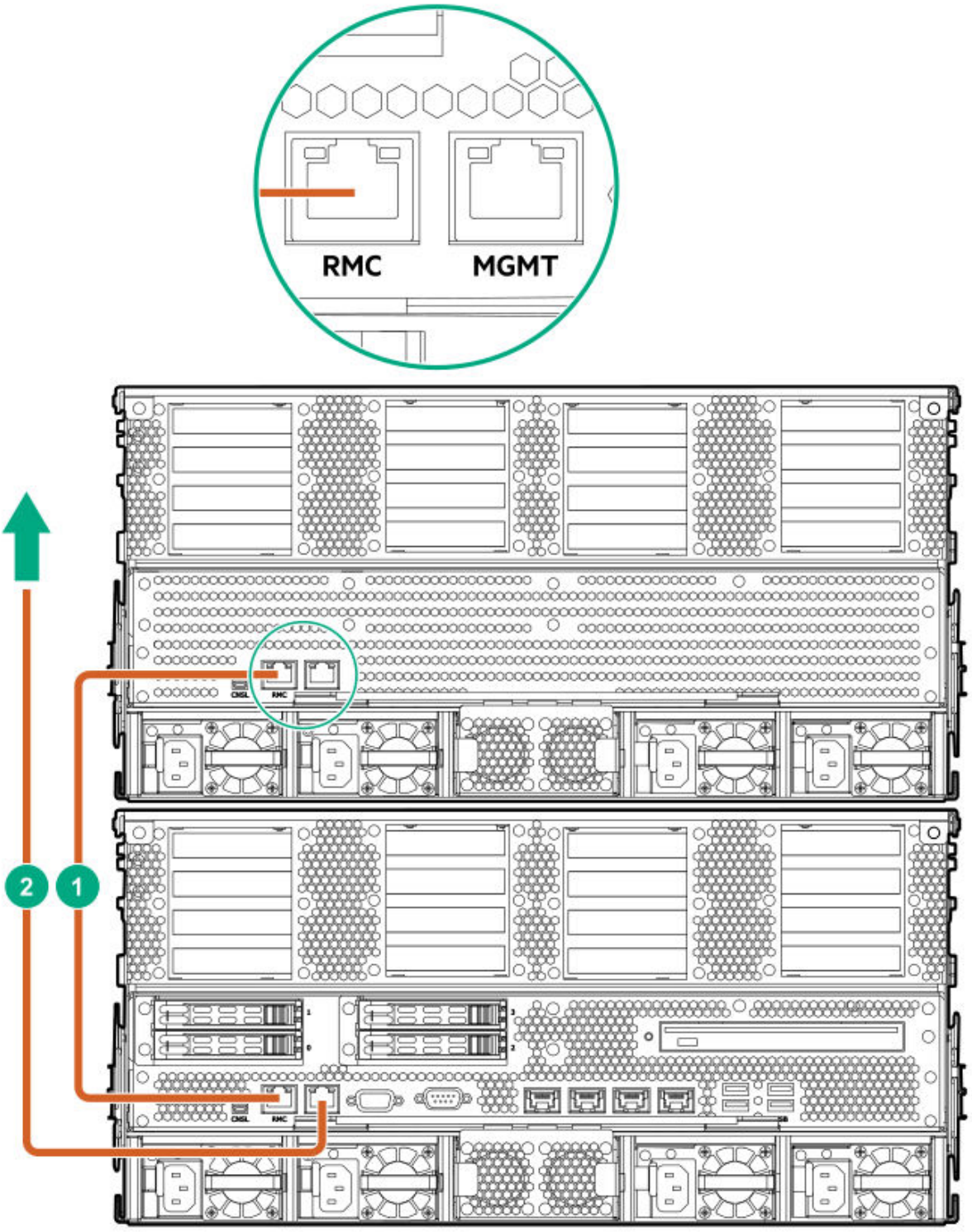
   

   In a partitionable system, an RMC is required regardless of the number of chassis.

   If there are three or more chassis in a system, an RMC is required.

   - In a one-chassis or two-chassis nonpartitionable system, you can use an RMC or an eRMC.

     The following figure shows how a two-chassis system that uses an eRMC is configured.

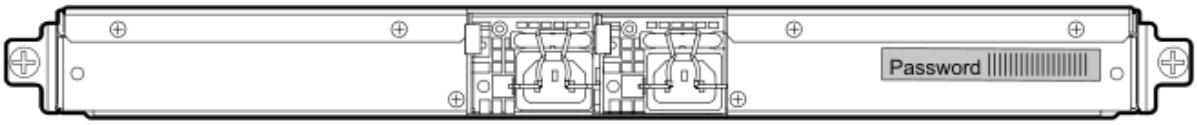


- ① RMC port to RMC port connection
- ② MGMT port to site management network connection

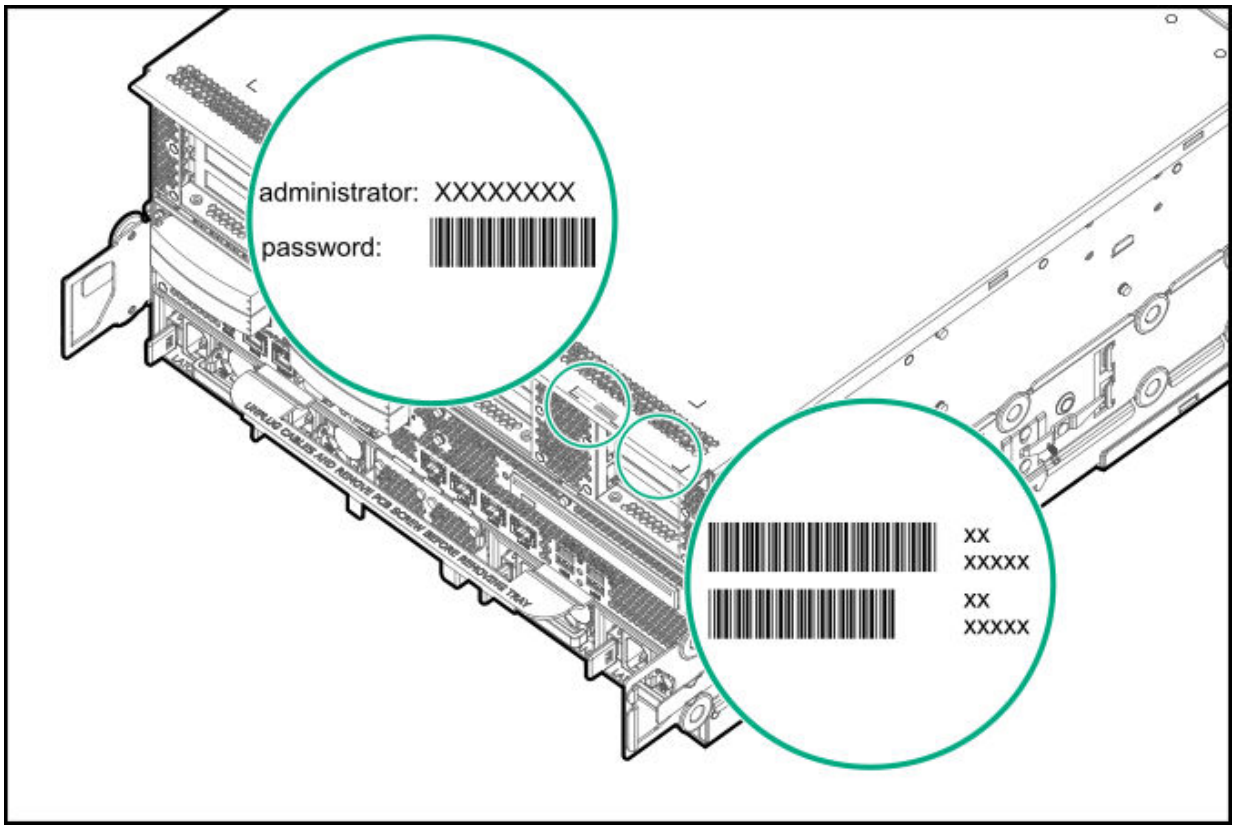
2. Locate the RMC password sticker.

   The sticker has a bar code and the factory default password written on it.

- If the system uses an RMC, this sticker is on the rear of the 1U rackmounted component.

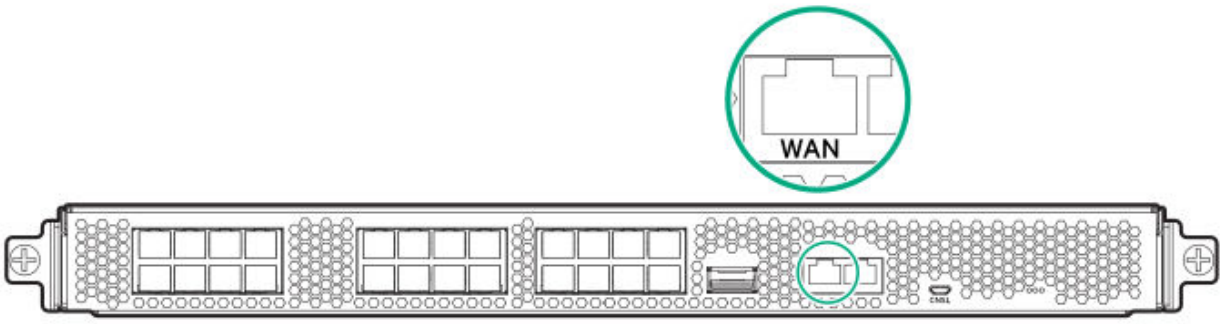


- If the system uses an eRMC, the sticker is on the top-right rear corner of the base chassis (at the lowest U position in the rack).

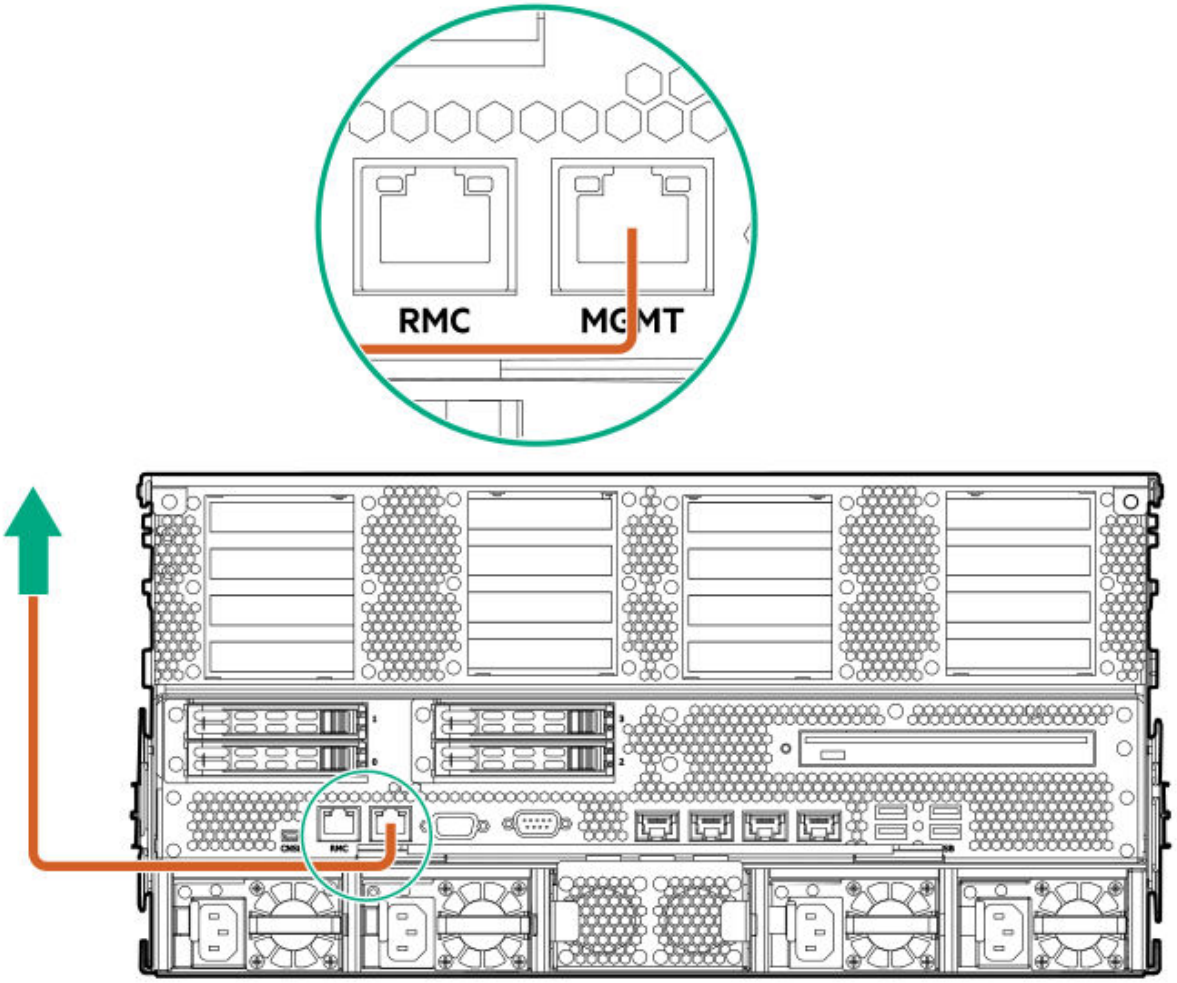


3. Use Ethernet cables and the expansion chassis figure in Step 1 to connect the RMC to the manageability network.

    - If the system uses an RMC, plug one end of the Ethernet cable into the WAN port on the RMC. Plug the other end into the manageability network.



