



Hewlett Packard
Enterprise

Configuring HPE Superdome Flex 280 Server

Part Number: 10-192002-Q323

Published: June 2023

Edition: 6

Configuring HPE Superdome Flex 280 Server

Abstract

Server configuration, operation, and administration procedures.

Part Number: 10-192002-Q323

Published: June 2023

Edition: 6

© Copyright 2020-2023 Hewlett Packard Enterprise Development LP

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent 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 vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for 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
10-192002-Q323	June 2023	6	<ul style="list-style-type: none">Updated workload profiles and attributes.Added details of <code>BootRetryCount</code> in Setting up boot options and boot retry count using the RMC CLI.
10-192002-Q322	June 2022	5	Added details of MMIOH Granularity in Superdome Flex 280 Server workload profiles and attributes .
10-192002-Q221	April 2021	4	
1012865453-CFG-0121A	January 2021	3	
1012865453-CFG-0121	January 2021	2	<ul style="list-style-type: none">Revise chassis depth detailsUpdate chassis architecture diagrams

Table of contents

- System overview
 - UPI processor interconnections
- Logging in to the RMC
 - Logging in to the RMC UI
 - Logging in to the RMC CLI through the CNSL port (Windows)
 - Logging in to the RMC through the CNSL port (Linux)
 - Zero configuration networking
 - Configuring Superdome Flex 280 Server using Windows
 - Access RMC
 - Using a web browser
 - Logging in to the RMC CLI through an SSH client
 - Configuring Superdome Flex 280 Server using Linux
 - Using the Linux system configured with routable IP address
 - Using the Linux system connected to the Superdome Flex 280 Server
- Default RMC password location
- Setting up the management network from the CLI
- Setting up the management network from the UI
- Setting up users from the CLI
- Setting up users from the UI
- Setting up RMC SNMP alert monitoring
- Configuring nPartition attributes
- Configuring system nPartition attributes from the UI
- Configuring the Custom workload profile
- Setting default nPartition attributes
- Superdome Flex 280 Server workload profiles and attributes
- Configuring memory mirroring
- Setting up boot order with the RMC UI
- Setting up boot options and boot retry count using the RMC CLI
- Setting up boot order with UEFI Boot Manager
- Secure boot
 - Default secure boot keys
 - Configuring Secure Boot on HPE Superdome Flex 280 Server
 - Configuring secure boot from the RMC UI
 - Configuring secure boot from the RMC CLI
 - Configuring Secure Boot with UEFI Boot Manager
 - Installing or reinstalling default Secure Boot keys
- Setting up remote media files with the RMC UI
- Websites
- Support and other resources
 - Accessing Hewlett Packard Enterprise Support

◦ Accessing Hewlett Packard Enterprise support

- Accessing updates
- Remote support
- Customer self repair
- Warranty information
- Regulatory information
- Documentation feedback

System overview

Superdome Flex 280 Server is a 5U rackmounted system that uses in-memory computing technology to enable real-time transactional and analytical processing.

Every Superdome Flex 280 Server has a base chassis providing BaseIO, management interfaces, and boot support. One expansion chassis can be added to expand the system to eight processor sockets. The required base chassis provides platform management through an embedded Rack Management Controller (eRMC).



NOTE: Although the user or reader may encounter both RMC and eRMC terminology in displays and documentation, the preferred term is always RMC.



Key features of Superdome Flex 280 Server

For complete details of the server hardware and configuration options, see [HPE Superdome Flex 280 Server QuickSpecs](#).

Features of HPE Superdome Flex 280 Server include:

- Supports 2, 4, 6, and 8 processor sockets with Intel Xeon 53xx, 63xx, and 83xx (Cooper Lake) processors in a two-chassis system (for example, when populated with 28-cores per processor this provides 224 processor cores in the system)
- Six Ultra Path Interconnect (UPI) links per socket providing unparalleled bandwidth and performance
- 48 DIMM slots per chassis (for example, when populated with 128 GB DIMMs this provides 6 TB of memory per chassis)
- Choice of I/O bays, including either 16 half-height I/O slots, or 8 full-height and 4 half-height I/O slots, per four-socket chassis
- Up to 10 drive bays per chassis
- Two 1GbE NIC ports, four USB ports
- Optional DVD
- Superdome Flex Analysis Engine for better diagnostics and mission-critical reliability

Each Superdome Flex 280 Server chassis may be configured with:

- Two or four Intel Xeon 53xx, 63xx, and 83xx (Cooper Lake) processors
- Up to 48 DDR4 DIMM slots (12 memory slots per processor)
- Up to 16 PCIe Gen 3 slots
- Eight fans
- Two or four power supplies
- BaseIO management, management USB port, and Ethernet ports (base chassis only)

Subtopics

[UPI processor interconnections](#)

UPI processor interconnections

A single-chassis configuration uses only internal UPI cables. Two-chassis configurations are connected with external UPI cables.

