Hewlett Packard Enterprise

HPE Superdome Flex 280 Server Administration Guide

Abstract

System administration commands, procedures, security, and management interfaces for HPE Superdome Flex 280 Server.

Part Number: 10-192008-Q323
Published: June 2023
Edition: 5

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
10-192008-Q323	June 2023	5	• Added `Severity_level` parameter in the following commands: ◦ **`SET REMOTE_LOG_SERVER`** ◦ **`SHOW REMOTE_LOG_SERVER`** ◦ **`set`** ◦ **`show`** • Updated `USERNAME` description in the **`test`** command.
10-192008-Q123	December 2022	4	• Updated UDP protocols. • Updated following sections: ◦ **Installing the latest complex firmware using SUM** ◦ **Installing the latest complex firmware using HPE OneView** • Added details of **Create a new IPMI user**. • Added `idc` details in the **`collect`**, **`remove`**, **`show`**, and **`upload`** commands. • Added server firmware updates in **When to use a server profile** and **OneView capabilities supported on HPE Superdome Flex family of servers** sections. `
10-192008-Q422	September 2022	3	Updated example command-line for test command.

Table Continued

Part number	Publication date	Edition	Summary of changes
10-192008-Q222	May 2022	2	• Added `TCP` protocol details for the following commands: ◦ **`SET`** ◦ **`set`** • Added new `connection={ldap,ldaps}` parameter in the **`set`** section. • Added `predictive_mem_health` option for the following commands: ◦ **Rack management controller (RMC) commands** ◦ **`apropos`** ◦ **`disable`** ◦ **`enable`** ◦ **`show`**
10-192008-Q421b	November 2021	1	Initial release as *HPE Superdome Flex 280 Server Administration Guide*

Contents

HPE Superdome Flex 280 Server manageability features

Superdome Flex 280 Server has an advanced manageability system that is always on, constantly monitoring and managing the system components, fabric, and infrastructure for mission-critical high availability.

Major Superdome Flex 280 Server management components include:

Rack Management Controller (RMC)

The main component in the management subsystem. The RMC connects to all the system chassis through a physically secure private LAN. It provides this functionality using an existing BMC management processor instead of a separate 1U server.

Baseboard Management Controller (BMC)

Chassis-level management. Configures and manages the hardware in that chassis as well as providing virtual media and virtual keyboard, video, or mouse (KVM) features.

Supported manageability software includes:

- HPE OneView
- HPE Insight Remote Support
- HPE Serviceguard for Linux
- Smart Update Manager

For an overview of management features, see **https://www.hpe.com/support/superdomeflex280-manageability**.

Rack management controller (RMC) tasks

The RMC includes a command set that you can use to perform administrative functions on the HPE Superdome Flex 280 Server. This chapter describes how to complete several administrative tasks.

NOTE: Although you may encounter both RMC and eRMC terminology in displays and documentation, the preferred term is RMC.

Connecting to the Rack Management Controller (RMC)

About this task

You can connect to the RMC in one of the following ways:

- Through a laptop attached to the RMC through the micro USB port.

  This connection is a direct-attached serial connection using the USB-A to Micro-USB-B cable that was included in the shipping crate.

  For example, this type of connection can be useful if you lost the RMC password. If you have lost your password, press the manageability reset button for five seconds or more. A system menu appears on the micro-serial console to recover or discover the default administration password. For this reason, Hewlett Packard Enterprise recommends that you restrict physical access to the system as part of your site security procedures.

  For information about connecting to the RMC using a laptop, see **Configuring HPE Superdome Flex 280 Server**.
- Through the web interface, access `https://<flex_rmc>` from your browser, where *flex_rmc* is the address or name of the RMC.
- Through the command line interface, through the secure shell (ssh) command.
- Through a network connection, through secure shell (ssh) command.

The following procedure explains how to connect to the RMC over a network connection. See **Configuring HPE Superdome Flex 280 Server** for information about setting networking parameters on the RMC.

Procedure

1. Use the secure shell (`ssh`) command to log into the RMC.

   The factory configures the default login for the RMC to be `administrator`.
2. Respond to the prompts for the login name and password.

```
remotehost% ssh administrator@flex_rmc
password: #####

HPE Superdome Flex 280 BMC,  Firmware Rev. 3.10.164-20210329_061054
(C) Copyright 2019-2021 Hewlett Packard Enterprise Development LP

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

RMC cli>
```

   For the password, enter the current RMC password for the `administrator` user, and press **Enter**.