- If the system uses an eRMC, plug one end of the Ethernet cable into the MGMT port on the base chassis BMC. Plug the other end into the manageability network.



Connecting the MGMT LAN port on the BMC to the manageability network

Prerequisites

Complete this procedure under the following conditions.

- You have a 1U RMC and you must use JViewer when installing the operating system software on the server.

  For more information about JViewer, see **HPE Superdome Flex Server OS Installation Guide**.

- When JViewer is required, the monarch chassis must be connected to the management LAN.

About this task

The MGMT LAN port facilitates end-user communication to the BMC.

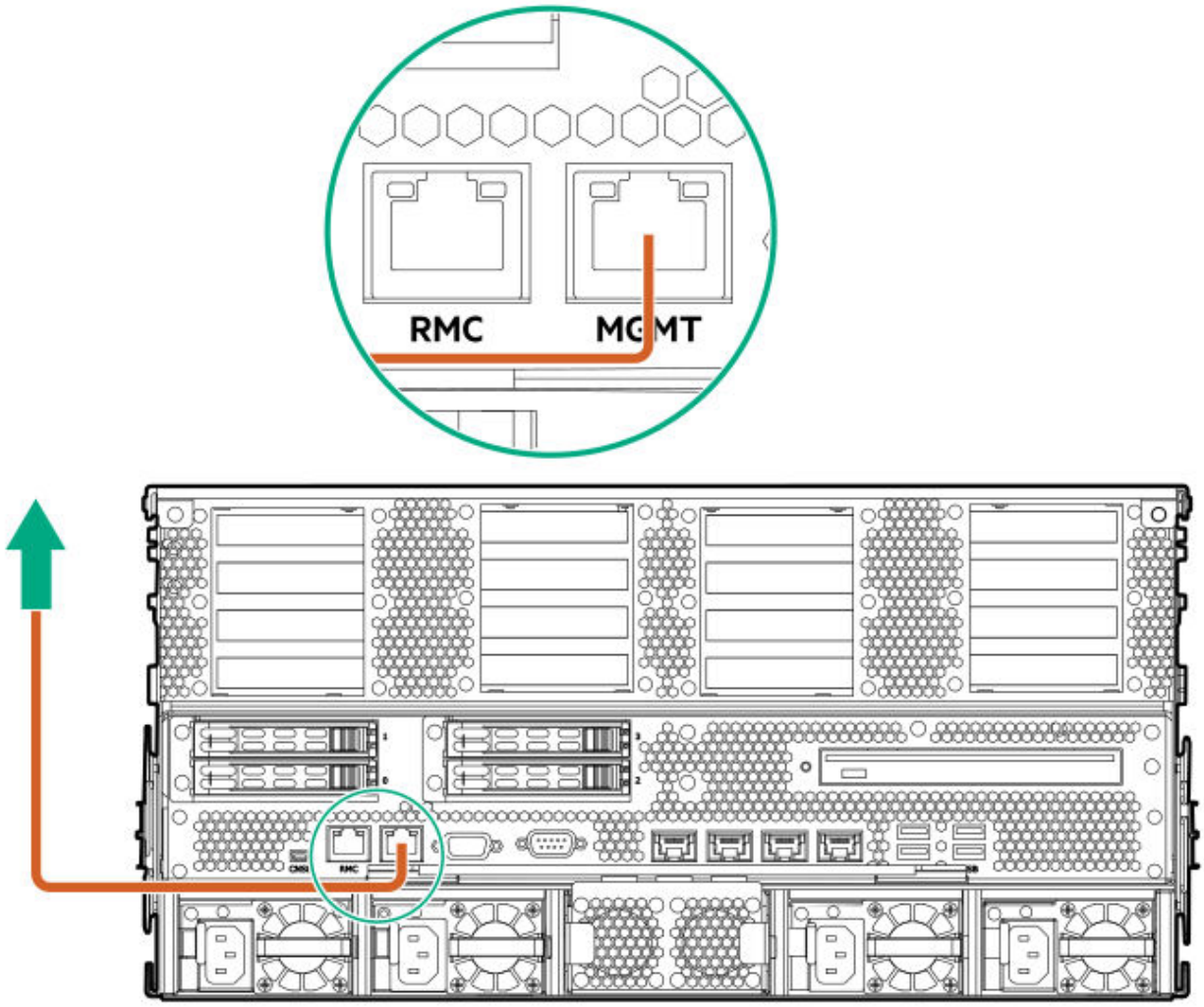
Procedure

1. Locate the chassis that contains the BMC.

   The BMC is located in the lowest numbered chassis, which resides at the bottom of the rack.

2. Plug one end of an Ethernet cable into the MGMT port on the BMC. Plug the other end of the Ethernet cable into the manageability network.

   The following figure shows the rear view of the server. The MGMT port is the Ethernet port that is second from the left.



You can configure the MGMT port with the `set network baseio=GEOID` RMC command.

NOTE

For full flexibility to redefine nPars in the future without adding LAN cables, connect all MGMT ports on the Base and Partitionable Chassis to the management LAN.

- For a non-partitionable system, consisting of a Base Chassis and additional Expansion Chassis, connect the MGMT port on the Base Chassis to the management LAN for JViewer communication.
- For a partitionable system, connect the MGMT port on the lowermost, monarch chassis for each nPar to the management LAN.

Configuring the RMC on the network

Prerequisites

The manageability network must be a private server management network within a corporate LAN.

To connect to the RMC, choose one of these two methods:

- **USB**—For more information, see Connecting the RMC to the network through a USB port.
- **AUX with cable**—For more information, see Connecting the RMC to the network through an AUX with LAN cable.

Subtopics

Connecting the RMC to the network through a USB port
Connecting the RMC to the network through an AUX with LAN cable

More information

Connecting the RMC to the network through a USB port
Connecting the RMC to the network through an AUX with LAN cable

Connecting the RMC to the network through a USB port

Prerequisites

The manageability network must be a private server management network within a corporate LAN.

Procedure

1. Locate the USB-A to Micro-USB-B cable that was included in the shipping crate.

   The cable is either part number 018-1667-001 or part number P0005521-001.

2. Plug in the cables.

   a. Plug the USB-A connector into the laptop.

   b. Do one of the following:

      - If the system uses an RMC, plug in the Micro-USB (USB Micro-B) connector into the CNSL port of the RMC.

- If the system uses an eRMC, plug in the Mini-USB (USB Mini-B) connector into the CNSL port of the RMC in the lowest numbered chassis (the base chassis).

> **NOTE**
>
> If you are using a Windows laptop, you might need to load the driver for the eRMC serial port or the driver shim for the RMC serial port. For information about loading these drivers, see **Accessing HPE Superdome Flex Server RMC or eRMC from Windows**.

3. In the serial terminal window, use your terminal emulation program instructions to set the following parameters:
   - Baud rate: 115200
   - Data bits: 8 (default)
   - Parity: No (default)
   - Stop bits: 1 (default)
   - Hardware flow control (RTS/CTS): No
4. Display the CLI prompt by pressing **Enter**.
5. Retrieve the planning information you collected in Preparing to configure the HPE Superdome Flex Server.
6. Specify the network settings.

```
set network addressing=METHOD gateway=GATEWAY_IP
hostname=HOSTNAME ipaddress=HOST_IP
netmask=SUBNETMASK
```

7. Specify the NTP server for the HPE Superdome Flex Server:

```
set ntp ipaddress=IP_ADDR | FQDN of NTP
```

8. If the RMC will participate in name resolution, add DNS name servers and a domain name search list.

```
RMC cli> add dns ipaddress=IPADDRESS1
RMC cli> add dns ipaddress=IPADDRESS2
RMC cli> add dns search=DOMAIN1
RMC cli> add dns search=DOMAIN2
```

9. Specify your time zone.
   a. Retrieve the list of time zone codes.

```
help set timezone str
```

b. Choose a location that is in your time zone and specify your time zone code:

```
set timezone str=CODE
```

For example:

```
RMC cli> set timezone str=America/Thunder_Bay
```

10. Change the RMC `administrator` user password.

```
set password
```

The system prompts for the `administrator` user password when the `administrator` user logs into the RMC over the network.

> **NOTE**
>
> The factory-assigned `administrator` user RMC password is on an Hewlett Packard Enterprise factory label as shown in Locate the RMC password sticker. If a customer changes this password, they assume responsibility for keeping this password known to their staff and to Hewlett Packard Enterprise representatives who might need the RMC password in the future.

11. Reboot the RMC for the changes to take effect.

```
reboot rmc
```

12. To test new IP address and password for the RMC, open another terminal window, and enter the following command:

```
ssh administrator@NEW_RMC_IP_ADDRESS
```

13. View the DNS configuration.

```
show dns
```

14. Display and make note of the RMC hostname and IP address.

```
show network
```

15. Verify the time and date settings.

```
show date
```

16. Remove the USB cable from the RMC and from your laptop.

Connecting the RMC to the network through an AUX with LAN cable

Prerequisites

The manageability network must be a private server management network within a corporate LAN.

Procedure

1. Connect LAN cable to RMC AUX.
2. SSH with laptop and log in to RMC.
3. Display the CLI prompt by pressing **Enter**.
4. Retrieve the planning information you collected in Preparing to configure the HPE Superdome Flex Server.
5. Specify the network settings.

   ```
   set network addressing=METHOD gateway=GATEWAY_IP
   hostname=HOSTNAME ipaddress=HOST_IP
   netmask=SUBNETMASK
   ```

6. Specify the NTP server for the HPE Superdome Flex Server:

   ```
   set ntp ipaddress=IP_ADDR | FQDN of NTP
   ```

7. If the RMC will participate in name resolution, add DNS name servers and a domain name search list.

   ```
   RMC cli> add dns ipaddress=IPADDRESS1
   RMC cli> add dns ipaddress=IPADDRESS2
   RMC cli> add dns search=DOMAIN1
   RMC cli> add dns search=DOMAIN2
   ```

8. Specify your time zone.
   a. Retrieve the list of time zone codes.

      ```
      help set timezone str
      ```

   b. Choose a location that is in your time zone and specify your time zone code:

      ```
      set timezone str=CODE
      ```

      For example:

      ```
      RMC cli> set timezone str=America/Thunder_Bay
      ```

9. Change the RMC `administrator` user password.

   ```
   set password
   ```

The system prompts for the `administrator` user password when the `administrator` user logs into the RMC over the network.

> **NOTE**
>
> The factory-assigned `administrator` user RMC password is on an Hewlett Packard Enterprise factory label as shown in Locate the RMC password sticker. If a customer changes this password, they assume responsibility for keeping this password known to their staff and to Hewlett Packard Enterprise representatives who might need the RMC password in the future.

.0. Reboot the RMC for the changes to take effect.

```
reboot rmc
```

.1. To test new IP address and password for the RMC, open another terminal window, and enter the following command:

```
ssh administrator@NEW_RMC_IP_ADDRESS
```

.2. View the DNS configuration.

```
show dns
```

.3. Display and make note of the RMC hostname and IP address by entering the following command.

```
show network
```

Changing the factory default IPMI command password recommendations

> **IMPORTANT**
>
> By default, the IPMI password is the same as the factory default rack management controller (RMC) `administrator` password. Hewlett Packard Enterprise recommends that you change the default IPMI password to match your site-specific RMC password.

The IPMI 2.0 specification has inherent security weaknesses. Consider using the Redfish manageability standard in Superdome Flex Server, which is designed to replace IPMI. Hewlett Packard Enterprise recommends that if you do not need to use IPMI, it must remain disabled. If you must use IPMI, use a separate management LAN and change the IPMI command password.

For information about how to use the `ipmi` command or the `ipmitool` command to access the RMC remotely, see **HPE Superdome Flex Server Administration Guide**.

Use one or both of the following procedures to change the IPMI password in specific system configurations.

- For all systems (using an RMC or an eRMC), to change the IPMI password, complete the following procedure.

  Changing the factory default IPMI password on the rack management controller (RMC)

- For systems using an RMC (not using an eRMC), complete the following procedure to change the IPMI password on the base chassis baseboard management controller (BMC).