Figure 1. Superdome Flex 280 Server single-chassis system architecture

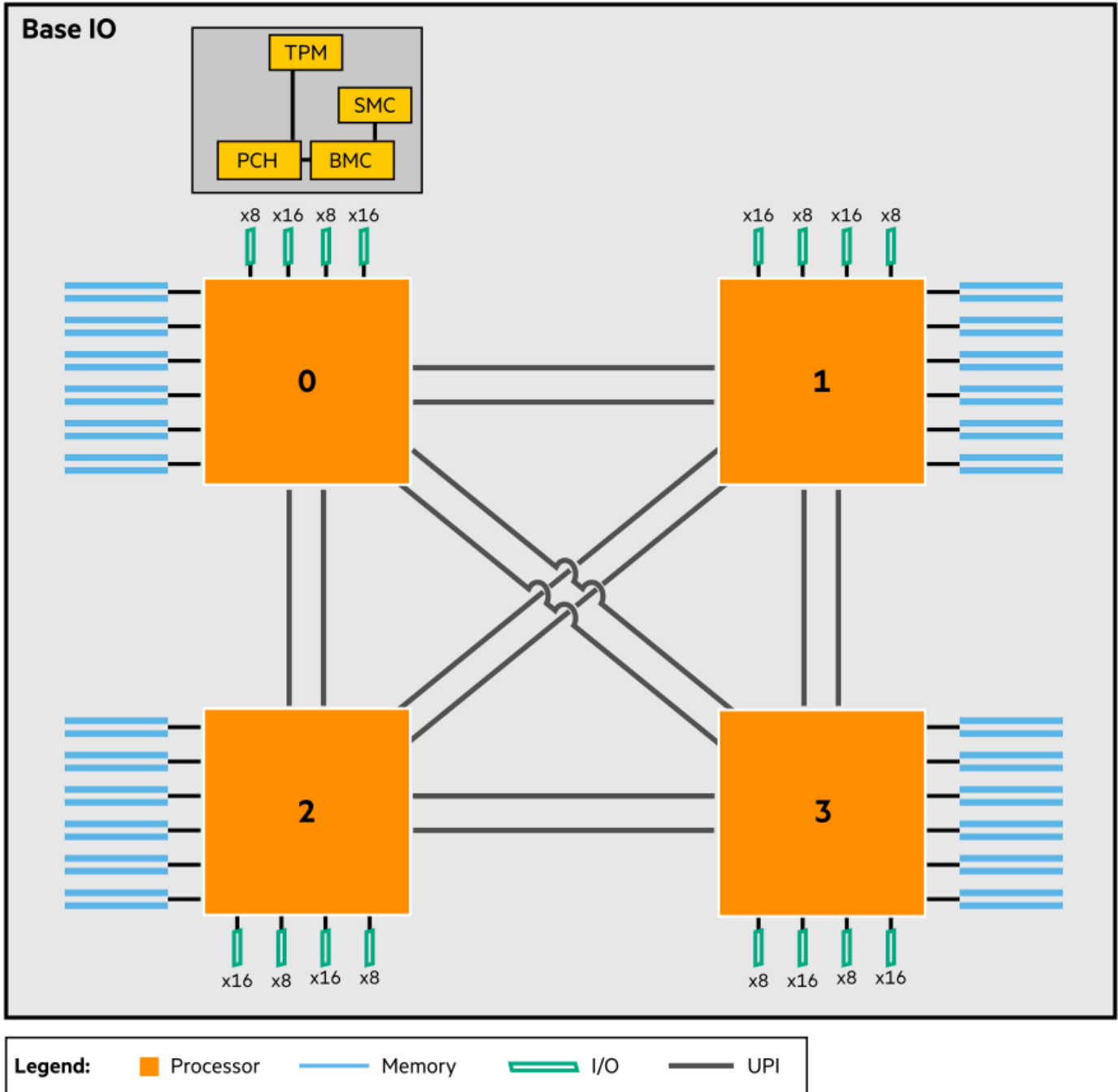
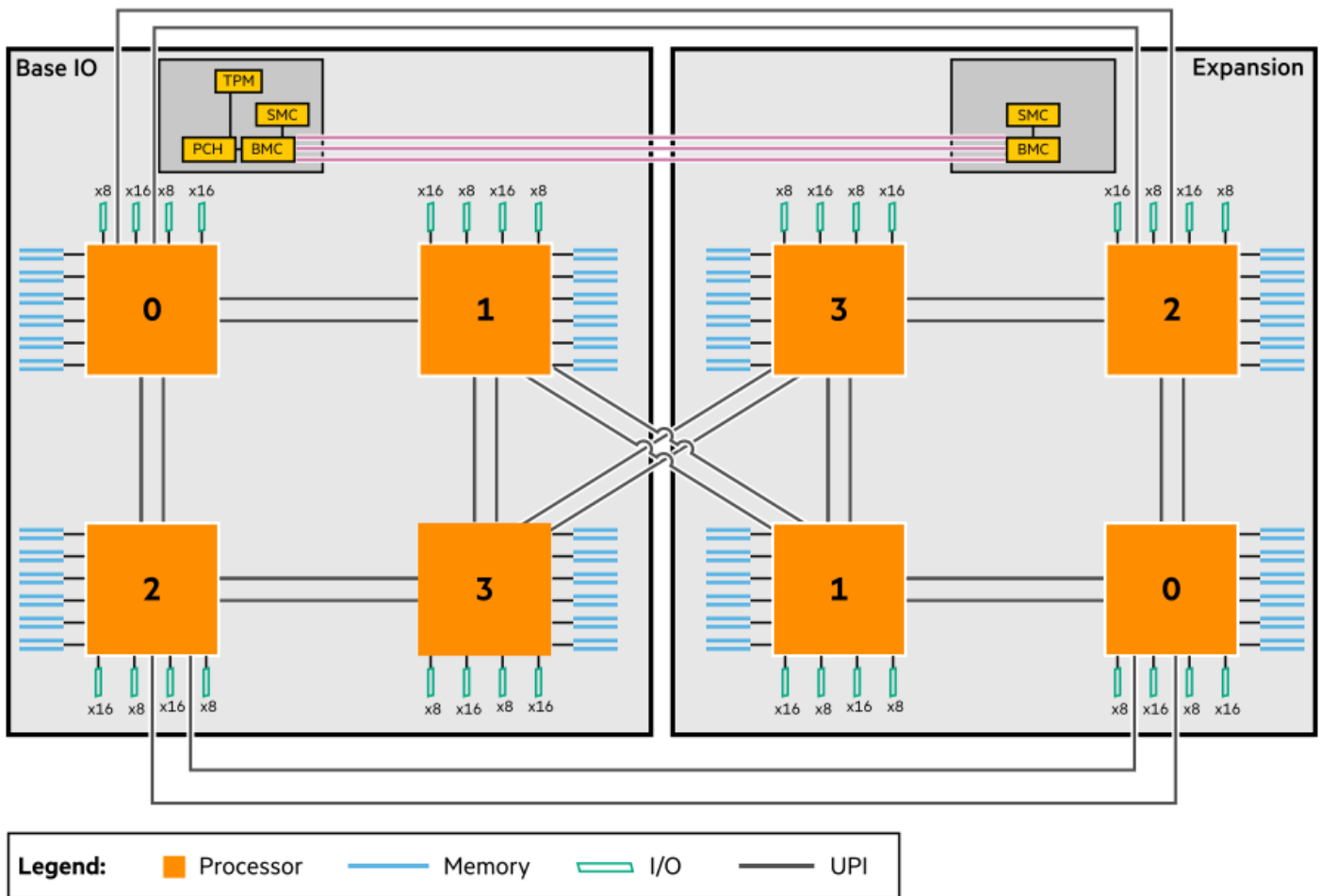


Figure 2. Superdome Flex 280 Server multichassis system architecture





Logging in to the RMC

Subtopics

[Logging in to the RMC UI](#)

[Logging in to the RMC CLI through the CNSL port \(Windows\)](#)

[Logging in to the RMC through the CNSL port \(Linux\)](#)

[Zero configuration networking](#)

Logging in to the RMC UI

Prerequisites

- An ethernet cable must be connected from the base chassis eRMC port to the management network.
- An IP address or hostname must be configured for the eRMC.

About this task

You can access the RMC UI management interface through a web browser. Log into the RMC and perform actions such as configuring nPartition, network, and managing users.

Procedure

1. Use a web browser to access the RMC UI at `https://RMC-IP-ADDRESS`.
2. Log in with the configured RMC user name and password, or with the default RMC user name and password printed on the pull-tab label if the default password has not been changed.

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

Figure 1. RMC UI view

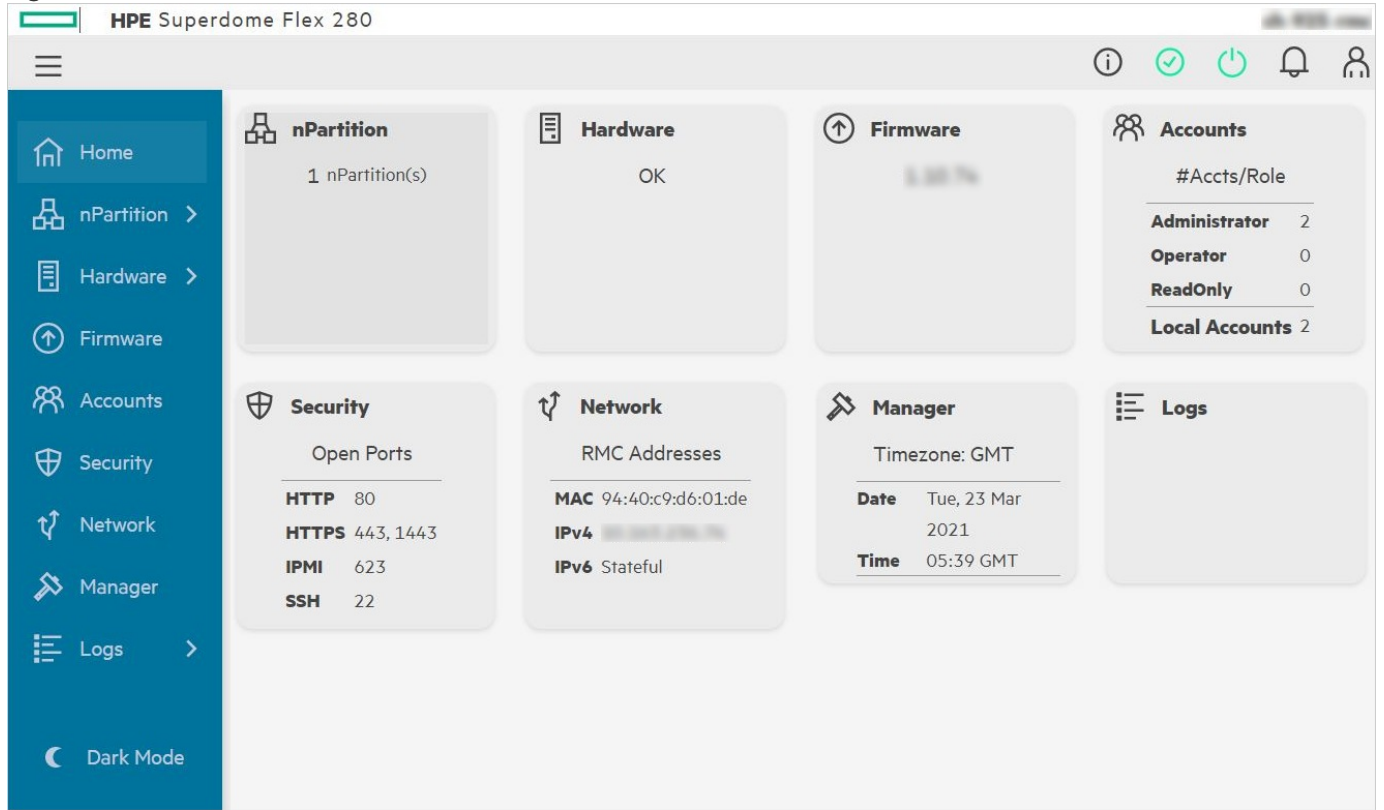
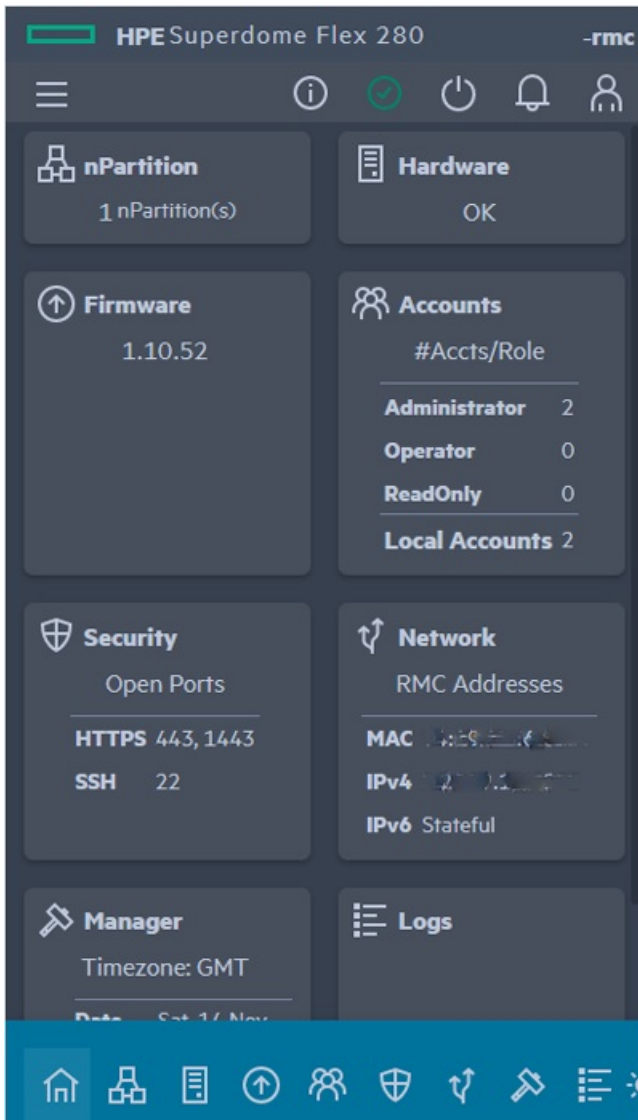