If you configured a site-specific RMC password during the installation and configuration process, use your site-specific password. Hewlett Packard Enterprise recommends that you configure a site-specific password.

If you did not specify a site-specific RMC password, use the factory-default RMC password. The factory-default RMC password appears on the password sticker. The password sticker is a bar coded sticker that appears on your system. The sticker is top-right rear corner of the base chassis.

For information about the placement of the password sticker, see **Configuring HPE Superdome Flex 280 Server**.

Powering on and booting an HPE Superdome Flex 280 Server system from a complete power off

About this task

The following procedure explains how to power on an HPE Superdome Flex 280 Server system from a complete power off.

Procedure

1. Visually inspect the system and make sure that the power circuit breakers are on.

   There is power to the RMC and to the BMCs as long as the RMC and the BMCs are attached to a power source.

2. Connect to the RMC and log in.
3. Check the state of the system.

   a. To view the partition configuration from the CLI, enter the following commands.

   ```
   RMC cli> show npar
   RMC cli> show complex
   ```

   If no errors are indicated or if the system health status is OK, then proceed to power up the system. If there are errors, run `RMC cli> show logs error` and resolve the errors before powering up the system.

   b. View the health state of the system from the UI.

   The health state of the system is displayed in the top bar as a health icon in the web interface.

   Table 1:

Icon	State
	Healthy state
	Warning condition
	Critical condition

   Click the Health icon to drill into the cause of any warnings or critical conditions.

4. To power up the system, using the configured `Boot Order`, enter `power on` or `power on npar pnum=0`.

   To power on the nPar from the UI, select **nPartition** > **Power Control**.

Alternatively, to power up the system directly to the UEFI Shell, enter `power on npar pnum=0 bootopt=UefiShell`.

5. To connect to the console, enter the following command:

   ```
   RMC cli> connect npar pnum=0
   ```

   Alternatively, from the UI, select **nPartition** > **Remote Console & Media** > **Launch Remote Web Console**.

   It can take 5 to 10 minutes for the console to display the output or become active.

6. When the `Shell>` prompt appears, select the correct filesystem to access the boot partition.

   a. To list the available filesystems:

      ```
      Shell> map fs*
      ```

   b. To select the desired filesystem:

      ```
      Shell> fs0:
      ```

7. Boot the system.

   - On Oracle Linux Unbreakable Enterprise Kernel (UEK) systems or on Red Hat Enterprise Linux (RHEL) systems, enter the following command:

     ```
     fs0:\> EFI\redhat\grubx64.efi
     ```

   - On SLES systems, enter the following command:

     ```
     fs0:\> EFI\sles\grubx64.efi
     ```

More information

Connecting to the Rack Management Controller (RMC)

Powering off an HPE Superdome Flex 280 Server

About this task

The following procedure explains how to power off an HPE Superdome Flex 280 Server system.

Procedure

1. For a system running on Linux, log into the HPE Superdome Flex 280 Server using an account with administrator or operator privileges, and enter the following command to stop the operating system and shut down the system:

   ```
   # shutdown -h
   ```

2. To verify that the Run State is Off:

   From CLI, enter the following command:

   ```
   RMC cli> show npar
   Partitions: 1

   Par  Run        Health     Chassis CPUs  CPU Cores DIMMs   Memory (GiB) IO Cards
   Num  State      Status     OK/In   OK/In OK/In     OK/In   RAM/PMem     OK/In
   ==== ========== ========== ======= ===== ========= ======= ============ ========
   p0   Off        OK         1/1     4/4   1536/1536 48/48   1535/0       0/0
   ```

```
* OK/In = OK/Installed
```

From UI, select **nPartition** > **Power Control** and observe the power state.

3. If the power is still on after an extended amount of time, log into the RMC using an account with administrator or operator privileges.

   - From CLI, enter the following command to power off a single partition:

     ```
     RMC cli> power off npar pnum=0 [force]
     ```

     The `force` option makes the partition perform an OS immediate (non-graceful) shutdown if the OS is still running.

   - From UI, select **nPartition** > **Power Control** and choose the required method to forcefully shutdown the nPar.

TIP: You can monitor the shutdown progress from the nPartition console.

Configuring the auto-power capability from the CLI

About this task

The auto-power capability enables the HPE Superdome Flex 280 Server to power up automatically when AC power is applied after a power outage.

This procedure explains how to:

- Retrieve the current auto-power setting information.
- Configure the auto-power setting.