  Changing the factory default passwords on the baseboard management controller (BMC)

Subtopics

Changing the factory-default IPMI password on the RMC
Changing the factory-default passwords on the BMC

Changing the factory-default IPMI password on the RMC

Prerequisites

You must be logged into RMC as the `administrator` user.

About this task

Complete this procedure for all systems using an RMC or an eRMC.

Procedure

1. Retrieve a list of user IDs using the `user list` command:

   ```
   ipmi command="user list"
   ```

   For example:

   ```
   RMC cli> ipmi command="user list"
   ID    Name        Callin  Link Auth   IPMI Msg       Channel Priv Limit
   2     ADMIN       true    false       true           ADMINISTRATOR
   ```

2. Examine the command output and note the `ADMIN` user ID.

   For example, in the preceding step, the user ID is `2`.

3. Change the password for the `ADMIN` user using the `user set password` command.

```
ipmi command="user set password USER_ID NEW_PASSWORD"
```

Specify the user ID you obtained earlier in this procedure. For example, `2` is the user ID of the `ADMIN` user.

More information

Verifying the HPE Superdome Flex Server is running correctly and can boot
Changing the factory-default passwords on the BMC

Changing the factory-default passwords on the BMC

Prerequisites

> **NOTE**
> Skip this section if your system is running with FW 3.0.512 or later.

Complete this procedure for systems using an RMC but not using an eRMC.

About this task

Hewlett Packard Enterprise recommends changing the password to a strong password for the administrator and `ipmi` on all BMCs. In addition, Hewlett Packard Enterprise recommends that the site-specific password you create match the password you chose for the RMC `administrator` user and the IPMI password for the RMC.

Procedure

1. Log in to the RMC through ssh as `administrator`.

   Use the password that was previously set for `administrator` on the RMC.

2. Run `BASEIOLIST` and make note of the base BMC `GEOID`.

   For example:

   ```
   RMC cli> baseiolist

       P000 [r001i01b]:   192.168.5.21      [08:00:69:17:A1:B1]
   ```

   The `GEOID` is `r001i01b` in this example.

3. List the base BMC IPMI users.

   ```
   RMC cli> bmc ipmi user list GEOID
   ```

Where:

GEOID

Is from step 2

Note the ID number for user `admin`.

For example:

```
RMC cli> bmc ipmi user list r001i01b

    ==== r001i01b ====
    ID  Name         Callin  Link Auth  IPMI Msg   Channel Priv Limit
    1                    false   false      true       ADMINISTRATOR
    2   admin            false   false      true       ADMINISTRATOR
```

For information about how to use the `ipmi` command or the `ipmitool` command to access the RMC remotely, see **HPE Superdome Flex Server Administration Guide**.

4. Change the base BMC user admin password: .

```
bmc ipmi user set password ID PASSWORD GEOID
```

Where:

ID

Is from step 3

Password

Is the new password

GEOID

Is from step 2

5. Verify that the base BMC IPMI `admin` user password has been changed.

```
bmc ipmi user test ID 16
                  PASSWORD GEOID
```

Make sure that `Success` is seen.

For example:

```
RMC cli> bmc ipmi user test 2 16 PASSWORD r001i01b

    ==== r001i01b ====
    Success
```

Verifying the HPE Superdome Flex Server is running correctly and can boot

Prerequisites

You can perform this procedure in one of the following ways:

- When directly cabled to the RMC (either a 1U rackmounted RMC or an eRMC).
- Using another computer at your site that can reach the system over a network connection.

> **NOTE**
> Hewlett Packard Enterprise recommends that you use the xterm terminal emulator. Some other terminal emulators do not accept the key sequences in the configuration procedures.

Procedure

1. Open two terminal sessions to the RMC, and log in as the `administrator` user in each session.

   On the monitor, orient the terminal sessions one on top of the other.

2. On your physical monitor, orient the terminal sessions one on top of the other.

3. In the bottom window, enter the following command:

   ```
   connect npar pnum=0
   ```

   This example shows partition 0. On a nonpartitionable system, all chassis are part of a single nPartition (partition 0). On a partitionable system, multiple nPartitions may be configured. In this window, you can observe the boot, look for error messages, or interrupt the boot sequence.

4. In the top window, enter the following command, and observe the output:

   ```
   show complex
   ```

   - If the output in the top window is similar to the following, the BMCs are configured properly. You can proceed to the next step in this procedure.

     ```
     RMC cli> show complex

     SSN: 5UF6510999

     RMCs:             1
             r001i11c RMC-UV400
     ```

```
BMCs:            2
        r001i01b IP147-BASEIO    P000
        r001i06b IP147           P000 BASEIO-DISABLED

Partitions:      1
        partition000 BMCs:    2
                r001i01b
                r001i06b
RMC cli>
```

- If the output contains a message that is similar to the following, the BMCs are not configured properly.

  ```
  WARNING: 2 BMC(s) are not configured
  ```

  If you receive this warning message, or if the BMCs fail to present, go to **Hewlett Packard Enterprise Support Center website**.

> **NOTE**
>
> After the chassis is connected to AC power, it can take up to two minutes for the BMC to be configured.

5. In the top window, enter the following command.

   ```
   power on npar pnum=0
   ```

   The `RMC cli>` prompt will appear after power has been applied, which can take 3 to 4 minutes.

6. In the top window, enter the following:

   a. Monitor the hardware initialization by entering the following command.

   ```
   RMC cli> show livelogs
   .
   .
   .
   .....  EFI_EXIT_BOOT_SERVICES
   ```

   b. When the line that ends in `EFI_EXIT_BOOT_SERVICES` appears, you can close this window. To exit the `livelogs` display, enter **`q`**.

7. In the bottom window, when the `Shell>` prompt appears (which can take several minutes), press **CTRL +]+q** to exit the shell.

More information

Configuring the RMC on the network

Configuring the RMC to forward SNMP alerts

Procedure

1. Verify that you are logged into the RMC as the `administrator` user.
2. Specify the destination IP address for SNMP alerts.

   ```
   set snmp forward_address=IP_ADDR
   ```

3. Reboot the RMC.

   ```
   RMC cli> reboot rmc
   ```

Subtopics

SNMP alerts

More information

SNMP alerts

SNMP alerts

A management information base (MIB) is a specification that defines management information and events. The management information consists of the system configuration, field-replaceable unit (FRU) information, and environmental information. The events are alert (SNMP trap) information that is generated when an environmental sensor trips a threshold. For example, a fan failure trips a threshold. The MIB definitions include the RMC and the server itself. The management software uses the MIB to convert low-level SNMP variables to readable names, such as `CPU2_TEMP`. The RMC and the BMCs manage SNMP alerts, with the RMC receiving the SNMP alerts that the BMCs generate.

Hewlett Packard Enterprise also supports the Redfish standard, with Redfish Alerting and Eventing available for subscription as well. Selected events are sent over the network toward specified event receivers. The event receivers send a subscription request to the RMC/BMC containing the types of event that they are prepared to receive and process. Setting up a client to receive these alerts is done according to the DMTF.org Redfish standard. You can use standard redfish clients, for example `Redfishtool`, to monitor and manage the RMC/BMC. For the richest monitoring experience, Hewlett Packard Enterprise recommends

HPE OneView (**http://hpe.com/go/oneview**). HPE OneView uses the Redfish alerting and eventing, rather than SNMP.

> **NOTE**
>
> The default SNMP community string on the HPE Superdome Flex Server should not modified. If the string is modified, the SNMP alerts are not generated and can impact the error reporting on the system.

Managing HPE Superdome Flex Server

Subtopics

Logging in to HPE Superdome Flex Server
RMC accounts and passwords
HPE Superdome Flex Server updates

Logging in to HPE Superdome Flex Server

There are two ways to log in to HPE Superdome Flex Server.

- Log in to the RMC with a browser first
- Logging in with JViewer

Subtopics

Logging in to the RMC with a browser
Logging in with JViewer
Configuring a virtual folder
Configuring a hard disk as virtual media

Logging in to the RMC with a browser

Procedure

1. Enable the RMC HTTPS protocol by entering the following command:

```
RMC cli> enable https

HTTPS is enabled
```

2. Open a browser and connect to the RMC by entering the following command

```
https://flex-rmc
```

3. Select the partition you want to manage.
4. Log in using your RMC credentials and click **Sign me in**.

   After you log in, the HPE Superdome Flex Server home page is displayed.

   From the home page, you can access management functions, such as:

   - Using HTML5 KVM and attaching an ISO.
   - Installing an OS or HPE Foundation Software (HFS). See **HPE Superdome Flex Server OS Installation Guide**.
   - Configuring a virtual folder
   - Configuring a hard disk as virtual media

   Using these management functions requires the use of the JViewer application that must be run from a privileged account. JViewer is described in the following sections.

More information

Configuring a virtual folder
Configuring a hard disk as virtual media

Logging in with JViewer

About this task

JViewer is a standalone Java application, and can be used to connect to HPE Superdome Flex Server. However, the RMC browser login is the recommended, more secure, connection method.

> **NOTE**
> Launching JViewer from a MacOS client is not supported

Procedure

1. Download JViewer with the Superdome Flex webpage.

2. Log in to JViewer.
3. Select **Download Virtual Media Application**, and then select the `jviewer-sa.jar` file.

   Note the folder where the file is downloaded.

Subtopics

Running JViewer from a privileged account
Supported JViewer clients

More information

Supported JViewer clients
Logging in to the RMC with a browser

Running JViewer from a privileged account

About this task

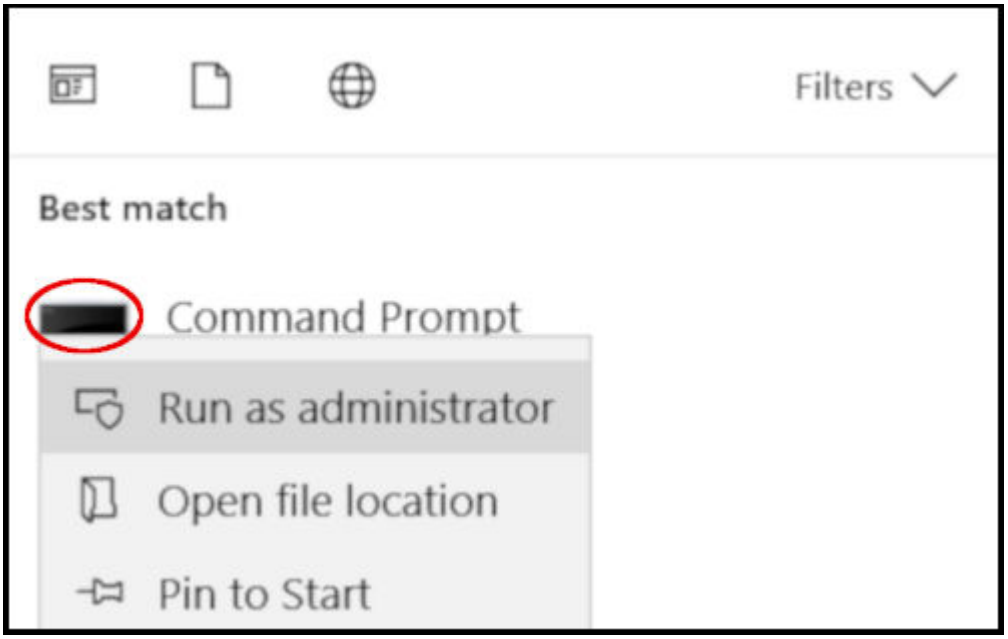
Using Virtual Hard Disks, vFolders, and DVD driver redirection requires that JViewer is run from a privileged account. On Windows 10, one approach is to access the Windows command line as the administrator user, and then run JViewer from that command line. For more information about using JViewer with vFolders, see the **HPE Superdome Flex Server OS Installation Guide**.

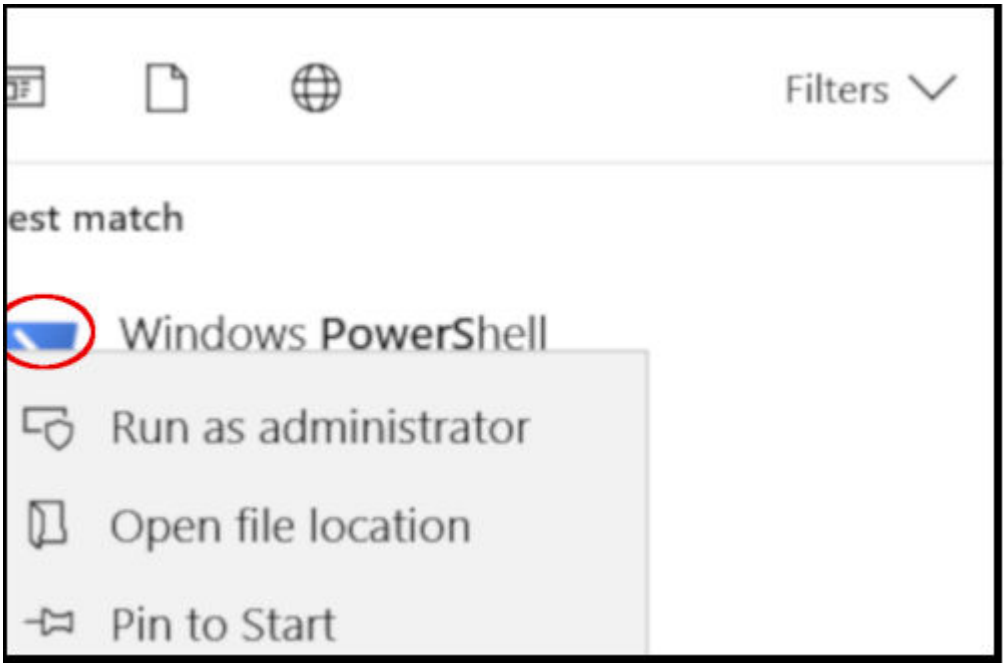
Procedure

Windows provides two command-line options.