Figure 2. RMC UI phone view





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

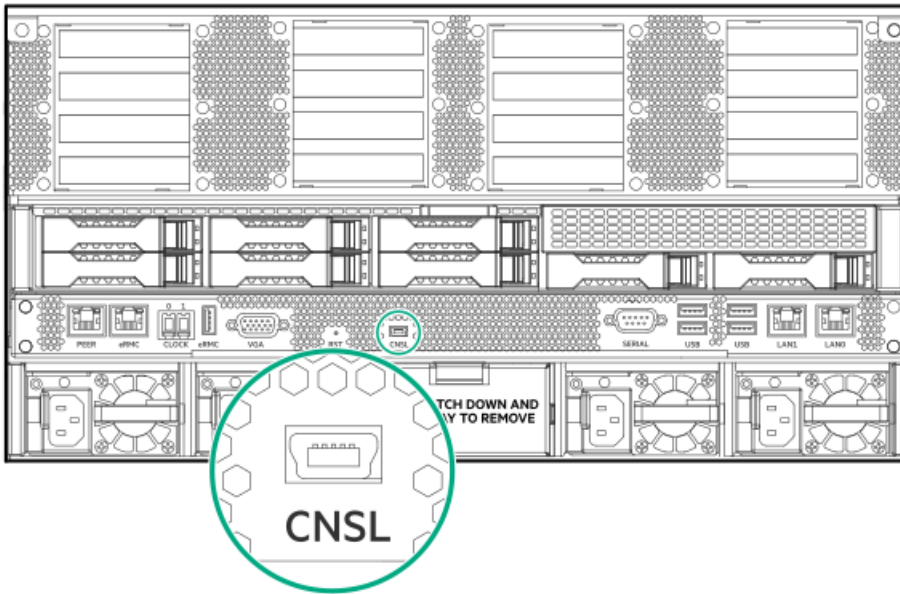
Prerequisites

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

Procedure

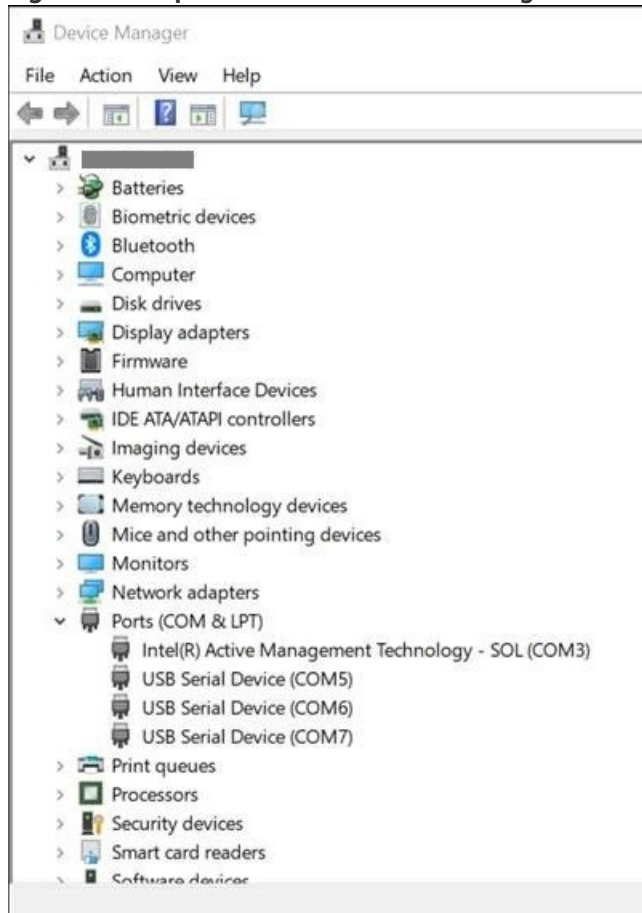
1. Connect a mini-USB cable between the Windows laptop port and the base chassis CNSL port.

Figure 1. CNSL port on chassis rear



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

Figure 2. COM ports in Windows Device Manager



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

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

Three COM ports represent the CNSL port.

- RMC port (CLI)
- SMC port (unused, no customer or service feature)



- Any other port (unused)

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

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

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

```
login as:
USER_NAME

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

End of keyboard-interactive prompts from server

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

=====

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

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

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

=====

example-rmc eRMC:r001u01c cli> help

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

example-rmc eRMC:r001u01c cli>
```



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

Prerequisites

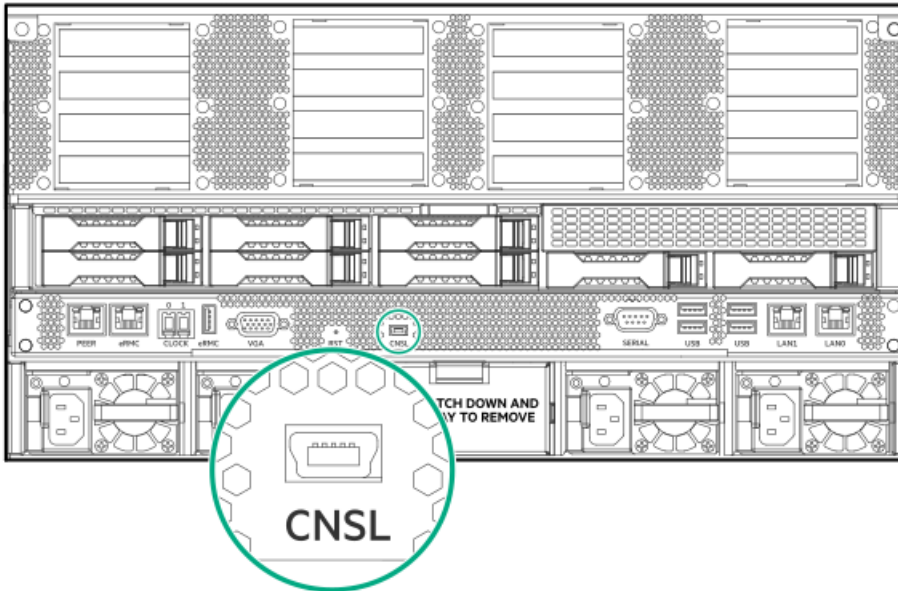
The FT230X device driver must be installed. You can download the device driver and setup instructions from <https://www.ftdichip.com/Drivers/D2XX.htm>. Linux systems might have the FT230X driver installed by default.