Procedure

1. From CLI, log into the RMC as a user with `administrator` role.
2. To check whether the auto-power capability is in enabled or disabled state, run the `show autopower` command.

   ```
   RMC cli> show autopower
   ==== r001u01 ====
   auto-power on is disabled
   ```

3. To configure the auto-power capability, run the following commands:

   - To enable auto-power, run:

     ```
     RMC cli> enable autopower
     ==== r001u01 ====
     auto-power on enabled (120 second delay)
     ```

   - To change the delay for auto-power, run:

     ```
     RMC cli> set autopower delay=SECONDS
     ```

     Where *SECONDS* is the number of seconds before the server powers up after AC power is applied.

- To disable auto-power, run:

```
RMC cli> disable autopower
==== r001u01 ====
auto-power on disabled
```

- To cancel auto-power after an AC power-up while the delay period has not yet expired, run:

```
RMC cli> cancel autopower
==== r001u01 ====
auto-power on cancelled
```

  You can use this command to cancel auto-power capability before the timeout expires, so the RMC will not automatically restore power to the nPartitions this time and the auto-power capability remains enabled for next time.

Configuring hyper-threading technology from the UI

About this task

Use the HPE Superdome Flex 280 Server nPartition attributes to configure the nPartition that includes enabling or disabling the Hyper-Threading (Attribute Name - HThread).

For more information about configuring nPartition Attributes, see **Configuring and Operating HPE Superdome Flex 280 Server**.

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.

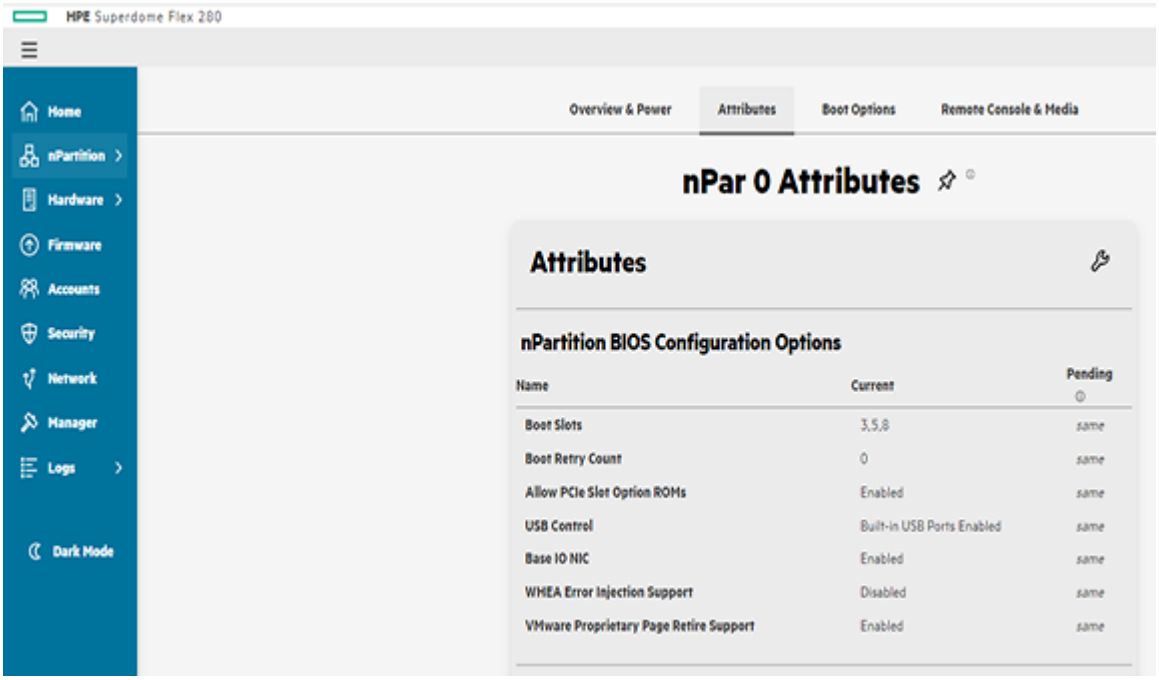


Figure 1: nPar attribute details

5. Click the  icon next to **Attributes**, then configure the attributes.
6. Under **Power and Performance Options**, select **Enabled** or **Disabled** from drop-down for **Intel(R) Hyper-Threading** option.
7. Click **Apply BIOS Attributes**.