- **Command Prompt**
- **Windows PowerShell**

1. In the search box, enter **`cmd`** or **`powershell`**.
2. Right-click the icon, and then select the **Run as administrator** option.





3. When the command line is displayed, run the JViewer using the following syntax:

```
java -jar jviewer-sa.jar [-hostname BMC_HOSTNAME] [-u USERNAME] [-p PASSWORD]
```

> **NOTE**
>
> `java` must be in your path, otherwise specify the full path to your installed `java.exe` file.

Supported JViewer clients

HPE Superdome Flex Server supports launching JViewer from the following client environments.

Table 1. HPE Superdome Flex Server recommended JDK versions

OS	Browser	Oracle Java versions	Open JDK versions
SLES 15	Firefox	JDK 7 and 8	JDK 8 to JDK 11
RHEL 7	Firefox	JDK 7 and 8	JDK 8 to JDK 11
Windows 2016	Firefox, Edge, Chrome, and Internet Explorer	JDK 7, 8, and 9	JDK 8 to JDK 11
MacOS	Not supported	Not supported	Not supported

Configuring a virtual folder

Prerequisites

You are logged in as an administrator. See Logging on to the RMC with a browser.

About this task

The virtual folder feature takes the selected folder from your PC and bundles it into an intermediate Disc Image File (`.ima`). The Disc Image File is then connected with the server through VMedia. When the image file is disconnected, any changes that were made to it from the server, may be synchronized back to the original folder. The contents of the original folder will be overwritten. The Disc Image File is then deleted.

Procedure

1. Log in to the webpage of the partition you want to manage and navigate to **Settings > Media Redirection > VMedia Instance Settings**.
2. On the **VMedia Instance Settings** page, change the **Hard disk instances** to a value representing the number of vFolders that you want to share with the server. Click **Save**.
3. On the KVM home page, select **Remote Control** and click **Download Virtual Media Application**.

   The `JViewer-sa.jar` file will be downloaded.
4. Run `JViewer-sa.jar`.

```
PS C:\Users\User\Downloads> java -jar .\JViewer-sa.jar -u administrator
-p secret -hostname flex-bmc2
```

5. Click the **Hard Disk/USB** tab and enter the following required information:

   Folder Path

   Contains the raw contents to be shared with the server. Browse to the folder name you want to share with the server, such as `vFolder`.

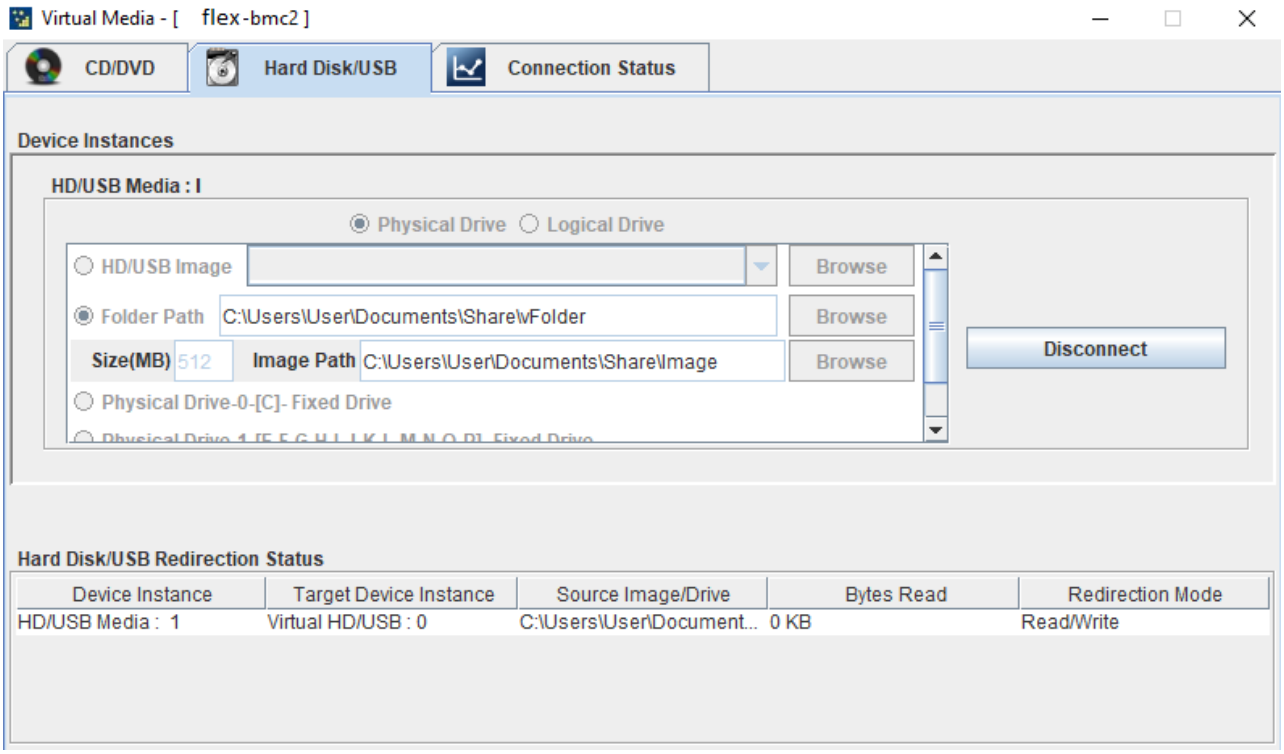
   Size (MB)

   Sets the size of the intermediate image file created from the folder path, that will be shared with the server. It has a maximum size of 512 MB and its size must be larger than the contents of the folder path. If you want to save data from the server back to the virtual folder, then create the image file large enough to accommodate the extra data.

   Image Path

   The location where the intermediate image file will be stored while the VMedia connection is active.

6. Click **Connect** next to the drive you selected.



When connected, the image file is shared with the server.

7. Power on the server with the RMC.

```
power on npar pnum=1 bootopt=Shell
```

`bootopt=Shell` forces the console to stop at the UEFI Shell prompt.

8. Access the console either by launching the KVM from the webpage or opening a text console from RMC.

```
connect npar pnum=p1
```

9. From the console, enter the `map -r` command and search for filesystem devices (FS) that have a USB designator.

```
Shell> map -r
Mapping table
     FS0: Alias(s):HD1m0c0:;BLK1:
          PciRoot(0x0)/Pci(0x14,0x0)/USB(0xC)

Shell> fs0:
FS0:\> dir
Directory of: FS0:\
01/18/2019 06:35             10,660  fs0.txt
01/18/2019 06:34
64  README.txt
          2 File(s)     10,724 bytes
          0 Dir(s)
```

10. Save the data from UEFI to the Virtual Folder.

For example: Save the output from the `map -r` command to the filename `map-r.txt`, which is then accessible on the PC in the shared "vFolder". To save the output from `map -r` back to the PC.

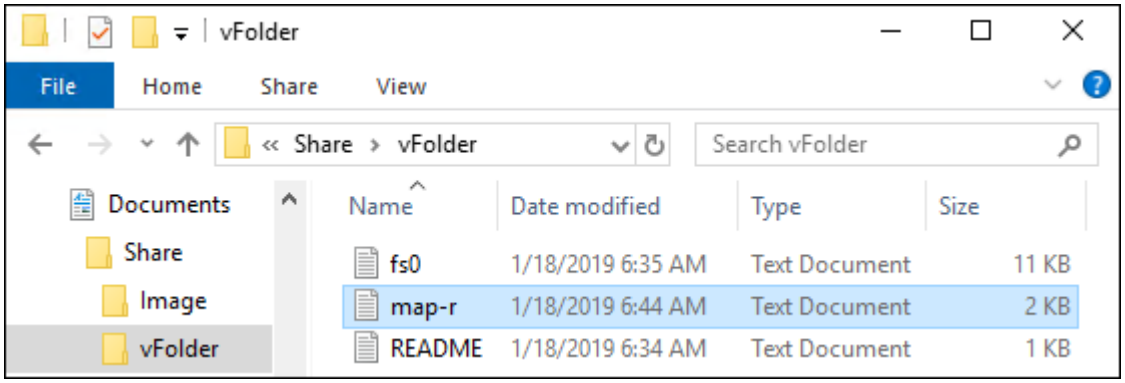
For example:

```
FS0:\> map -r > map-r.txt
FS0:\> dir
Directory of: FS0:\
01/18/2019 06:35             10,660  fs0.txt
01/18/2019 06:34
64  README.txt
07/22/2018 22:52              1,576  map-r.txt
          3 File(s)     12,300 bytes
                                    0 Dir(s)
```

11. In the Virtual Media application on the PC, click **Disconnect**.

12. In the **Synchronize to Disk** warning dialog, click **Yes** to synchronize the disk image file back to the vFolder on the PC.

When synchronization is complete, the changes made on the server are now visible under the vFolder.



3. (Optional) You can disconnect and reconnect as needed. Whenever the Virtual Media connection state changes, the devices on the server must be rescanned using the `reconnect -r` command.

```
FS0:\> reconnect -r
FS0:\> map -r
```

More information

Running JViewer from a privileged account

Configuring a hard disk as virtual media

Prerequisites

You are logged in as an administrator. See Logging on to the RMC with a browser.

About this task

A physical hard disk containing FAT or FAT32 partitions can be mounted as virtual media for UEFI.

Procedure

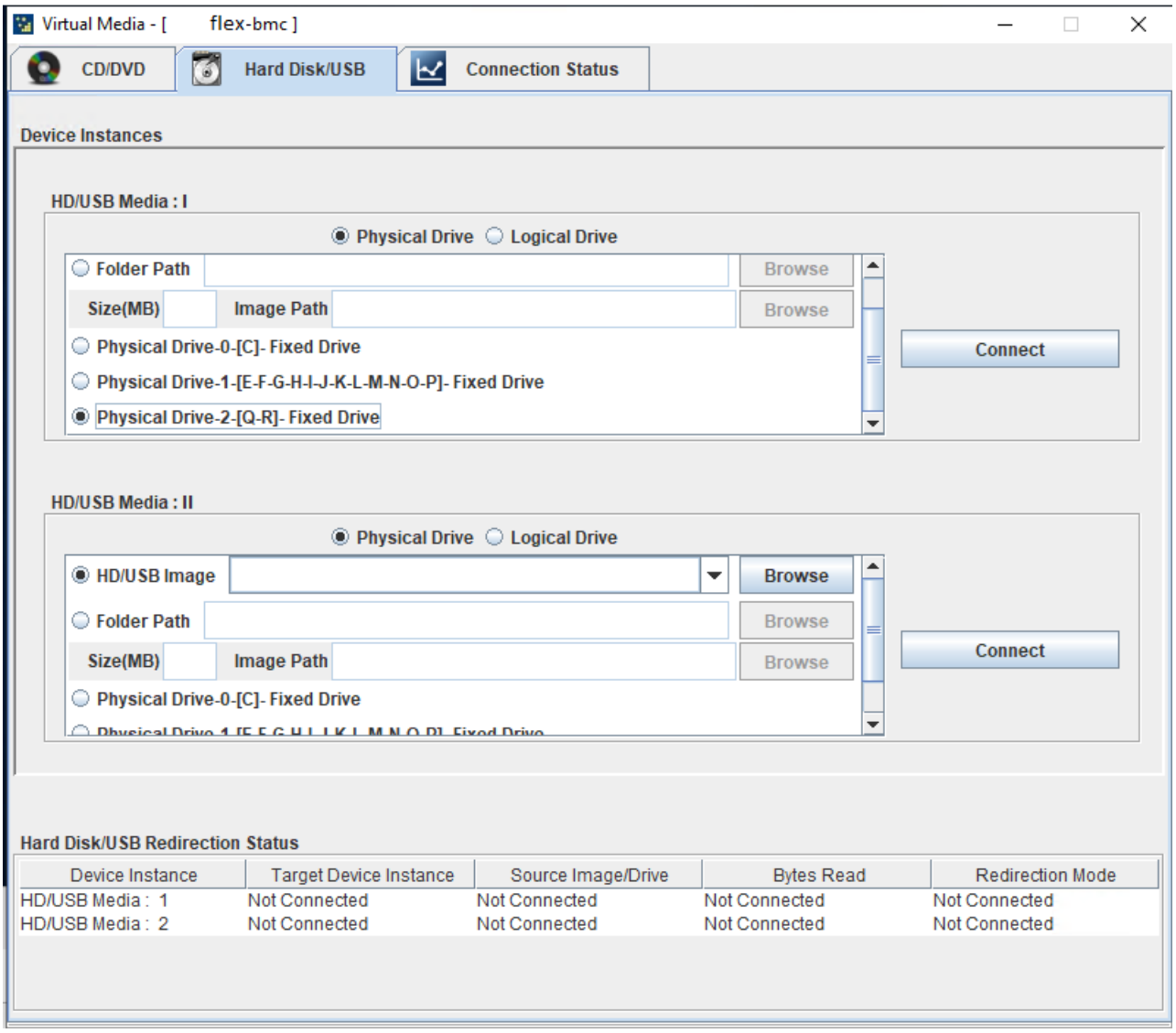
1. Run the download `jviewer-sa.jar`.

```
java -jar jviewer-sa.jar [-hostname
                    BMC_HOSTNAME] [-u
                    USERNAME] [-p
                    PASSWORD]
```