Procedure

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

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

Figure 1. CNSL port on chassis rear



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

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

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

3. Press Enter to access the RMC CLI prompt.

Zero configuration networking

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

Subtopics

[Configuring Superdome Flex 280 Server using Windows](#)

[Configuring Superdome Flex 280 Server using Linux](#)

Configuring Superdome Flex 280 Server using Windows

Procedure

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

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

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

Table 1. Browser proxy settings

Google Chrome	Firefox	Microsoft Edge
<p>a. Go to Settings > Advanced > Open your computer's proxy settings</p> <p>The Automatic proxy setup page appears.</p> <p>b. Ensure that the setting of the following options are:</p> <ul style="list-style-type: none">• Automatically detect settings — Off• Use setup script —Off• Use a proxy server — Off	<p>Go to Options > Network Settings >Settings > No proxy</p>	<p>a. Go to Settings > Advanced > Open Proxy Settings> Open Proxy settings</p> <p>The Automatic proxy setup page appears.</p> <p>b. Ensure that the setting of the following options is:</p> <ul style="list-style-type: none">• Automatically detect settings — Off• Use setup script —Off• Use a proxy server — Off

5. Unblock LLLMNR and mDNS ports.

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

Subtopics

Access RMC

Access RMC

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

- Using a web browser

or

- Logging in to the RMC CLI through an SSH client

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

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





Subtopics

[Using a web browser](#)

[Logging in to the RMC CLI through an SSH client](#)

Using a web browser

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

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

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

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

Logging in to the RMC CLI through an SSH client

You can use an SSH client from the Windows PC or laptop to log in to the RMC CLI.

1. SSH to the `RMC<RMC MAC Address>`.
2. Log in with a configured RMC user name and password, or with the default RMC user name and password printed on the pull-tab label if the default password has not been changed.

After the Superdome Flex 280 Server has been configured, access the RMC UI using the new configured standard routable IP address.

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

Configuring Superdome Flex 280 Server using Linux

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

- [Using the Linux system configured with routable IP address](#)
- [Using the Linux system connected to the Superdome Flex 280 Server](#)

Subtopics

[Using the Linux system configured with routable IP address](#)

Using the Linux system configured with routable IP address

About this task

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

Procedure

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

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

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

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

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

or

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

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

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

Using the Linux system connected to the Superdome Flex 280 Server

About this task

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

Procedure

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

Default RMC password location

An information pull-tab with the administrator account credentials and network address details for the Superdome Flex 280 Server RMC is located at the rear of each chassis. To access the Superdome Flex 280 Server RMC, use the details from the pull-tab of the base chassis. The base chassis is located at the lowest U-position in the rack. The default user and password for the RMC administrator account is available on the pull-tab.

Figure 1. Information pull-tab location on chassis rear



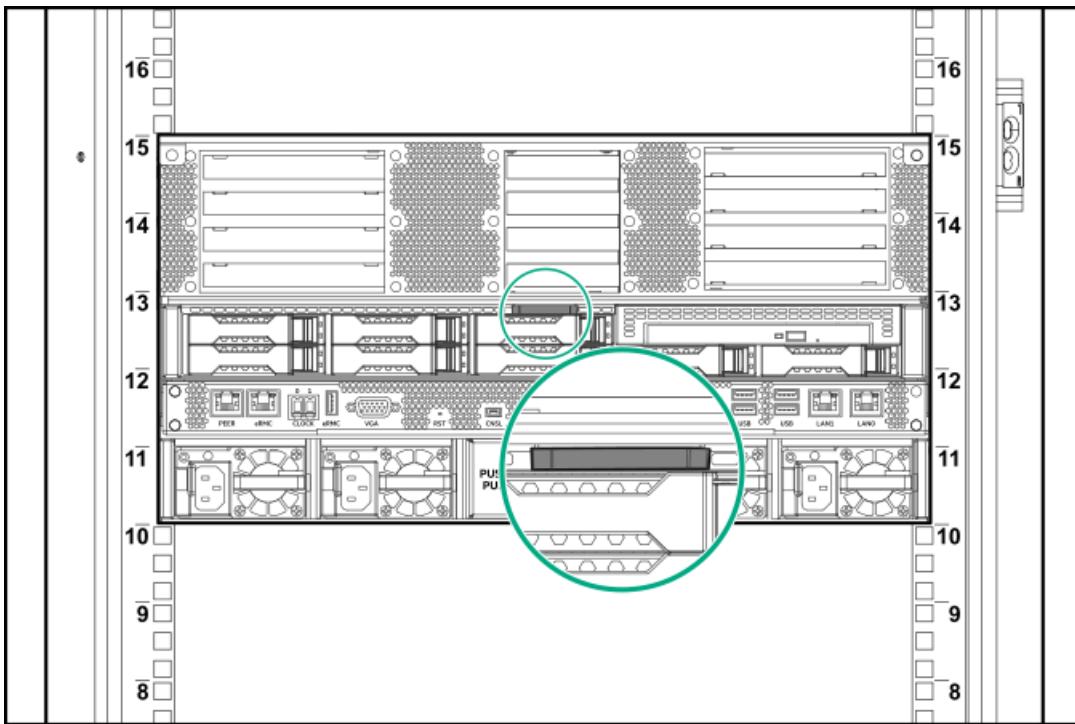
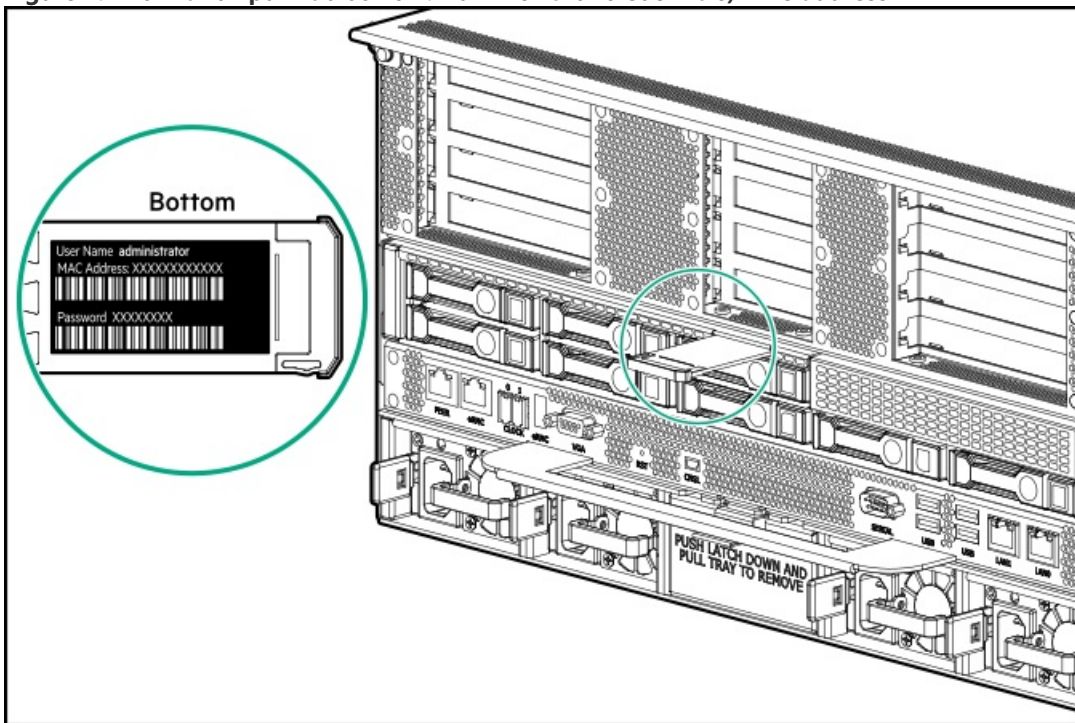