Configuring RAS from the UI

About this task

Use the HPE Superdome Flex 280 Server nPartition attributes to configure the nPartition to apply a workload profile (Attribute Name - WorkloadProfile) and modify the Advanced Memory Protection attributes (Attribute Name - AdvancedMemProtection). For more information about configuring nPartition attributes and configuring the Custom workload profile, see **Configuring and Operating HPE Superdome Flex 280 Server**.

CAUTION: Hewlett Packard Enterprise strongly recommends using `AdvancedMemProtection=ADDDC` to enable memory RAS features. HPE RAS features provide higher resiliency to DIMM faults versus standard memory error-correcting code (ECC). When `AdvancedMemProtection=AdvancedEcc`, memory RAS features are disabled and therefore could result in compromised system resiliency and a potential server outage.

You might experience high failure rates of DIMMs using `AdvancedMemProtection=AdvancedEcc`.

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.

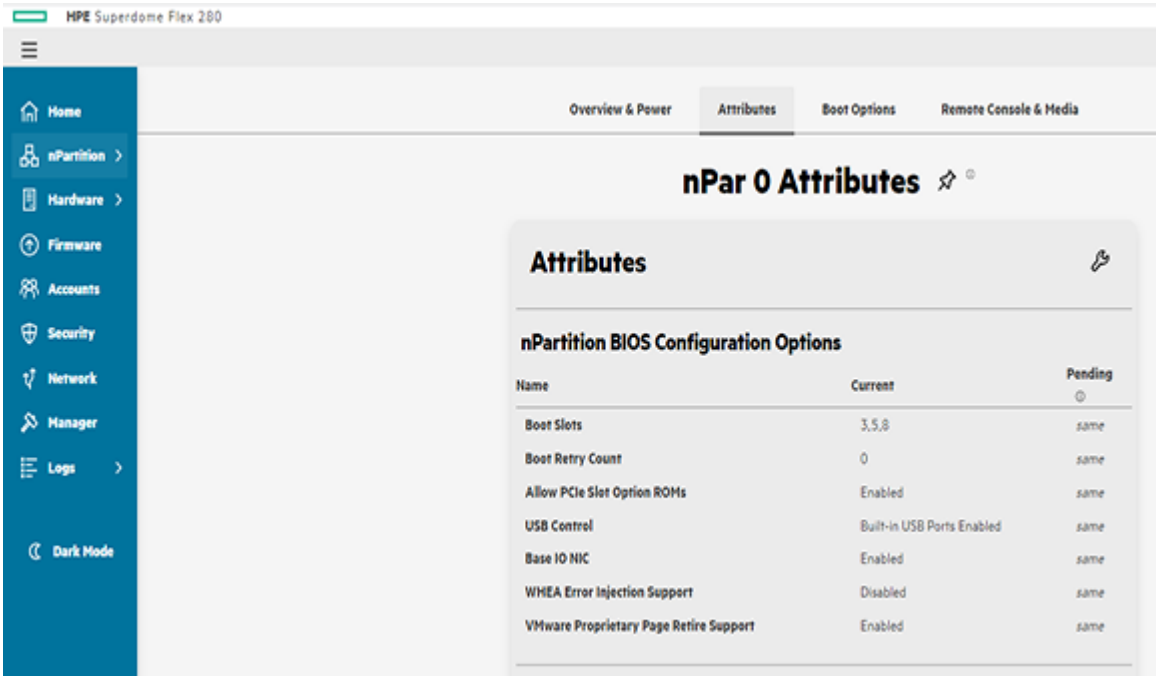


Figure 2: nPar attribute details

5. Click the  icon next to **Attributes**, then configure the attributes.
6. Under **Workload Optimization Options**, select **Custom** option for **Workload Profile**.
7. Select the required attributes for **Advanced Memory Protection**.
8. Click **Apply BIOS Attributes**.

Configuring RMC user accounts and user roles

About this task

You can manage user accounts from UI or from CLI. User roles can be defined when creating a user account.

Procedure

1. From the CLI, enter the `add user` command.

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

   USERNAME

   Specify the name of a new user based on the following specification:

   - You can add a maximum of 30 users.
   - *USERNAME* must begin with a letter and is case-sensitive.
   - *USERNAME* must be unique to all other user names and group names.