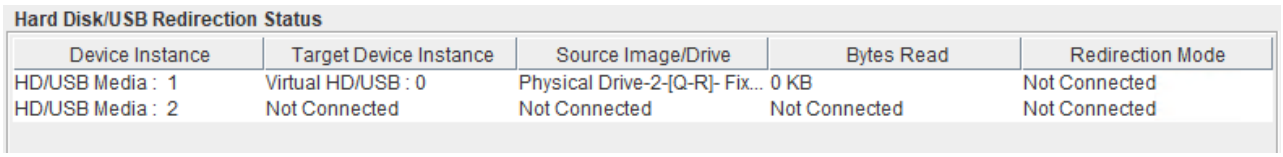
   The Virtual Media GUI opens.

2. On the **Hard Disk/USB** tab, scroll through the list of physical drives and select the drive you want to mount as Virtual Media.

In this example, the `Physical-Drive-2-[Q-R]-Fixed Drive` is selected. This drive has two logical partitions, drive Q and drive R. Both partitions are configured as FAT32 so that they are accessible as Virtual Media.



3. Click **Connect** beside the drive you selected.



The **Hard Disk/USB Redirection Status** panel at the bottom of the window is updated.

4. If the server is not powered on, power it on from the RMC.

```
power on npar pnum=0 bootopt=Shell
```

`bootopt=Shell` forces the console to stop at the UEFI Shell prompt.

5. Launch the KVM for console access.

   After power-up, the system will boot to the UEFI Shell, where the Virtual Media is accessible from USB file system devices.

6. To view these devices:

   a. From the UEFI Shell, issue a `map -r` command.

   b. Search for newly created file system (FS) devices that are designated with **USB**.

   c. If the devices are not visible, reboot the system.

   In the following example, there are two new devices, FS0 and FS1, both with the USB designator. These devices did not exist prior to mounting the Virtual Media. Each device corresponds to a FAT or FAT32 logical partition from the machine running `Jviewer-sa.jar`. There are two FAT32 logical partitions, so two FS devices are created.

```
Shell> map -r
Mapping table

     FS0: Alias(s):HD0m0c0a2:;BLK2:
          PciRoot(0x0)/Pci(0x14,0x0)/USB(0xC,Ox0)/USB(0x2,0x0)/
Unit(0x0)/HD(2,GPT,748A7DAF-EB0E-42DA-824A-5B3FF51810F4,0x8000,
0x800000)
     FS1: Alias(s):HD0m0c0a3:;BLK3:
          PciRoot(0x0)/Pci(0x14,0x0)/USB(0xC,0x0)/USB(0x2,0x0)/
Unit(0x0)/HD(3,GPT,88D9175B-0EBC-46AE-9654-0007781192B0,0x808000,
0x800000)
```

7. Identify each logical partition.

   To determine which logical partition is mounted to each FS file system, it will be necessary to uniquely identify the partition.

   a. Create a uniquely named file on each logical partition before mounting the Virtual Media.

      In this case, on logical drive Q, a folder named `Drive Q - FAT32`, and on drive R a folder named `Drive R - FAT32` was created. These files were arbitrarily created only to help identify which drive is mapped to which FS file system.

```
FS1:\> fs0:
FS0:\> dir
Directory of: FS0:\
01/18/2019  01:42 <DIR>         4,096  Drive Q - FAT32
          0 File(s)           0 bytes
          1 Dir(s)
```

```
FS0:\> fs1:
FS1:\> dir
Directory of: FS1:\
01/18/2019  04:19 <DIR>         4,096  Drive R - FAT32
          0 File(s)           0 bytes
          1 Dir(s)
```

b. While the physical drive is connected, the logical partitions mounted as Virtual Media are not accessible from the machine running `JViewer-sa.jar`. To access the logical drives locally, you must first exit `JViewer-sa.jar`.

Results

You now have read and write access to the Virtual Media.

More information

Running JViewer from a privileged account

RMC accounts and passwords

HPE Superdome Flex Server user accounts are managed by a system administrator using the RMC/eRMC CLI or the Redfish interface. These user accounts can be used to authenticate at all Superdome Flex Server interfaces such as RMC/BMC CLIs, Redfish, web GUI, and JViewer.

Password requirements

- Passwords may include combinations of these types of characters:
  - Upper case letters
  - Lower case letters
  - Numbers
  - Special characters - including `!@#$%^&*()!@`
- Password length is dependent on the types of characters used. The minimum length is eight characters, with the minimum length increased by two characters for each type not included.
  - Passwords only containing one type of character must be at least 14 characters.
  - Passwords containing two types of character must be at least 12 characters.
  - Passwords containing three types of character must be at least 10 characters.

- Passwords containing all four types of characters must be at least 8 characters.

Dot character in LDAP names

The dot (.) character is a valid character in user and group names. However, the Superdome Flex Rack Management Controller (RMC)/Embedded Rack Management Controller (eRMC) Command Line Interface (CLI) disallows the dot (.) in user and group names. As a result, LDAP group names with a dot (.) cannot be used by the Superdome Flex RMC/eRMC commands.

The following is an example of an error reported by the RMC when a dot (.) is used in an LDAP group name:

```
RMC> add ldap_group name=UNIX.SUPPORT.GG

Usage: add ldap_group name=GROUP_NAME role={administrator, custom_cli,
monitor, operator}

ERROR: argument name: Group name is not valid. Group name must
begin with a letter. Acceptable characters include alphanumeric,
dash, and underscore.
```

White spaces in LDAP names

Configuration syntax for LDAP groups cannot contain white space. If you would like to force white space, use "\20" instead. For example:

```
set ldap groupdn="ou=IT",ou=Service\20Groups,dc=customer,dc=ab"
```

User roles

User accounts are divided into three roles or privilege levels, assigned when new users are added.

Monitor

Can perform minimal operations such as view current settings, logs, and system health.

Operator

Can perform all Monitor functions plus create, modify, delete, and power on/off partitions.

Administrator

Can perform all functions including configure network settings, enable/disable network services, generate certificates, and create or remove user accounts.

custom_cli

Can access only npar console.

Passwords

Passwords are assigned when new users are added and may be changed by the user at any time.

The administrator initial default password is changed by the administrator once the new system is installed and configured.

Subtopics

LDAP user authentication
User account management with the RMC CLI

More information

User account management with the RMC CLI

LDAP user authentication

Lightweight Directory Access Protocol, or LDAP, is a protocol for authentication, retrieval, and maintenance of directory information. HPE Superdome Flex Server can be configured to authenticate users over LDAP.

> **NOTE**
> The server only supports LDAPS (Lightweight Directory Access Protocol over Secure Socket Links) connections to the LDAP server.

For more information and examples about using RMC LDAP commands, see the **HPE Superdome Flex Server Administration Guide**.

Subtopics

LDAP configuration
Adding new LDAP groups
Modifying LDAP groups
Removing LDAP groups and LDAP group filters
Displaying the current LDAP groups
Enabling LDAP authorization on the RMC
Disabling LDAP authorization on the RMC
Validating the LDAP configuration

LDAP configuration

LDAP configuration is managed using the CLI on the RMC. Successfully configuring the HPE Superdome Flex Server for LDAP authentication requires providing the LDAP server details, associating group entries on the LDAP server with user roles, and enabling LDAP on the RMC. Any LDAP user account which is a member of an authorized group will be able to log into the RMC with the specified group role.

```
RMC cli> apropos ldap

add ldap_group name=GROUP_NAME
role={administrator,custom_cli,monitor,operator}
clear ldap [server] [port] [login] [binddn] [bindpw] [sid] [basedn]
[userfilter] [userdn] [groupfilter] [groupdn]
disable ldap
enable ldap
modify ldap_group name=GROUP_NAME
role={administrator,custom_cli,monitor,operator}
remove ldap_group name=GROUP_NAME
remove ldap_user_data
set ldap [server=SERVER] [port=SSL_PORT] [login=LOGIN_ATTRIBUTE]
[binddn=BIND_DN] [bindpw] [sid=AD_DOMAIN_SID] [basedn=BASE_DN]
[userfilter=USER_FILTER]
[userdn=USER_DN] [groupfilter=GROUP_FILTER] [groupdn=GROUP_DN]
[connection={ldap,ldaps}]
show ldap
show ldap_group
test ldap [username=USERNAME] [verbose]
```

Subtopics

Configuring LDAP server details
Clearing LDAP settings
Displaying the current LDAP settings

More information

Configuring LDAP server details
Clearing LDAP settings
Displaying the current LDAP settings

Configuring LDAP server details

Procedure

Configure the LDAP server details by using the `set ldap` command.

Example minimal configuration:

```
set ldap server=dir_server.company.com basedn="dc=company,dc=com"
```

Example with additional search settings for user and group:

```
set ldap server=dir_server.company.com port=636 login=uid
    set ldap basedn="ou=org,dc=company,dc=com"
    set ldap userdn="ou=devs,ou=org,dc=company,dc=com"
userdn="ou=test,ou=org,dc=company,dc=com"
    set ldap userfilter="objectClass=posixAccount"
    set ldap groupdn="ou=groups,ou=org,dc=company,dc=com"
    set ldap groupfilter="objectClass=posixGroup"
```

Example for an Active Directory server:

```
set ldap server=dir_server.company.com login=sAMAccountName
    set ldap basedn="dc=company,dc=com"
    set ldap userfilter="(&(objectClass=user)(!(objectClass=computer))"
    set ldap groupfilter="objectClass=group"
    set ldap sid=S-1-5-21-3623811015-3361044348-30300820
```

Example for server that requires a bind name and password:

```
Set bindpw to be prompted for a bind password (if not in script mode)
    set ldap server=dir_server.company.com port=636 login=uid
    set ldap basedn="dc=company,dc=com" binddn="cn=admin,dc=company,dc=com"
    set ldap bindpw
     Please enter the bind password: _
```

Subtopics

Set LDAP command information

More information

Set LDAP command information

Set LDAP command information

The `set LDAP` command is used from the RMC command line to configure the LDAP server details.

```
Usage: set ldap [server=SERVER] [port=SSL_PORT] [login=LOGIN_ATTRIBUTE]
[binddn=BIND_DN] [bindpw] [sid=AD_DOMAIN_SID] [basedn=BASE_DN]
[userfilter=USER_FILTER] [userdn=USER_DN] [groupfilter=GROUP_FILTER]
[groupdn=GROUP_DN] [connection={ldap,ldaps}]
```

The `server` and `basedn` must be provided. The `port`, `login`, `userfilter`, and `groupfilter` default to the values **636**, **uid**, **(objectClass=posixAccount)**, and **(objectClass=posixGroup)** respectively. These values may be changed as required. The other details are optional and are used to further refine the LDAP searches of the directory information.

The `set ldap` command has many examples in its help output. See `help set ldap` for more information.

```
RMC cli> help set ldap

Set LDAP configuration.
Note: Strings containing equal signs or spaces must be quoted.

If configuring LDAP for Active Directory, you will need to set the login,
userfilter, and groupfilter parameters because the default values of "uid",
"objectClass=posixAccount", and "objectClass=posixGroup" are insufficient.
If the user entries on the AD server do not contain uidNumber and gidNumber
attributes, you may use the objectSID attribute by setting sid to the
domain value of the server.  See the Active Directory example below.
```

Review the output of the `help set ldap` command for examples of using this command.