Figure 2. Information pull-tab bottom: Administrator credentials, MAC address



Setting up the management network from the CLI

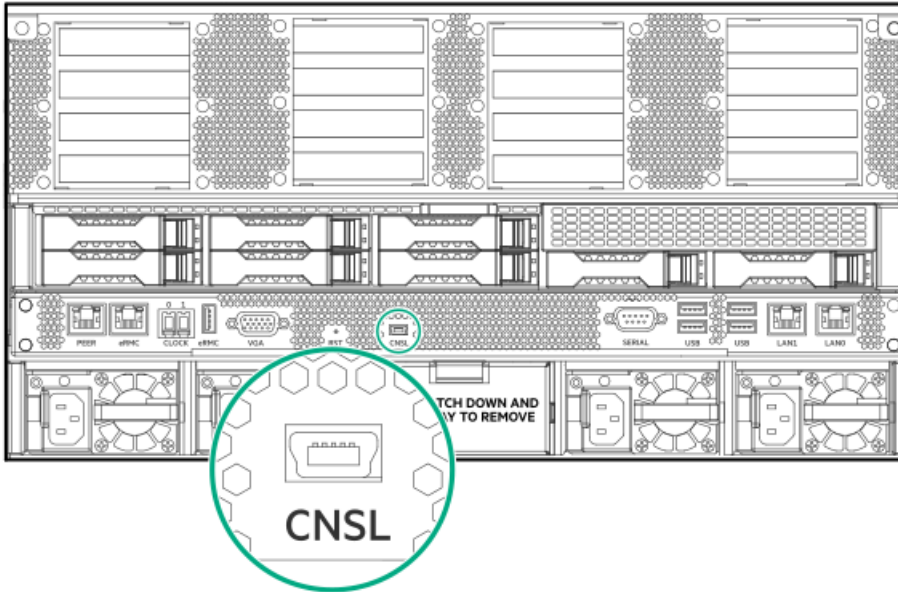
Prerequisites

- Laptop with drivers for direct connection
- USB-A to USB Mini-B adapter cable
- Network configuration details for your management LAN
- RMC administrator account credentials

Procedure

1. Connect to the CNSL port on the back of the base chassis using the USB adapter cable.

Figure 1. CNSL port location



2. Log in to the RMC using the default RMC administrator account.
3. Specify the network settings.

If the network setting method is static, run:

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

If the network setting method is DHCP, run the `set network addressing=dhcp` command.

4. If the RMC participates in name resolution, add DNS name servers and a domain name search list.

```
add dns ipaddress=IPADDRESS1
add dns ipaddress=IPADDRESS2
add dns search=DOMAIN1
add dns search=DOMAIN2
```

5. Specify the NTP server for the Superdome Flex 280 Server.

```
set ntp server=SERVER | FQDN of NTP
```

6. Specify your time zone.

- a. Retrieve the list of time zone specification strings by running the `help set timezone str` command.
- b. Choose a location that is in your time zone and specify your time zone by running the `set timezone str=CODE` command.

```
set timezone str=America/Thunder_Bay
```

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

```
reboot rmc
```

8. To test new IP address and password for the RMC, open another terminal window (on Linux) or use a tool that supports SSH (on Windows) and enter the following command:

```
ssh administrator@NEW_RMC_IP_ADDRESS
```

For Windows, use the supported SSH tool.

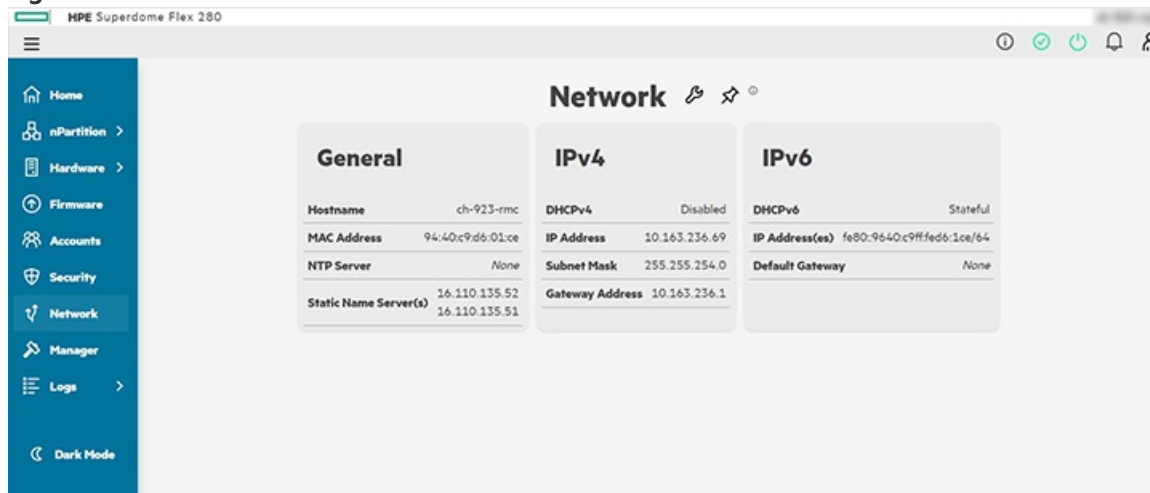
9. To view the NTP server for the Superdome Flex 280 Server, run the `show ntp` command.
10. To view and confirm the DNS configuration, run the `show dns` command.
11. To view the RMC hostname and IP address, run the `show network` command.


Setting up the management network from the UI

Procedure

1. Use a web browser to access the RMC UI at `https://RMC-IP-ADDRESS`.
2. Log in to the RMC UI.
3. Click Network on the main screen or the menu bar on the left.

Figure 1. RMC Network UI



4. Click the  icon next to Network.
5. Enter the required details.
6. To confirm the changes, click Submit.

Setting up users from the CLI

About this task

The Superdome Flex 280 Server RMC can have a maximum of 30 local users, with specified roles that control access to the RMC. If LDAP/AD is configured, there is no limit on LDAP users. User roles must be specified while creating user accounts.

Procedure

1. Log in to the RMC.
2. Run the `add user` command.

```
add user name=USERNAME role={administrator,operator,monitor}
```

The `add user` command has the following specifiers:

name (*USERNAME*)

Specify the name of the user that you want to add to the system.

role

Each role has a different level of privileges and are assigned when creating a user account.

RMC role name	Redfish role name	Privileges
administrator	Administrator	All privileges including ability to create, delete, and edit other user accounts
operator	Operator	Power control, setting a profile, and BIOS parameters
monitor	ReadOnly	Change own password, access read-only JViewer, and access read-only console

3. Enter a password for the user account. The password requirements are as follows:

- 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 six characters, with the minimum length increased by two characters for each type not included. The maximum length is 40 characters.
 - Passwords only containing one type of character must be at least 12 characters.
 - Passwords containing two types of character must be at least 10 characters.
 - Passwords containing three types of character must be at least eight characters.
 - Passwords containing all four types of characters must be at least six characters.

The user is added.

4. (Optional) To verify the user list, run `show user list` command.

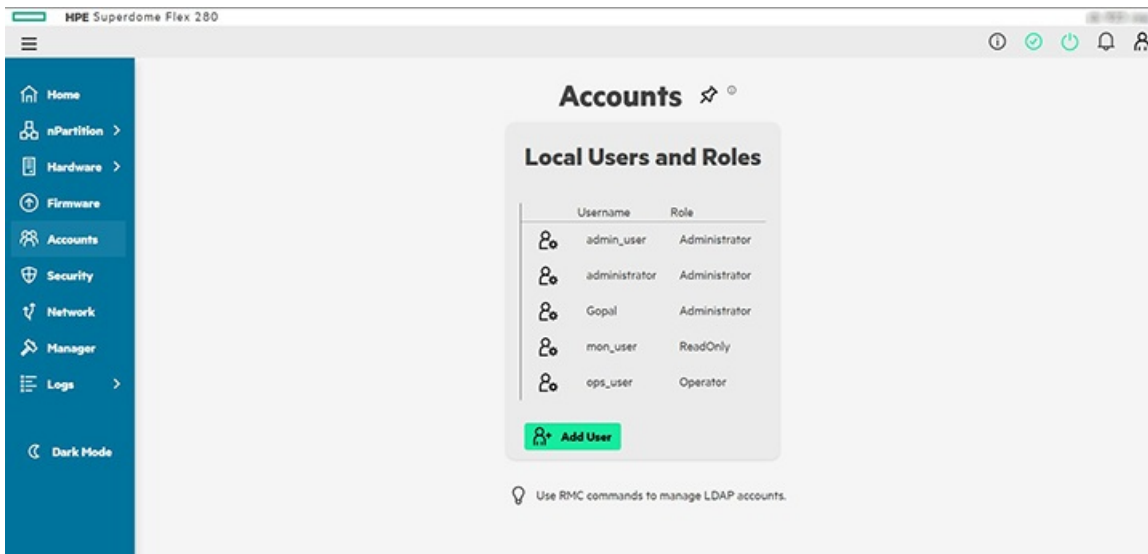
- To view the current user's details, run `show user` command.
- To delete an existing user, run `remove user name=USERNAME` command.

Setting up users from the UI

Procedure

1. Use a web browser to access the RMC UI at `https://RMC-IP-ADDRESS`.
2. Log in to the RMC UI.
3. Click Accounts on the main screen or the menu bar on the left.