- *USERNAME* can be from 2 to 20 characters long including alphanumeric characters and dash, and underscore among the special characters.
- Certain user names are reserved for RMC and are as follows:

User name	Reserved on RMC
Administrator	X
backup	
bin	
daemon	X
dbus	
ftp	
haldaemon	
logger	X
mail	
nobody	
ntp	X
operator	
proxy	
root	X
sshd	X
sys	
sysadmin	X
sync	
www-data	

When creating the user, the system also prompts you to create a password.

NOTE: The password can be of 6 to 64 characters long including all printable characters. The default minimum number of characters required is 8.

2. When creating the user, the RMC also prompts you to create a password. Enter a password for the user account.

   The password can be from 6 to 64 characters long and can include all printable characters. The default minimum number of characters required is 8.

3. To verify the user list, enter the command `show user list`.

   - To see details of the current user, enter the command `show user`.
   - To delete an existing user, enter the command `remove user name=`*`USERNAME`*.

   From UI, select the **Accounts** menu to manage user accounts.

More information

`add`
`show`
`remove`

User roles

HPE Superdome Flex 280 Server supports role-based user accounts that provide each user account with privileges to improve security. Roles can be configured for RMC or Redfish. Up to 30 user accounts can be created.

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

Retrieving HPE Superdome Flex 280 Server system configuration information

From UI, select **Hardware** menu to view the system configuration.

From CLI, you can use the `show complex` command to view system configuration and baseboard management controller (BMC) identifiers.

Many RMC commands and `ipmi` commands require you to specify one of these IDs when you want the command to operate on a specific BMC. The command syntax permits you to shorten the IDs by omitting the leading `0` characters. In these commands, if you decide to omit any leading `0` characters, omit all. For example, you can specify the BMC ID `r001u01b` as `r1u1b`, by omitting the `0` character.

```
RMC cli> show complex


SSN: 5UF6512345

RMCs:             1
        r001u01c eRMC


BMCs:             2
        r001u01b BASE-CHASSIS         P000
        r001u06b EXPANSION-CHASSIS    P000


Partitions:       1
        partition000 BMCs:    2
                r001u01b
                r001u06b
```

The output shows the following:

- This system has one RMC, and its node name is `r001u01c`.
- There are two chassis BMCs, and their IDs are `r001u01b` and `r001u06b`.
- There is one partition, p0, and it contains both chassis.

Monitoring log files

About this task

The Superdome Flex 280 Server logs events of RMC, BMCs, and server. From UI, select the **Logs** menu to view log files. From CLI, the `show logs` command returns the value of various log files.

- `show logs audit`
- `show logs console target={BMC_GEOID | pnum=0} [socket={0-3}] [full]`
- `show logs dmesg [target=`*`target`*`]`
- `show logs error [mca | cmc | type=`*`SEVERITY`*` | id=`*`BUNDLE_ID`*` | pnum=`*`0`*`]`
- `show logs hel [all] [hex] [target=`*`TARGET`*`]`
- `show logs iel [live]`

  Same as `show livelogs`
- `show logs rcu [list | id=`*`HEX_ID`*` | file=`*`FILENAME`*`] [verbose]`
- `show logs sel [target=`*`TARGET`*`]`
- `show logs support [ieldepth=`*`DAYS`*`]`
- `show logs syshist [verbosity={0,1,2} | raw]`

The following procedure shows how to retrieve hardware event log file and the RMC start-up log file.