Example minimal configuration:

```
RMC cli> set ldap server=dir_server.company.com basedn="dc=company,dc=com"
```

Example with additional search settings for user and group:

```
RMC cli> set ldap server=dir_server.company.com port=636 login=uid
    set ldap basedn="ou=org,dc=company,dc=com"
    set ldap userdn="ou=devs,ou=org,dc=company,dc=com"
userdn="ou=test,ou=org,dc=company,dc=com"
    set ldap userfilter="objectClass=posixAccount"
    set ldap groupdn="ou=groups,ou=org,dc=company,dc=com"
    set ldap groupfilter="objectClass=posixGroup"
```

Example for an Active Directory server:

```
RMC cli> set ldap server=dir_server.company.com login=sAMAccountName
    set ldap basedn="dc=company,dc=com"
    set ldap userfilter="(&(objectClass=user)(!(objectClass=computer))"
    set ldap groupfilter="objectClass=group"
    set ldap sid=S-1-5-21-3623811015-3361044348-30300820
```

Example for server that requires a bind name and password:

```
RMC cli> Set bindpw to be prompted for a bind password (if not in script
mode)
    set ldap server=dir_server.company.com port=636 login=uid
    set ldap basedn="dc=company,dc=com" binddn="cn=admin,dc=company,dc=com"
    set ldap bindpw
     Please enter the bind password: _
```

Example for changing connection type `- LDAP` or `LDAPS`:

```
Use "ldap://" for secure communication with LDAP server.
set ldap connection=ldap

Use "ldaps://" for secure communication with LDAP server.
set ldap connection=ldaps
```

Default values if not set:

```
port        = 636
login       = uid
userfilter  = "(objectClass=posixAccount)"
groupfilter = "(objectClass=posixGroup)"
```

The login parameter is the name of the LDAP attribute that contains the unique identifier of the LDAP entry which will be used as the username.

There are two supported ways of establishing group membership in an LDAP group entry; either by a **memberUid** or a **member** attribute.

- The **memberUid** attribute contains a username which is used to search for the corresponding LDAP user entry.
- The **member** attribute contains LDAP DNs which identify a user or nested group.

If group membership is provided by the **memberUid** attributes, the value of a **memberUid** must match the value of the login parameter; for example, the username must be added as a **memberUid** of a group entry. If **member** attributes are used, then user entries are fully identified by the DN values without regard for the username.



NOTE

The space character for the DN string can be included by replacing space with `\20` (for example. backslash followed by the digits two and zero). In the following example, DN with OU customer service org is represented as `customer\20service\20org`.

Ldap names with space are supported from FW 3.40.126. Strings containing space must be enclosed with quotes.

```
set ldap
groupdn="ou=groups,ou=customer\20service\20org,dc=compan
y,dc=com"
add ldap_group name="group name" role=monitor
set ldap groupdn='ou=”abc def”,dc=abc,dc=local'
set ldap basedn='dc=”abc lab”,dc=local'
test ldap username=”user name”
```

More information

Configuring LDAP server details

Clearing LDAP settings

Procedure

Remove or reset LDAP settings by using the `clear ldap` command.

```
RMC cli> clear ldap sid

Updating LDAP configuration and restarting service if necessary...
```

Displaying the current LDAP settings

Procedure

Display the current LDAP settings by using the `show ldap` command.

```
RMC cli> show ldap

Enabled: True

Server: dir_server.company.com
Port: 636

Bind DN:
Bind Password:

Login Attribute: uid
Base DN Search 1: ou=org,dc=company,dc=com

User Filter: (objectClass=posixAccount)
User DN Search 1:

Group Filter: (objectClass=posixGroup)
Group DN Search 1:

AD Domain SID:

Connection : ldaps
```

Adding new LDAP groups

Procedure

Grant users of an existing LDAP group access and privileges to the RMC by using the `add ldap_group` command.

```
RMC cli> add ldap_group name=HPE_Superdome_Flex_users role=operator

Updating LDAP configuration and restarting service if necessary...
Added LDAP group: HPE_Superdome_Flex_users
```

Modifying LDAP groups

Procedure

Change the privilege level for an LDAP group by using the `modify ldap_group` command.

```
RMC cli> modify ldap_group name=HPE_Superdome_Flex_users
role=administrator

Updating LDAP configuration and restarting service if necessary...
Updated LDAP group: HPE_Superdome_Flex_users
```

Removing LDAP groups and LDAP group filters

Procedure

1. To remove an LDAP group and revoke access by members of the group, use the `remove ldap_group` command.

   ```
   RMC cli> remove ldap_group name=HPE_Superdome_Flex_users

   Updating LDAP configuration and restarting service if necessary...
   Removed LDAP group: HPE_Superdome_Flex_users
   ```

2. To clear ldap group filter use the `clear ldap groupfilter` command.

   ```
   RMC:r001u01c cli> help clear ldap

   Clear LDAP configuration attributes.
   ```

```
Example to clear user and group filters:

        clear ldap userfilter groupfilter

Example to clear all:

        clear ldap

Usage: clear ldap [server] [port] [login] [binddn] [bindpw] [sid]
[basedn] [userfilter] [userdn] [groupfilter] [groupdn] [connection]
[tls_cert]

RMC:r001u01c cli>
```

Displaying the current LDAP groups

Procedure

Display the current list of authorized LDAP groups by using the `show ldap_group` command.

```
RMC cli> show ldap_group

 Group Name   Role
 -----------  --------------
 Users        operator
```

Enabling LDAP authorization on the RMC

Prerequisites

- The server details are set
- The LDAP groups are defined

Procedure

Enable LDAP authorization on the RMC by using the `enable ldap` command.

```
RMC cli> enable ldap

Updating LDAP configuration and restarting service if necessary...
LDAP is enabled
```

Disabling LDAP authorization on the RMC

Procedure

Disable LDAP authorization on the RMC by using the `disable ldap` command.

```
RMC cli> disable ldap

Updating LDAP configuration and restarting service if necessary...
LDAP is disabled
```

Validating the LDAP configuration

About this task

You can run a test to verify the following:

- LDAP is enabled on the RMC
- The RMC can communicate with the LDAP server
- All defined groups exist in the LDAP server database
- A user (if provided) exists and is a ember of an authorized LDAP group

Procedure

Validate the LDAP configuration by using the `test ldap` CLI command.

```
RMC cli> test ldap username=user1

Beginning test...

Ping Test
---------

# ping -c2 dir_server.company.com
```

```
# ping6 -c2 dir_server.company.com

Ping Test was successful.
Group Search Test
-----------------

Attempting LDAP search for group1 in ou=org,dc=company,dc=com DN scope...

# LDAPTLS_REQCERT=allow
# ldapsearch -LLL -v -x -l 90 -d 4 -H ldaps://dir_server.company.com:636 -b
"ou=org,dc=company,dc=com" "(&(objectClass=posixGroup)(cn=group1))" cn

Entry for group1 was found.

Group Search Test was successful.
User Search Test
----------------

Attempting LDAP search for user1 in ou=org,dc=company,dc=com DN scope...

# LDAPTLS_REQCERT=allow
# ldapsearch -LLL -v -x -l 90 -d 4 -H ldaps dir_server.company.com:636 -b
"ou=org,dc=company,dc=com" "(&(objectClass=posixAccount)(uid=user1))" uid

Entry for user1 was found.

User Search Test was successful.
LDAP Client Test
----------------

# nslcd --check
NSLCD is running.

# id user1
uid=6105(user1) gid=6105 groups=6105,6109(group1)

Authorized groups: 'group1'
User groups: 'group1'

LDAP Client Test was successful.

Test is complete.
```

User account management with the RMC CLI

You use the CLI on the RMC to manage user accounts on the HPE Superdome Flex Server system. You also use the RMC CLI to add users to or remove users from the system, and to change user roles and passwords.

For more information about RMC commands, see **HPE Superdome Flex Server Administration Guide**.

Subtopics

Logging in to the RMC
Displaying RMC user information
Adding RMC users
Removing RMC users
Changing RMC user passwords
Changing RMC user roles
Resetting the administrator password

Logging in to the RMC

Procedure

1. Open an SSH session and enter the following phrase:

   ```
   ssh administrator@name or ip address of RMC
   ```

   The user is authenticated by an SSH key or password prompt.

   ```
   ssh administrator@flex-rmc
   ...
   administrator@flex-rmc's password: administrator password

   HPE Superdome Flex BMC
   ```

2. At the CLI prompt, enter the appropriate command to manage user accounts.

   ```
   commands
   ```

   Enter **`help`** for a list of available RMC commands.

   ```
   help
   ```

   The `apropos` command is useful for finding related commands. It searches the CLI commands usage strings for matching strings. To find commands related to user accounts:

```
RMC cli> apropos user

add user name=USERNAME role={administrator,custom_cli,monitor,operator}
clear ldap [server] [port] [login] [binddn] [bindpw] [sid] [basedn]
[userfilter] [userdn] [groupfilter] [groupdn]
remove ldap_user_data
remove user name=USERNAME
set ldap [server=SERVER] [port=SSL_PORT] [login=LOGIN_ATTRIBUTE]
[binddn=BIND_DN] [bindpw] [sid=AD_DOMAIN_SID]
[basedn=BASE_DN] [userfilter=USER_FILTER] [userdn=USER_DN]
[groupfilter=GROUP_FILTER] [groupdn=GROUP_DN] [connection={ldap,ldaps}]
set password [username=USERNAME]
show user
show user list
test ldap [username=USERNAME] [verbose]
```

Displaying RMC user information

Procedure

1. List all RMC users using the `show user list` command.

```
RMC cli> show user list

   User Name        Role
   ---------------- ------------
 * administrator    administrator
   John_Doe         operator
   Brenda_Smith     monitor
   Thomas           custom_cli

 * denotes the current user
```

2. View information about the current RMC user using the `show user` command.

```
RMC cli> show user

Current User Information:
     Name: administrator
     Role: administrator
```

Adding RMC users

Procedure

1. Create an RMC user account using the `add user` command.

   ```
   USER ROLE role=
   ```

   For example:

   ```
   RMC cli> add user name=Mary_Albright role=monitor

   Changing password for Mary_Albright
   New password: ***********
   Retype password: ***********
   Password for Mary_Albright changed by sysadmin

   User added.
   ```

2. Verify that new user account has been successfully added:

   ```
   show user list
   ```

Removing RMC users

Procedure

1. Remove RMC users using the `remove user` command.

   ```
   remove user name=USERNAME
   ```

   For example:

   ```
   RMC cli> remove user name=Mary_Albright

   Killing user processes.
   Removing user account.
   Removing user home directory.
   User removed.
   ```

2. Verify that the user account has been removed by using the `show user list` command.

   ```
   show user list
   ```

Changing RMC user passwords

About this task

Users with the `custome_cli` or `monitor` or `operator` roles can change only their password.

Users with the `administrator` role can change any user password.

Procedure

Reset your password or other users' password by using the `set password` command.

To change your own password:

```
RMC cli> set password

Changing password for Mary_Albright
Old password: ***********
New password: ********
Retype password: ********
Password for Mary_Albright changed by Mary_Albright
```

To change another user's password:

```
RMC cli> set password username=Mary_Albright

Changing password for Mary_Albright
New password: ********
Retype password: ********
Password for Mary_Albright changed by sysadmin
```

Changing RMC user roles

Procedure

1. Remove the user account by using the `remove user name` command.

   ```
   remove user name=USERNAME
   ```

   For example:

   ```
   RMC cli> remove user name=Mary_Albright

   Killing user processes.
   Removing user account.
   Removing user home directory.
   User removed.
   ```

2. Create the user account with a new role using the `add user name` command.

   ```
   add user name=USERNAME role=USER ROLE
   ```

   For example:

   ```
   RMC cli> add user name=Mary_Albright role=operator

   Changing password for Mary_Albright
   New password: ***********
   Retype password: ***********
   Password for Mary Albright changed by sysadmin

   User added.
   ```

   The existing user password can be reused or changed to a new password.

3. Verify the user account has been successfully updated to include the new role.

   ```
   show user list
   ```

Resetting the administrator password

About this task

If the password for the default administrator account is lost, it can be reset to the factory default by any user with administrator privileges.

Procedure

1. Use the `set password default` command to reset the administrator default password.

   ```
   RMC cli> set password default

   Setting administrator default password
   Password set successfully
   ```

2. After resetting the administrator password to the factory default, you must immediately change it to a secure password again.

HPE Superdome Flex Server updates

Subtopics

Updating HPE Superdome Flex Server firmware
Updating the operating system
Updating HPE Foundation Software for Linux systems
Updating the I/O firmware and drivers on HPE Superdome Flex Server systems

Updating HPE Superdome Flex Server firmware

About this task

This topic describes how to update HPE Superdome Flex Server firmware using a system firmware bundle. For information about other update methods, see the "Firmware Update" section of the **www.hpe.com/support/superdomeflex-management-whitepaper** white paper.

A list of firmware and software components and versions to install on the server is available in the Superdome Flex release sets at **https://www.hpe.com/support/superdome-flex-release-sets**.