Figure 1. User accounts



4. Click Add User.
5. Enter the user name and assign a role to the user.

RMC role name	Privileges
Administrator	All privileges, including ability to create, delete, and edit other user accounts
Operator	Power control, setting a profile, and BIOS parameters
Monitor	Change own password, access <code>access read-only JViewer</code> , and access read-only console

6. To add the user, click Submit.

Setting up RMC SNMP alert monitoring

About this task

The Superdome Flex 280 Server RMC can be configured to send SNMP alerts to a specified IP address for remote monitoring.

Procedure

1. Log in to the RMC with an administrator role.
2. To specify the destination IP address for SNMP alerts, run the `set snmp` command.

```
set snmp forward_address=FORWARD_ADDRESS [port=FORWARD_PORT] [protocol=PROTOCOL]
```

Where `forward_address` can be either an IPv4 or IPv6 address, or hostname.

The specified IP address used for forwarding SNMP alerts, optionally using the port and protocol specified.

3. Reboot the RMC.

```
RMC cli> reboot rmc
```

4. (Optional) To remove SNMP forwarding IP address, run the `remove snmp` command.

```
remove snmp forward_address=FORWARD_ADDRESS
```

Where `forward_address` can be either an IPv4 or IPv6 address, or hostname.

Configuring nPartition attributes

About this task

nPartition attributes control the nPartition configuration.

Attribute values are applied during the nPartition boot process. You can configure the attribute values either when nPartition is powered off, or during the booting process (at UEFI or running an OS). Attribute changes that are made while an nPartition boots are applied the next time it you reboot the system.

Procedure

1. Access the server management interface.

You can configure nPartition attributes from the RMC web GUI (nPartition > Attributes), or the RMC web GUI or the CLI `modify npar attributes` command or through Redfish APIs.

2. You can set the attribute values to either default values or configure custom attribute values.

Setting an nPartition to default attribute values configures all values and applies the default workload profile.

Configuring an individual attribute or applying a workload profile applies specific values, but leaves other optional values unchanged.

```
example eRMC:r001u01c cli>
modify npar attributes WorkloadProfile=HPC

SUCCESS

Partitions: 1

Current: Setting from most recent npar boot
Pending: Setting pending next npar boot
Default: Default setting. Set all attributes to default using 'set npar default attributes'

Partition 0:

Attribute
=====
BootSlots
  Current: 3,5,8
  Pending: 3,5,8
  Default: 3,5,8
-----
...

example eRMC:r001u01c cli>
modify npar attributes HThread=Disabled

SUCCESS

Partitions: 1
...
```

3. Reboot the nPartition to apply the modified nPartition attribute values.

To view the current nPartition attribute value and the nPartition attribute values that are not applied yet, use the RMC web GUI (nPartition > Attributes) or the RMC `show npar attributes` command.

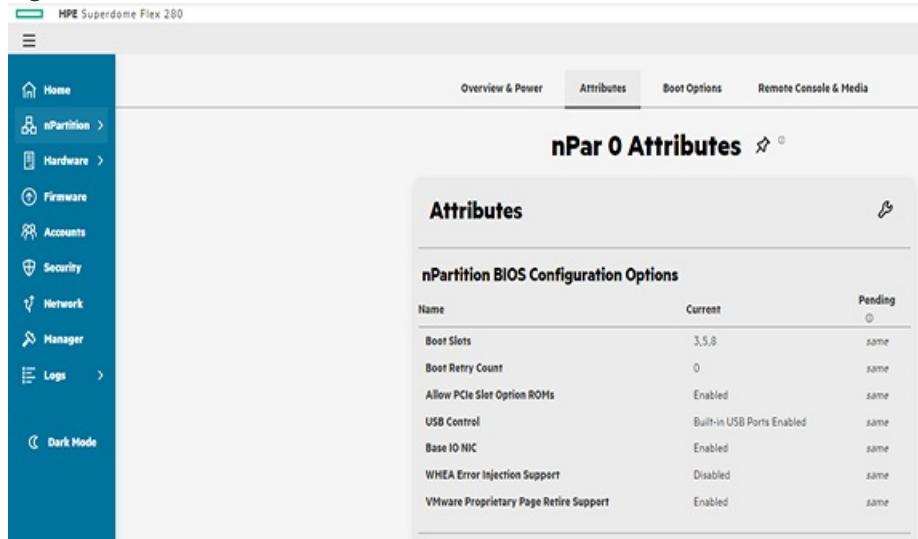


Configuring system nPartition attributes from the UI

Procedure

1. Use a web browser to access the RMC UI at `https://RMC-IP-ADDRESS`.
2. Log in to the RMC UI.
3. Click nPartition on the main screen or the menu bar on the left.
4. Click the Attributes tab.

Figure 1. nPar attribute details



5. Click the  icon next to Attributes, then configure the attributes.

Configuring the Custom workload profile

About this task

Use the Custom workload profile to configure nearly all nPartition attributes with specific values.

Other workload profiles allow some attributes to be customized and have specific settings for other attributes.

Procedure

1. Access the server management interface through the RMC UI or the CLI.

To configure the Custom workload profile, use the RMC UI (nPartition > Attributes) or the RMC `modify npar attributes` command.

```
example eRMC:r001u01c cli>  
modify npar attributes WorkloadProfile=Custom
```

```
SUCCESS
```

```
Partitions: 1
```

```
Current: Setting from most recent npar boot
Pending: Setting pending next npar boot
Default: Default setting. Set all attributes to default using 'set npar default attributes'
```

Partition 0:

Attribute

=====
BootSlots

```
Current: 3,5,8
Pending: 3,5,8
Default: 3,5,8
```

BootRetryCount

```
Current: 0
Pending: 0
Default: 0
```

AllowPcieSlotOpRoms

```
Current: Enabled
Pending: Enabled
Default: Enabled
```

UsbControl

```
Current: UsbEnabled
Pending: UsbEnabled
Default: UsbEnabled
```

BaseIoNic

```
Current: Enabled
Pending: Enabled
Default: Enabled
```

ErrorInjection

```
Current: Disabled
Pending: Disabled
Default: Disabled
```

PageRetireSupport

```
Current: Enabled
Pending: Enabled
Default: Enabled
```

WorkloadProfile

```
Current: MC
Pending: Custom
Default: MC
```

...

2. Set nPartition attributes to custom values.

```
example eRMC:r001u01c cli>
modify npar attributes AdvancedMemProtection=AdvancedEcc

SUCCESS

Partitions: 1
```

```

...
-----
  NumaGroupSizeOpt
    Current:    Clustered
    Pending:    Clustered
    Default:    Clustered
-----
  AdvancedMemProtection
    Current:    ADDDC1
    Pending:    AdvancedEcc
    Default:    ADDDC
-----
...

```

3. Reboot the nPartition.

nPartition attributes are applied when you reboot the nPartition.

To view the current and pending nPartition attribute values, use the RMC UI (nPartition > Attributes) or the CLI `show npar attributes` command.

¹ The Adaptive Double Device Data Correction feature (ADDDC setting) is in effect now. Advanced ECC Support (AdvancedEcc setting) is applied when you reboot the system.

Setting default nPartition attributes

About this task

You can configure all nPartition attributes to the default values by setting workload profile to Mission critical (MC).

Procedure

1. Access the server management interface through the RMC UI or the CLI.

To set the default values for nPartition attributes, use the `set npar default attributes` RMC command or nPartition > Attributes > Settings Icon > Reset Defaults in pop-up in the RMC web GUI.

```

eRMC:r001u01c cli>
set npar default attributes

Setting all attributes to default values for partition p0...
SUCCESS

eRMC:r001u01c cli>

eRMC:r001u01c cli> show npar attributes

Partitions: 1

Current:  Setting from most recent npar boot
Pending:  Setting pending next npar boot
Default:  Default setting.  Set all attributes to default using 'set npar default attributes'

Partition 0:

```



```

Attribute
-----
BootSlots
  Current:    3,5,8
  Pending:    3,5,8
  Default:    3,5,8
-----
...

```

2. Boot or reboot the nPartition.

nPartition attributes are applied when you reboot nPartition.

To view the current and pending nPartition attribute values, use the RMC UI (nPartition > Attributes) or the RMC `show npar attributes` command.

Superdome Flex 280 Server workload profiles and attributes

Superdome Flex 280 Server supports the following nPartition system attributes and workload profiles.

For detailed descriptions of all attributes, see the RMC web GUI.