Procedure

1. Log into the RMC as the `administrator` user.
2. Enter the `show logs hel all` command to retrieve hardware event logs.

```
RMC cli> show logs hel all
 UV4_NI1_HCERR_SUMMARY                    : 0x0000000000000001
 UV4_NI1_HCERR_FIRST                      : 0x0000000000000001
 UV4_NI1_HCERR_TIME_STAMP                 : 0x80003DC074E22444
 UV4_NI1_NL0_HCERR_SUMMARY                : 0x000000000000004C
 UV4_NI1_NL0_HCERR_FIRST                  : 0x0000000000000008
 UV4_NI1_NL0_HCERR_OVERFLOW               : 0x0000000000000000
 UV4_NI0_AOERR0_SUMMARY                   : 0x0000000000000002
 UV4_NI0_AOERR0_FIRST                     : 0x0000000000000002
 UV4_NI0_AOERR0_TIME_STAMP                : 0x80003DC074E224C4
 UV4_NI0_NL1_AOERR_SUMMARY                : 0x0000000000000008
 UV4_NI0_NL1_AOERR_FIRST                  : 0x0000000000000008
 UV4_NI0_NL1_AOERR_OVERFLOW               : 0x0000000000000000
 UV4_NI1_AOERR0_SUMMARY                   : 0x0000000000000001
 UV4_NI1_AOERR0_FIRST                     : 0x0000000000000001
```

```
 UV4_NI1_AOERR0_TIME_STAMP                  : 0x80003DC074E22504
 UV4_NI1_NL0_AOERR_SUMMARY                  : 0x0000000000000008
 UV4_NI1_NL0_AOERR_FIRST                    : 0x0000000000000008
 UV4_NI1_NL0_AOERR_OVERFLOW                 : 0x0000000000000000
++++ r001u06b 20210805 07:36:56
**** RESET ****
++++ r001u06b 20210805 08:04:34
**** RESET ****
++++ r001u06b 20210805 08:09:59
**** RESET ****
++++ r001u06b 20210805 08:24:25
**** RESET ****
++++ r001u06b 20210805 08:39:07
**** RESET ****
++++ r001u06b 20210805 09:54:57
**** RESET ****
++++ r001u06b 20210805 10:30:33
**** RESET ****
++++ r001u06b 20210805 10:50:55
**** RESET ****
++++ r001u06b 20210805 11:19:45
**** RESET ****
++++ r001u06b 20210805 11:41:36
**** RESET ****
++++ r001u06b 20210805 18:33:22
**** RESET ****
++++ r001u06b 20210805 18:34:46
**** RESET ****
++++ r001u06b 20210805 18:38:26
**** RESET ****
++++ r001u06b 20210805 18:40:55
**** RESET ****
++++ r001u06b 20210805 18:43:20
**** RESET ****
<type h for help>  lines 33209-33256/33256  (END)
```

The `show logs hel all` command output contains information about correctable memory errors, uncorrectable memory errors, machine checks, and other events.

3. Enter the `show logs dmesg` command to retrieve the RMC start-up log file.

```
RMC cli> show logs dmesg
...

[    3.024725] VFS: Mounted root (cramfs filesystem) readonly on device 1:0.
[    3.031567] devtmpfs: mounted
[    3.034931] Freeing unused kernel memory: 204k freed

...
```

More information

show

Remote syslog

HPE Superdome Flex 280 Server RMC supports remote logging of the system events. The transmitted system log consists of Integrated Event Log (IEL) events like power transition, failure events, information refresh, and others. You can configure the remote logging functionality through the RMC Command Line Interface (CLI).

SET

Syntax

```
SET REMOTE_LOG_SERVER address=<server_address> [port=PORT] [protocol=PROTOCOL] [severity_level=SEVERITY_LEVEL]
```

Description

Set the IP address or hostname of remote log server to enable remote logging. You can optionally provide port number and protocol to be used for connecting to remote log server. Reboot RMC for the newly configured server settings to take effect.

Parameters

`Address`

Remote server IP address or hostname. IP address can be IPv4 or IPv6.

`Port`

The port number to be used can optionally be provided for connecting to the remote log server. Default port number is 514. Port numbers allowed to be specified are 1–65535.

`Protocol`

The protocol to be used can optionally be provided for connecting to the remote log server. The supported protocols are `UDP` and `TCP`. Default protocol is `UDP`.

`Severity_level`

The severity level can optionally be provided for selecting the severity level. Default severity level is `info`. The supported input values can be:

- `debug`
- `info`
- `warn`
- `critical`
- `fatal`

Permissions

The user must have server administrator privileges.

Example input

```
SET REMOTE_LOG_SERVER address=192.168.1.1 [port=514] [protocol=UDP] [severity_level=info]
```

TEST

Syntax

```
TEST REMOTE_LOG
```

Description

After configuring remote log server, run the test command to verify RMC to remote log server communication.

Permissions

Administrator

Example input

```
RMC cli> test remote_log
```

```
RMC cli> ping -c2 10.11.12.135
```

Example output

```
Ping Test was successful.
A test log message has been sent to the system log.
Verify remote server for test message.
```

CLEAR

Syntax

```
CLEAR REMOTE_LOG_SERVER
```

Description

Clears configured remote log server settings and disables sending system log to the remote log server. Reboot RMC to disable logging to remote server.

Permissions

The user must have server administrator privileges.

SHOW

Syntax

```
SHOW REMOTE_LOG_SERVER
```

Description

Displays configured remote log server details.