> **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.

Procedure

1. Download the latest firmware for the HPE Superdome Flex Server system, go to the **www.hpe.com/support/superdome-flex-software** page.
2. On the HPE Superdome Flex Server page, select **Type** “ Firmware ” and **Subtype** “System”.
3. Choose one of the following methods from the list:
   - **Manual**: 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 or HPE OneView**: Choose the firmware bundle labeled “HPE Superdome Flex Server Firmware Bundle <version>”.
     - **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 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.

Updating the operating system

It is important that the operating system is maintained to include the latest security updates and patches. Each OS has a unique procedure for enabling automatic or manual updates. Refer to the following for the location of the vendor provided update procedures for your OS.

Red Hat Enterprise Linux

See the Red Hat Enterprise Linux Administrator's Guide at **https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/index**. The update instructions can be found in section 9.7, "Automatically Refreshing Package Database and Downloading Updates with Yum.cron".

SUSE Linux Enterprise Server

See **https://www.suse.com/documentation/sles-12/book_sle_admin/data/cha_onlineupdate_you.html**

Oracle Linux

See **https://www.oracle.com/linux** for information about subscribing to live patches with Kspice.

Oracle VM Server

See **https://www.oracle.com/technetwork/documentation/vm-096300.html** and select **View Library** for your Oracle VM Server version. See the "Upgrading Oracle VM" chapter in the Oracle VM Installation and Upgrade Guide for Release x.x for information about updating Oracle VM Server.

VMware vSphere

See the Running VMware vSphere on HPE Superdome Flex Server white paper at **www.hpe.com/support/superdome-flex-vmware** for information regarding installing and updating VMware. VMware on HPE Superdome Flex Server contains HPE value-add components requiring a custom ISO image to get the latest drivers and HPE components.

Microsoft Windows Server

See the Running Microsoft Windows Server on HPE Superdome Flex Server white paper at **http://www.hpe.com/support/superdome-flex-windows** or Installing and running Microsoft Windows Server 2019 on HPE Superdome Flex Server at **www.hpe.com/support/superdome-flex-windows-2019** for information regarding installing and updating Microsoft Windows Server.

Updating HPE Foundation Software for Linux systems

Procedure

1. Update the HPE Foundation Software on Linux systems.

   For more information, see the **https://www.hpe.com/support/superdome-flex-software**.

2. Narrow your search by selecting `type = Software`. This site includes access to the latest HFS ISO files, Release Notes, and installation or update instructions for all supported Linux operating systems.

> **NOTE**
>
> HFS is also available from the Software Delivery Repository (SDR). The SDR provides an easier to install bits using `yum` or zypper directly on specific packages. To use the SDR, follow the instructions provided at **http://downloads.linux.hpe.com/SDR/project/hpe-foundation/**.

Updating the I/O firmware and drivers on HPE Superdome Flex Server systems

Procedure

1. Update the I/O firmware and drivers on the HPE Superdome Flex Server. The HPE Superdome Flex I/O Service Pack image can be found at the **www.hpe.com/support/superdome-flex-software** page.

2. Select `type = Software` and search for the I/O Service Pack for HPE Superdome Flex Servers Family.

HPE Persistent Memory on HPE Superdome Flex Server

Hewlett Packard Enterprise supports HPE Persistent Memory on HPE Superdome Flex Server with Intel Xeon 62xx and 82xx (Cascade Lake) processors.

For details on supported PMM configurations and related administration and maintenance tasks, see **HPE Persistent Memory Guide for HPE Superdome Flex Server**.

Configuring iSCSI boot

Prerequisites

The chassis must contain a Mellanox 100Gb IB/Eth 841QSFP28 card in the supported boot slot.

Procedure

1. At the UEFI Shell, use the `dh` command to list device details and verify that iSCSI components are present.
2. Enter the UEFI Shell command `exit` to access the boot menu.
3. Select **Device Manager**.
4. Select **iSCSI Configuration**.
5. Enter the **iSCSI Initiator Name**.

   This is the worldwide unique name, in iSCSI Qualified Name (IQN) format.
6. Select **Add an Attempt** to create an iSCSI boot attempt.
7. Select the MAC address of the iSCSI card.
8. (Optional) Select **Attempt Name** and enter the name you want to use for this attempt.
9. Select the **iSCSI Mode** menu item and change the status to **Enabled**.
10. Enter the network information for this attempt.
    a. Select the IP version you want to use under the **Internet Protocol** menu item.
    b. (Optional) Set the number of times to attempt reconnecting under the **Connection Retry Count** menu item.
    c. (Optional) Set the time in seconds to time out the connection under the **Connection Establishing Timeout** menu item.
    d. Enter the network information for the initiator, including the IP address, subnet mask, and gateway.

e. Enter the target network information, including the name, IP address, port, and boot LUN.

f. Select the **Authentication Type** menu item and select **None**, and then select the desired type.

1. Select **Save Changes** to save this attempt and return to the **iSCSI Configuration** menu.
2. Select **Continue** to enter UEFI Shell.
3. At the UEFI Shell, enter the reset command to reboot the system.
4. After the reboot, at the UEFI Shell, use the `dh` command to verify that the iSCSI components have been configured properly.

Secure Boot

HPE Superdome Flex 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.



NOTE

Secure Boot is only supported on systems with firmware versions 2.5.246 or later and HFS versions1.3 or later on Linux systems.

Secure Boot requires signed I/O firmware drivers. Currently all 10/25Gb I/O adapters supported on Superdome Flex Server also support Secure Boot operation. See the Superdome Flex Server **www.hpe.com/support/superdome-flex-quickspecs** for a list of supported i/O adapters.

Subtopics

Secure boot features
Enabling Secure Boot with CLI
Enabling Secure Boot with Boot Manager
Disabling Secure Boot with CLI
Disabling Secure Boot with Boot Manager
Installing or reinstalling default Secure Boot keys
Secure Boot Configuration menu
Custom Secure Boot Options menu
Troubleshooting OS Secure Boot issues

Secure boot features

When secure boot is enabled on Superdome Flex 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, and to newly created Superdome Flex Server partitions.

Many secure boot configuration changes require resetting the partition 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` and `hexedit` commands.

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

Subtopics

Default secure boot keys

Default secure boot keys

The default keys include signatures for supported operating systems.

The Superdome Flex 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
- SUSE Linux Enterprise Secure Boot Signkey
- Microsoft Windows Production PCA 2011
- Microsoft Corporation KEK 2K CA 2023
- Microsoft Option ROM UEFI CA 2023
- Microsoft UEFI CA 2023

- Windows UEFI CA 2023
- VMware ESX40 certificate
- VMware certificate 2017

Enabling Secure Boot with CLI

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. Enter one of the following commands:
   - If there are no nPartitions in the system, enter:

     ```
     create npar pnum=1 chassis=all secure_boot=on
     ```

     NOTE

     `chassis=all` can be replaced by the chassis IDs. Example: `chassis=r001i01b roo1i06b`

   - If an nPartition exists, enter:

     ```
     modify npar pnum=x secure_boot=on
     ```

     NOTE

     The nPartition must be powered OFF before enabling.

3. Verify the Secure Boot enabled state using the `show` command.

   ```
   show npar verbose
   ```

4. Power ON the nPartition.

Enabling Secure Boot with Boot Manager

Procedure

1. Interrupt the boot process and access UEFI.

   Press **F2** to access the UEFI Boot Manager.

2. Access the **Secure Boot Configuration** menu.

   At Boot Manager, select the **Device Manager** menu, then select the **Secure Boot Configuration** menu.

3. 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.

      Use the **Custom Secure Boot Options** menu to manually install keys. Using this option also changes the system to User Mode and enables secure boot.

4. 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

Secure Boot Configuration menu
Custom Secure Boot Options menu
Default secure boot keys

Disabling Secure Boot with CLI

About this task

Secure Boot can be enabled and disabled using RMC commands.

Procedure

To disable Secure Boot:

1. Log in to the RMC CLI.
2. Enter one of the following commands:

- If there are no nPartitions in the system, enter:

```
create npar pnum=1 chassis=all secure_boot=off
```

> **NOTE**
>
> `chassis=all` can be replaced by the chassis IDs. Example: `chassis=r001i01b roo1i06b`

- If an nPartition exists, enter:

```
modify npar pnum=x secure_boot=off
```

> **NOTE**
>
> The nPartition must be powered OFF before enabling.

3. Verify the Secure Boot disabled state using the `show` command.

```
show npar verbose
```

4. Power ON the nPartition.

Disabling Secure Boot with Boot Manager

Procedure

1. Interrupt the boot process and access UEFI.

   Press **F2** to access the UEFI Boot Manager.

2. Access the **Secure Boot Configuration** menu.

   At Boot Manager, select the **Device Manager** menu, then select the **Secure Boot Configuration** menu.

3. Uncheck the **Attempt Secure Boot** option.

4. 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

Secure Boot Configuration menu

Installing or reinstalling default Secure Boot keys

Prerequisites

A system must be in Setup mode (no keys installed) for the **Install Default Keys** option to be available.

If a system has Secure Boot keys installed, delete the PK (platform key) to put the system in Setup mode.

About this task

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

Procedure

1. Interrupt the boot process and access UEFI.

   Press **F2** to access the UEFI Boot Manager.

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 **Install Default Keys** option.

   This option also changes the system to User Mode and enables Secure Boot.

4. 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

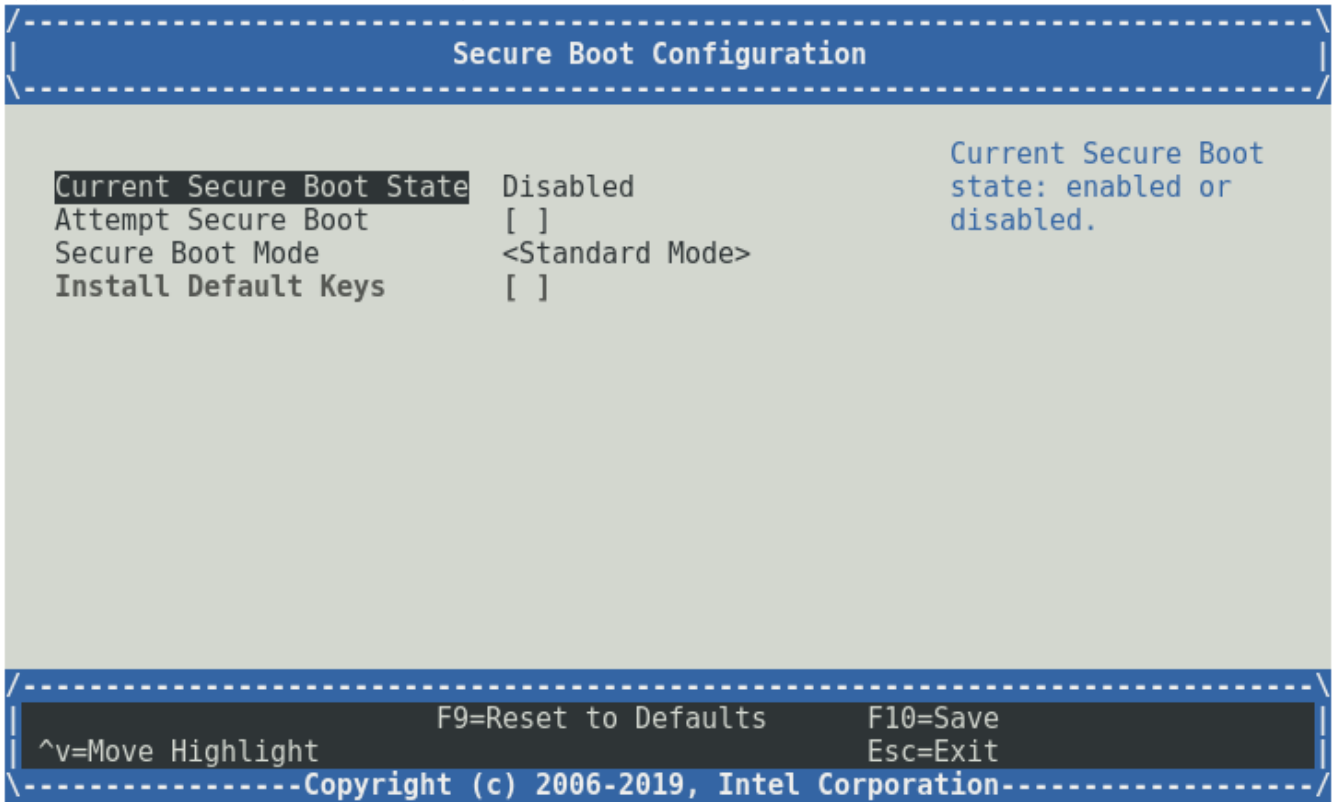
Secure Boot Configuration menu
Default secure boot keys

Secure Boot Configuration menu

You access the **Secure Boot Configuration** menu from UEFI. At Boot Manager select the **Device Manager** menu, then select **Secure Boot Configuration**.