Table 1. Workload optimization options

Attribute	Mission Critical profile setting	High Performance Compute profile setting	Attribute name (CLI)	Valid setting/Supported values (CLI)
Workload Profile	Mission Critical (default)	High Performance Compute	<code>WorkloadProfile</code>	<code>MC</code> <code>HPC</code> <code>IMDB</code> <code>Virtualization</code> <code>Custom</code>
Power Regulator	OS Control Mode	Static High Performance	<code>PowerRegulator</code>	<code>StaticHighPerf</code> <code>OsControl</code>
Minimum Processor Idle Power Core C-State	C6 State	No C-states	<code>MinProcIdlePower</code>	<code>C6</code> <code>C1E</code> <code>NoCStates</code>
Minimum Processor Idle Power Package C-State	Package C6 (nonretention) State	No Package State	<code>MinProcIdlePkgState</code>	<code>C6Retention</code> <code>C6NonRetention</code> <code>NoState</code>
Energy/Performance Bias	Balanced Performance	Maximum Performance	<code>EnergyPerfBias</code>	<code>MaxPerf</code> <code>BalancedPerf</code> <code>BalancedPower</code> <code>PowerSavingsMode</code>
Intel UPI Link Power Management	Enabled	Disabled	<code>IntelUpiPowerManagement</code>	<code>Enabled</code> <code>Disabled</code>



Attribute	Mission Critical profile setting	High Performance Compute profile setting	Attribute name (CLI)	Valid setting/Supported values (CLI)
Intel Turbo Boost Technology	Enabled	Enabled	ProcTurbo	Enabled Disabled
Energy Efficient Turbo	Enabled	Disabled	EnergyEfficientTurbo	Enabled Disabled
Uncore Frequency Scaling	X (Auto)	Maximum	UncoreFreqScaling	Auto Maximum Minimum
Sub-NUMA Clustering	X (Disabled)	X	SubNumaClustering	Enabled Disabled
NUMA Group Size Optimization	Clustered	Clustered	NumaGroupSizeOpt	Flat Clustered
Advanced Memory Protection	Adaptive Double Device Data Correction (ADDDC)	Advanced ECC Support	AdvancedMemProtection	ADDDC AdvancedEcc Mirrored
Intel NIC DMA Channels (IOAT)	Enabled	Enabled	IntelNicDmaChannels	Enabled Disabled
SR-IOV	X (Enabled)	Disabled	Sriov	Enabled Disabled
Intel Virtualization Technology (Intel VT)	X (Enabled)	Disabled	IntelProcVt	Enabled Disabled
Intel VT-d	X (Auto)	Auto	IntelProcVtd	Auto Enabled
Processor x2APIC Support	Auto	Auto	ProcX2Apic	Auto ForceEnabled



Table 2. Workload optimization options - continued

Attribute	In-Memory Database profile setting	Virtualization profile setting
Workload Profile	In-Memory Database	Virtualization
Power Regulator	OS Control Mode	X ¹
Minimum Processor Idle Power Core C-State	C6 State	X
Minimum Processor Idle Power Package C-State	Package C6 (non-retention) State	X
Energy/Performance Bias	Balanced Performance	X
Intel UPI Link Power Management	Enabled	X
Intel Turbo Boost Technology	Enabled	X
Energy Efficient Turbo	Enabled	X
Uncore Frequency Scaling	Auto	X
Sub-NUMA Clustering	Disabled	X
NUMA Group Size Optimization	Clustered	X
Advanced Memory Protection	Adaptive Double Device Data Correction (ADDDC)	X
Intel NIC DMA Channels (IOAT)	Enabled	X
SR-IOV	Disabled	Enabled
Intel Virtualization Technology (Intel VT)	Disabled	Enabled
Intel VT-d	Auto	Enabled
Processor x2APIC Support	Auto	X

¹ In the given profile, the setting can be changed to any value, that is floating and not forced.

Table 3. Power and performance options

Attribute	Mission Critical profile setting	High Performance Compute profile setting	CLI form	CLI options
Intel Hyper-Threading	X (Enabled)	X	HThread	Enabled Disabled
HW Prefetcher	Enabled	Enabled	HwPrefetcher	Enabled Disabled
Adjacent Sector Prefetch	Enabled	Enabled	AdjSecPrefetch	Enabled Disabled
DCU Stream Prefetcher	Enabled	Enabled	DcuStreamPrefetcher	Enabled Disabled

Attribute	Mission Critical profile setting	High Performance Compute profile setting	CLI form	CLI options
DCU IP Prefetcher	Enabled	Enabled	DcuIpPrefetcher	Enabled Disabled
LLC Prefetch	X (Disabled)	X	LlcPrefetch	Enabled Disabled
LLC Dead Line Allocation	X (Enabled)	X	LlcDeadlineAlloc	Enabled Disabled
Local/Remote Threshold	Auto	Auto	LocalRemoteThreshold	Auto Manual
UPI RRQ Threshold	X (15)	X	UpiRrqThreshold	0-31
UPI IRQ Threshold	X (4)	X	UpiIrqThreshold	0-31
Snoop Throttle Configuration	X (Auto)	X	SnoopThrottleConfig	Auto Disabled Low Medium High
Enhanced Processor Performance	X (Disabled)	X	EnhancedProcPerf	Enabled Disabled
Enabled Cores per Processor	X (0)	X	EnabledCoresPerProc	0-N ¹
Intel DMI Link Frequency	Auto	Auto	IntelDmiLinkFreq	Auto DmiGen1 DmiGen2
Maximum Memory Bus Frequency	Auto	Auto	MaxMemBusFreqMHz	Auto MaxMemBusFreq2933 MaxMemBusFreq2667 MaxMemBusFreq2400 MaxMemBusFreq2133 MaxMemBusFreq1867
Memory Refresh Rate	X (Refreshx1)	X	MemRefreshRate	Refreshx1 Refreshx2
Memory Patrol Scrubbing	Enabled	Enabled	MemPatrolScrubbing	Enabled Disabled
MMIOH Granularity ²	64GB	64GB	MmiohGranularity	64GB , 256GB , 1024GB

¹ N is Max supported cores as per Processor SKU. When set to 0 or N, all cores in Processor are enabled
² Supported from 7HPE Superdome Flex 280 Server version 1.35.12 onwards.

Table 4. Power and performance options - continued

Attribute	High Performance Compute profile setting	Virtualization profile setting
Intel Hyper-Threading	X	X
HW Prefetcher	Enabled	X
Adjacent Sector Prefetch	Enabled	X
DCU Stream Prefetcher	Enabled	X
DCU IP Prefetcher	Enabled	X
LLC Prefetch	X	X
LLC Dead Line Allocation	X	X
Local/Remote Threshold	Auto	X
UPI RRQ Threshold	X	X
UPI IRQ Threshold	X	X
Snoop Throttle Configuration	X	X
Enhanced Processor Performance	X	X
Enabled Cores per Processor	X	X
Intel DMI Link Frequency	Auto	X
Maximum Memory Bus Frequency	Auto	X
Memory Refresh Rate	X	X
Memory Patrol Scrubbing	Enabled	X

Configuring memory mirroring

Prerequisites

Memory mirroring is only supported in a subset of memory configurations. Here are the memory mirroring rules.

- Memory mirroring is supported in the 4, 6, and 12 DDR4 DIMMs per CPU configurations.
- Memory mirroring is NOT supported in the 1 DDR4 DIMM per CPU configuration.
- Memory mirroring is NOT supported when Persistent Memory DIMMs are installed.

About this task

Memory mirroring provides the maximum protection against uncorrected memory errors that might otherwise result in a system failure. When enabled, there is a trade-off between memory capacity and reliability, as user-accessible memory will be reduced to half of the total available memory.

Procedure

1. Access the server management interface.

To configure the Custom workload profile, use the RMC web GUI (nPartition > Attributes) or the RMC `modify npar attributes` command.

```
eRMC:r001u01c cli>
modify npar attributes WorkloadProfile=Custom

SUCCESS
```

2. Set nPartition attribute Advanced Memory Protection to Mirrored Memory.

```
eRMC:r001u01c cli>
modify npar attributes AdvancedMemProtection=Mirrored

SUCCESS
```

3. Boot or reboot the nPartition.


nPartition attributes take effect the next time the nPartition boots.