Permissions

Administrator, Operator, and Monitor

Example input

```
RMC cli> show remote_log_server
```

Example output

```
-- Remote log server Information --
Server: 10.11.12.135
Port: 514
Protocol: udp
Severity_level: info
```

Remote syslog format

The syslog format is provided below. The syslog include time stamps, event messages, severity, host IP addresses, diagnostics, and other related information required for server diagnostics.

```
Server date and Time <RMC host Name>|Syslog severity|<IEL Event Index>|<IEL
Event Type>|<IEL Event Source>|<nPAR #>|<IEL Severity>|<64-bit data>|<IEL
Event Keyword>|<Decoded Data>|<IEL Event description>
Server Date and Time: Data and time when event received recorded by remote
server.
RMC host Name: RMC host name recorded by remote server.
Syslog severity: Syslog event severity.
IEL Event Index: IEL Event Number
IEL Type: Event type, for example: MFW, SFW, OS, PET.
IEL Source: Source of event, for example chassis r001u01b.
nPar#: The partition number.
IEL Severity: Level 0 (minor) to 7 (fatal). Note that this is the opposite
of syslog level where 0 is the highest severity.
64-bit data: IEL payload. Further decoded in Decoded Data
IEL Keyword: Event Keyword, for example: DCD_OS_LAST_SHUTDOWN_GRACEFUL
Decoded Data: Decoded 64-bit data, if applicable. Empty otherwise. Note that
ASCII string payload will always be decoded in "".
IEL full description: Full description of the <IEL Keyword>
Syslog severity is as per generic syslog alert levels, below are possible
values for syslog severity.
0:Fatal
2:Critical
4:Warning
6:Info
7:debug
```

Updating firmware

Hewlett Packard Enterprise recommends that all firmware on all devices in your system be updated to the latest version after hardware installation is complete. Hewlett Packard Enterprise also encourages you to check back often for any updates that might have been posted.

There are three methods for updating the complex firmware; using SUM (Smart Update Manager), using HPE OneView, or manually. Each method uses a different firmware bundle available at **www.hpe.com/support/superdome-flex-software**. Detailed installation instructions are provided in each bundle.

Installing the latest complex firmware using SUM

The Smart update Manager (SUM) utility enables you to deploy firmware components from either an easy-to-use interface or a command line. SUM has an integrated hardware discovery engine that discovers the installed hardware and the current versions of firmware in use on target servers. SUM also has logic to install updates in the correct order and ensure that all dependencies are met before deployment of a firmware update. SUM also contains logic to prevent version-based dependencies from destroying an installation. This logic ensures that updates are handled in a manner that reduces any downtime required for the update process.

Detailed installation instructions are provided in the SUM bundle titled "HPE Superdome Flex 280 Server Firmware Bundle <version>" available at **https://www.hpe.com/support/superdomeflex280-software** (select Subtype = System).

For more information about SUM, see the **HPE Smart Update Manager User Guide**.

NOTE: You can also update firmware manually. For more information about manually updating the firmware, see the detailed instructions provided in the release notes for the firmware bundle.

More information

Updating firmware manually

Installing the latest complex firmware using HPE OneView

About this task

The HPE OneView utility enables you to deploy firmware updates through the HPE OneView interface.

NOTE: Updating firmware with HPE OneView requires HPE OneView version 5.5 or later.

Detailed installation instructions are provided in the HPE OneView bundle titled “HPE Superdome Flex 280 Server Firmware Bundle <version>” and available at **www.hpe.com/support/superdomeflex280-software**.

For more information about HPE OneView, see *HPE OneView User Guide* at **https://www.hpe.com/info/oneview/docs**.

NOTE: You can also update firmware manually. For more information about manually updating the firmware, see the detailed instructions provided in the release notes for the firmware bundle.

More information

Updating firmware manually

Updating firmware manually

About this task

The following procedures explain how to update all the firmware on an HPE Superdome Flex 280 Server. These procedures upgrade the firmware on the RMC and on the BMCs.

You can perform firmware updates online or offline. The firmware release notes indicate whether updates support online firmware update or not.

Updating firmware offline

About this task
You can update the firmware from the UI or from the CLI.

Procedure

a. To update the firmware from the UI, first power off the nPartition. Select **nPartition** > **Power Control**

b. Monitor the power status in **Power Control**. Whenthe power status indicates powered off, update the firmware.

c. Select **Firmware** > **Update**.

d. To view the updated firmware version select **Firmware**.

1. o update the firmware from the CLI, first obtain a copy of the HPE Superdome Flex 280 Server Firmware Bundle from **http://www.hpe.com/support/superdomeflex280-software**.