This menu lists current boot settings and manages changes to Secure Boot options.

Figure 1. UEFI Secure Boot Configuration menu



Current Secure Boot State

Secure Boot enablement for the system, either enabled (keys are checked before UEFI execution) or disabled (keys not checked before execution).

Attempt Secure Boot

Option for enforcing Secure Boot. Checked indicates that Secure Boot will be enabled after the next system reset. You must reset the system after changing this option.

Customize Secure Boot

Option for accessing the **Custom Secure Boot Options** menu to manage the boot mode, key registration, and other options.

Custom Secure Boot Options

Manually manage the boot mode, key registration, and other options. This submenu is available only after selecting **Customized** from the **Customize Secure Boot** menu.

Install Default Keys

Option for installing the default secure boot keys. All Secure Boot data is overwritten with a default set for supported operating systems.

Installing the default keys also enables Secure Boot checking.

More information

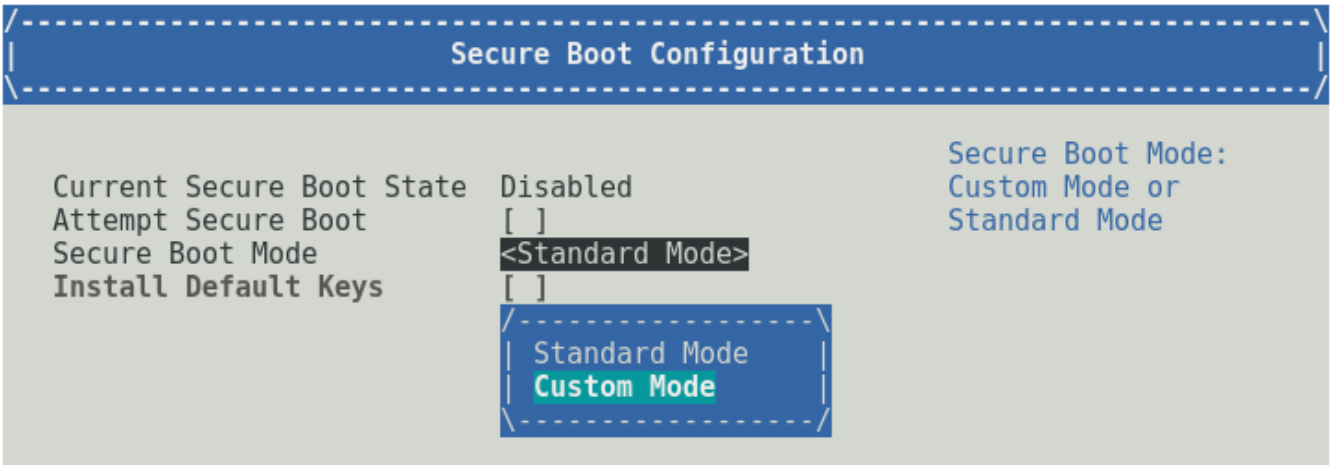
Default secure boot keys

Custom Secure Boot Options menu

To customize UEFI Secure Boot options and keys, use the **Custom Secure Boot Options** menu.

1. Access the **Custom Secure Boot Options** menu from UEFI.
2. At Boot Manager select the **Device Manager** menu, then the **Secure Boot Configuration** menu.
3. At **Customize Secure Boot**, select **Customized**, then select the **Custom Secure Boot Options** submenu.

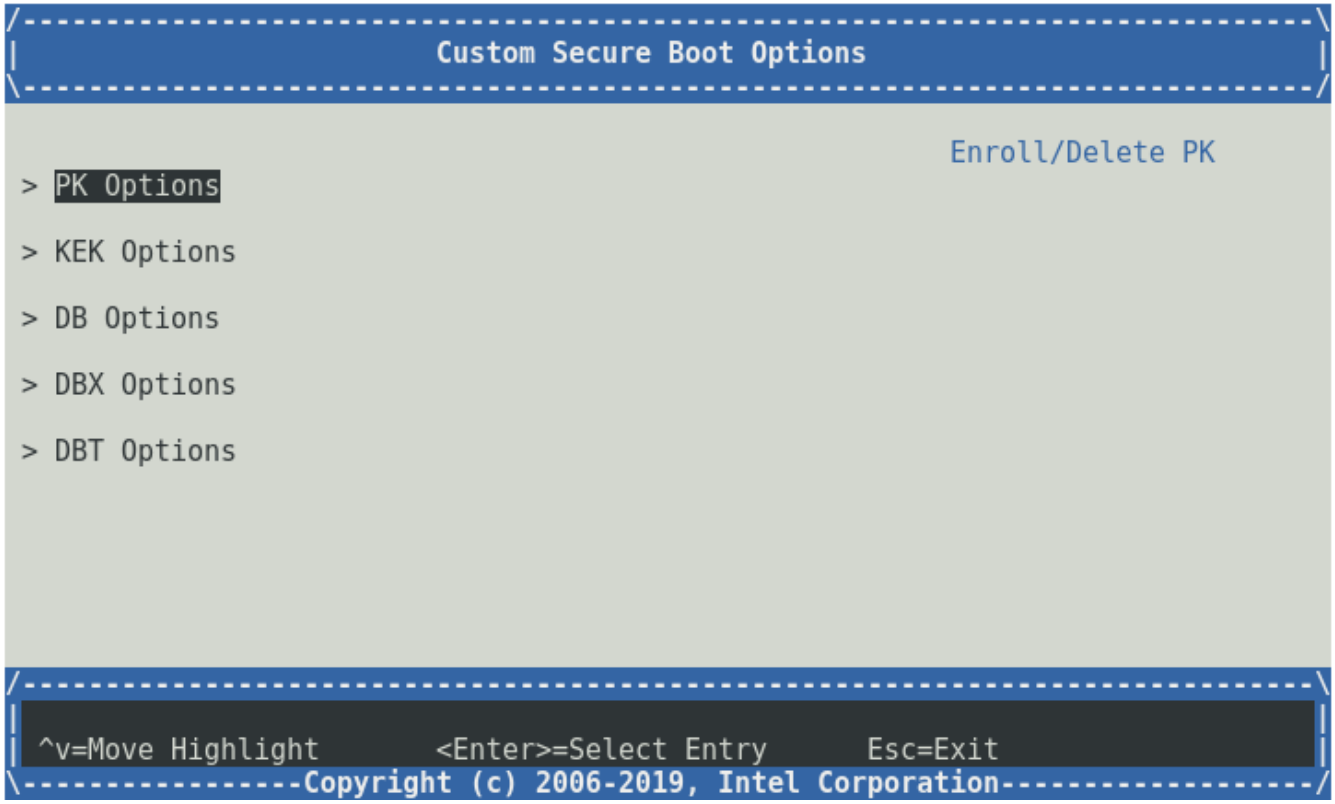
Figure 1. UEFI Customize Secure Boot submenu



Custom Secure Boot options

Custom options for Secure Boot include the mode, key enrollment, and whitelist and blacklist signatures.

Figure 2. UEFI Custom Secure Boot Options menu



The custom Secure Boot key options are:

PK Options

Platform key options.

Only one platform key may be enrolled. To enroll a different platform key, any existing platform key must first be deleted.

You can enroll a platform key using a certificate file (X.509 DER format). The file must be available on a UEFI file system.

KEK Options

Key Exchange Keys options.

You can enroll additional signature keys to establish a trusted relationship between an operating system and the system firmware.

DB Options

Database of allowed signatures (whitelist).

DBX Options

Database of disallowed signatures (blacklist).

DBT Options

Not currently supported.

Troubleshooting OS Secure Boot issues

Subtopics

Cannot enable the Attempt Secure Boot option
OS boot fails from boot manager
OS boot fails with security violation message at UEFI Shell
OS update may fail on Superdome Flex servers running Linux with Secure Boot enabled

Cannot enable the Attempt Secure Boot option

Symptom

The **Attempt Secure Boot** option in the **Secure Boot Configuration** menu cannot be selected.

Solution 1

Cause

The Secure Boot keys have not been installed and the user intends to use the default keys.

Action

Install the default keys. To install the default keys, select the **Install Default Keys** option.

Solution 2

Cause

The Secure Boot keys have not been installed and the user intends to use custom keys.

Action

Enroll custom keys. To enroll custom keys, set the **Customize Secure Boot** option to **Customized** and use the **Custom Secure Boot Options** submenu to enroll custom keys.

More information

Secure Boot Configuration menu
Custom Secure Boot Options menu

OS boot fails from boot manager

Symptom

The OS fails to boot from the boot manager and immediately returns to the boot menu. The progress log contains the `SECURE_BOOT_IMAGE_CHECK_FAILED` message.

Cause

Secure Boot is configured, but the OS does not support Secure Boot.

Action

Disable Secure Boot, or install an OS that supports Secure Boot.

More information

Installing or reinstalling default Secure Boot keys

OS boot fails with security violation message at UEFI Shell

Symptom

The system console displays the `Command Error Status: Security Violation` message, and the firmware does not load the OS. The progress log contains the `SECURE_BOOT_IMAGE_CHECK_FAILED` message.

Cause

Secure Boot is configured, but the OS does not support Secure Boot.

Action

Disable Secure Boot, or install an OS that supports Secure Boot.

More information

Installing or reinstalling default Secure Boot keys

OS update may fail on Superdome Flex servers running Linux with Secure Boot enabled

Symptom

On Superdome Flex servers running firmware version 3.0.512 on a Linux OS with Secure Boot enabled, an OS update may fail while trying to update the Secure Boot keys. The error message includes the text: `Failed to create authenticated variable`.

Action

As a workaround, if using Linux on an HPE Superdome Flex Server with server firmware 3.0.512, do not update the OS while running with Secure Boot enabled.

- To check if Secure Boot is enabled, at the RMC cli enter:

```
RMC cli> show npar verbose
```

- To enable or disable Secure Boot, power off the nPartition and then at the RMC CLI enter:

```
RMC CLI> modify npar pnum=x secure_boot=[on|off]
```

Additional details on Secure Boot can be found in the HPE Superdome Flex Server OS Installation Guide at: **http://www.hpe.com/support/superdome-flex-os**

Websites

HPE Superdome Flex Server websites

HPE Superdome Flex Server product page

www.hpe.com/support/superdome-flex-product

HPE Superdome Flex Server customer documentation

www.hpe.com/support/superdome-flex-docs

HPE Superdome Flex Server software

www.hpe.com/support/superdome-flex-software

HPE Superdome Flex Server Software Delivery Repository

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

Server operating systems and virtualization software

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

HPE Superdome Flex Server QuickSpecs

www.hpe.com/support/superdome-flex-quickspecs

HPE Foundation Software (HFS) and Linux version support matrix

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

HPE Superdome Flex Server spare parts list

www.hpe.com/support/superdome-flex-spareparts

HPE Superdome Flex Server release sets (support matrix)

www.hpe.com/support/superdome-flex-release-sets

HPE Superdome Flex Server support documentation

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

Related product websites

HPE 9361-4i RAID Controller (Q2N11A)

1. Go to the Broadcom MegaRAID SAS 9361-4i product page.

   https://www.broadcom.com/products/storage/raid-controllers/megaraid-sas-9361-4i

2. Select the **Documentation** tab.
3. Under **User Guide** select:
   - 12Gb/s MegaRAID SAS RAID Controllers User Guide
   - 12Gb/s MegaRAID SAS Software User Guide

HPE 3154-8e RAID Controller (Q6M15A)

- **HPE Smart Storage Administrator User Guide**
- Microsemi Adaptec Smart HBA & RAID - Installation And User's Guide
  1. Go to the Microsemi Adaptec SmartRAID 3154-8e product page.

     https://storage.microsemi.com/en-us/support/raid/sas_raid/asr-3154-8e/

  2. Select the **Documentation** tab and download the guide.

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

For additional websites, see Support and other resources.

Support and other resources

Subtopics

Accessing Hewlett Packard Enterprise Support
HPE product registration
Accessing updates
Remote support
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

HPE product registration

To gain the full benefits of the Hewlett Packard Enterprise Support Center and your purchased support services, add your contracts and products to your account on the HPESC.

- When you add your contracts and products, you receive enhanced personalization, workspace alerts, insights through the dashboards, and easier management of your environment.
- You will also receive recommendations and tailored product knowledge to self-solve any issues, as well as streamlined case creation for faster time to resolution when you must create a case.

To learn how to add your contracts and products, see **https://www.hpe.com/info/add-products-contracts**.

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

  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 Account 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 Tech Care Service

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

HPE Complete Care Service

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

Warranty information

To view the warranty information for your product, see the **warranty check tool**.

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, click the **Feedback** button on the page of an opened document on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**). Use this feature to send any errors, suggestions, or comments. This process captures all document information.