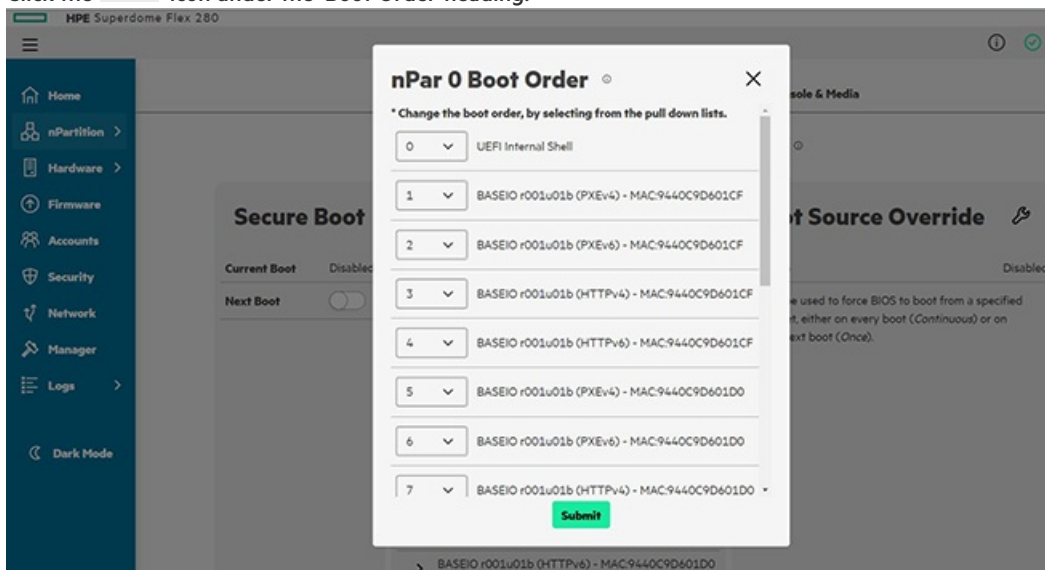
To view the current and pending nPartition attribute values, use the RMC web GUI (nPartition > Attributes) or the CLI `show npar attributes` command.

Setting up boot order with the RMC UI

Procedure

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

- a. Click the  icon under the Boot Order heading.



- b. Choose the boot option you want to change and click the pull-down list.
 - c. Select the position for the boot option from the list.
 - d. To confirm the changes, click Submit.
6. Re-verify the system boot order. The system uses the listed boot order during the next system boot.

Setting up boot options and boot retry count using the RMC CLI

About this task

The Superdome Flex 280 Server can be booted from multiple sources using RMC commands. The boot options can be specified during power on, power reset, or during reboot. You can also specify the number of boot retry attempts to be made on a BootOrder list. Specify the boot retry count using nPar attribute `BootRetryCount` with an allowed range 0–255. The default value is 0. 255 is a special value where system gets into an infinite boot loop mode until the system is successfully booted with one of the UEFI boot options configured in the system.

When a specific boot source type is selected, then a boot retry attempt is made on the configured boot source type only.

Procedure

1. Log in to the RMC CLI.

2. Verify the boot option required.

The following boot options are available:

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

3. Specify boot retry count using `modify npar` command.

```
modify npar attributes pnum=p0 [bootretrycount=<value>]
```

4. Choose one of the following options:

- Power on—If you are powering on the server, run the `power on` command.
 - If you want each of the option in the boot order list to be retried for the number of times specified in `bootretrycount`, run

```
power on npar pnum=0
```
 - If you want a specific boot source type to be retried for the number of times specified in `bootretrycount`, run

```
power on npar pnum=0 [bootopt=BOOTOPT]
```
- Power reset or reboot—If you are resetting the power or rebooting, run the `power reset` or `reboot` command.
 - If you want each of the option in the boot order list to be retried for the number of times specified in `bootretrycount`, run

```
power reset npar pnum=0
```

```
reboot npar pnum=0 [force]
```
 - If you want particular boot source type to be retried for the number of times specified in `bootretrycount`, run

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

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

 - If power is on, by default the `power reset` or `reboot` command performs a graceful OS shutdown then restarts the server.
 - If `force` is specified, `power reset` or `reboot` command performs an OS immediate (non-graceful) shutdown

instead, and then restarts the server.

Setting up boot order with UEFI Boot Manager

Procedure

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

Secure boot

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

Secure boot features

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

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

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

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

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



NOTE:

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

Subtopics

[Default secure boot keys](#)

[Configuring Secure Boot on HPE Superdome Flex 280 Server](#)

[Installing or reinstalling default Secure Boot keys](#)

Default secure boot keys

The default keys include signatures for supported operating systems.

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

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

Configuring Secure Boot on HPE Superdome Flex 280 Server

About this task

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

Procedure

- [Configure Secure Boot with the RMC UI](#)
- [Configure Secure Boot with the RMC CLI](#)
- [Configure Secure Boot with the UEFI Boot Manager](#)

Subtopics

[Configuring secure boot from the RMC UI](#)

[Configuring secure boot from the RMC CLI](#)

[Configuring Secure Boot with UEFI Boot Manager](#)

Configuring secure boot from the RMC UI

Procedure

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



Configuring secure boot from the RMC CLI

Prerequisites

- System must be powered off.

About this task

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

Procedure

To enable secure boot:

1. Log in to the RMC CLI.
2. Verify that the system is powered off. If not, run `power off npar` command.
3. Run the `modify npar` command.

- To enable `Secure Boot`, run

```
modify npar secure_boot=on
```

- To disable `Secure Boot`, run

```
modify npar secure_boot=off
```

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

```
show npar verbose
```

5. Power on the system.

```
power on npar
```

Configuring Secure Boot with UEFI Boot Manager

Procedure

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

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

3. Enable or disable secure boot.

To enable secure boot:

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

- a. Enable Secure Boot with the default keys.

Select the `Attempt Secure Boot` option.

- b. Install custom keys.

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

To disable secure boot, clear the `Attempt Secure Boot` option.

4. To apply the changes, reset the system.

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

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

Press Enter to reset the system.

More information

Default secure boot keys

Installing or reinstalling default Secure Boot keys

Prerequisites

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

About this task

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

Procedure

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

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

3. Select the Custom Secure Boot Options menu.

Change the Secure Boot Mode option to Custom Mode, then select the Custom Secure Boot Options menu.

4. Delete all KEK keys.

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

5. Delete all DB keys.

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

6. Delete all DBX keys.

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

7. Delete the PK key.

Select the PK Options menu, then select the Delete Pk checkbox. Press Y to confirm.

8. Reset the system to apply the changes.

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

More information

Default secure boot keys

Setting up remote media files with the RMC UI




Prerequisites

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

About this task

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

Procedure

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

This enables you to configure the file server options, IP address, media path, and login credentials.

6. Connect to the file server by clicking Connect.
7. Select the image files.

Two image files can be selected and inserted.

To remove an image file, click Eject.

- a. Click the Select Media Files drop-down list under the Media Files heading.
- b. Select an image file in the specified file path.
- c. Click Insert. The selected image file is inserted.

Websites

HPE Superdome Flex 280 Server websites

- Product page
www.hpe.com/support/superdomeflex280-product
- Customer documentation
www.hpe.com/support/superdomeflex280-docs
- Software
www.hpe.com/support/superdomeflex280-software
- HPE Foundation Software
<https://downloads.linux.hpe.com/SDR/project/hpe-foundation/>
- Hewlett Packard Enterprise server operating systems and virtualization software
www.hpe.com/us/en/servers/server-operating-systems.html
- HPE Superdome Flex 280 Server QuickSpecs

www.hpe.com/support/superdomeflex280-quickspecs

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

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

- Customer advisories

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

- Spare parts list

www.hpe.com/support/superdomeflex280-spareparts

- Release sets (support matrix)

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

- Safety and regulatory information

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

- Recycling information

www.hpe.com/recycle

- Visio templates

www.visiocafe.com/hpe.htm

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

- Supported browsers

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

HPE Superdome Flex 280 Server support documentation

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

Support and other resources

Subtopics

[Accessing Hewlett Packard Enterprise Support](#)

[Accessing updates](#)

[Remote support](#)

[Customer self repair](#)

[Warranty information](#)

[Regulatory information](#)

[Documentation feedback](#)

Accessing Hewlett Packard Enterprise Support



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

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

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

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

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

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

- To download product updates:

Hewlett Packard Enterprise Support Center

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

My HPE Software Center

<https://www.hpe.com/software/hpesoftwarecenter>

- To subscribe to eNewsletters and alerts:

<https://www.hpe.com/support/e-updates>

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

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

IMPORTANT:

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

Remote support

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

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

HPE Get Connected

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

HPE Tech Care Service

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

HPE Complete Care

<https://www.hpe.com/services/completecure>

Customer self repair

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

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

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, use the Feedback button and icons (at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (<https://www.hpe.com/support/hpesc>) to send any errors, suggestions, or comments. This process captures all document information.