2. Download the new firmware bundle to a location on a computer which is accessible from the RMC over the local network.

3. Log into the RMC as the `administrator` user and provide the password when prompted.

For example:

```
remotehost% ssh administrator@flex-rmc
```

4. To verify that the RMC is configured to use a DNS, enter the following command:

   ```
   RMC cli> show dns
   ```

   If necessary, use the `add dns` command to configure DNS access.

5. Power off the system.

   ```
   RMC cli> power off npar pnum=x
   ```

6. To update the firmware, enter the following command:

   ```
   RMC cli> update firmware url=path_to_firmware
   ```

   For *path_to_firmware*, specify the location on the local computer that specifies the location of the firmware bundle that you downloaded. Acceptable paths to the location are `https`, `sftp`, and `scp`.

   For example:

   ```
   RMC cli> update firmware url=https://myhost.com/bundle
   ```

   The firmware supports specifying the protocol and port in *path_to_firmware*.

   For example:

   ```
   update firmware url=https://myhost.com/bundle
   update firmware url=https://myhost.com:1234/bundle
   ```

7. Wait for the RMC to reboot.

8. To verify the new firmware level, enter the following command:

   ```
   RMC cli> show firmware verbose
   ```

9. To activate new system firmware, enter the following command:

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

   Where *x*=partition number. *x*=0 will power up the entire system.

Updating firmware online

About this task

You update the firmware from the UI or from the CLI.

Procedure

a. When you update the firmware from the UI, select a bundle that resides on an HTTPS server.

b. From the UI, select **Firmware** > **Update**.

c. To activate new system firmware on an nPartition select **nPartion** > **Power Control** > **Graceful Restart**.

1. To update the firmware through the CLI, first obtain a copy of the HPE Superdome Flex 280 Server Firmware Bundle from **http://www.hpe.com/support/superdomeflex280-software**.

2. Download the new firmware bundle to a location on a computer which is accessible from the RMC over the local network.
3. Log into the RMC as the `administrator` user and provide the password when prompted.

   For example:

   ```
   remotehost% ssh administrator@flex-rmc
   ```

4. To verify that the RMC is configured to use a DNS, enter the following command:

   ```
   RMC cli> show dns
   ```

   If necessary, use the `add dns` command to configure DNS access.

5. To update the firmware, enter the following command:

   ```
   RMC cli> update firmware url=path_to_firmware
   ```

   For *path_to_firmware*, specify the location on the local computer that specifies the location of the firmware bundle that you downloaded. Acceptable paths to the location are `https`, `sftp`, and `scp`.

   For example:

   ```
   RMC cli> update firmware url=https://myhost.com/bundle
   ```

   The firmware supports specifying the protocol and port in *path_to_firmware*.

   For example:

   ```
   update firmware url=https://myhost.com/bundle
   update firmware url=https://myhost.com:1234/bundle
   ```

6. Wait for the RMC to reboot.
7. To verify the new firmware level, enter the following command:

   ```
   RMC cli> show firmware verbose
   ```

   a. Confirm that the configured complex bundle version matches the new firmware version.
   b. Confirm that the configured nPartition bundle version matches the new firmware version.
   c. Confirm that the firmware on all devices matches the new firmware version.

   NOTE: Configured nPartitions show the previous firmware version until they are rebooted.

8. To activate new system firmware on an nPartition, enter the following command:

   ```
   RMC cli> reboot npar pnum=0
   ```

NOTE: The new system firmware will not be activated on an nPartition until the **`reboot npar`** command is entered.

Downgrading firmware

About this task

CAUTION: Hewlett Packard Enterprise does not recommend downgrading to a prior firmware release. Performing this task may result in loss of data and/or system functionality.

Firmware releases include fixes for known vulnerabilities and/or updates designed to avoid future vulnerabilities. Downgrading firmware may expose you to security vulnerabilities. Some firmware releases might not support downgrading for this reason. In such cases the limitation is documented in the release notes.

Procedure

1. Apply the prior firmware version using online or offline firmware upgrade processes.

   NOTE: If you are using SUM, you cannot use the `exclude npar` option for downgrading to a previous firmware version.

2. After applying the prior firmware version, you must restart the system or partition.

More information

Updating firmware offline
Updating firmware online

Creating a crash dump file

About this task

You can request that the operating system write a crash dump file. The dump directory is specified in:

- `/etc/sysconfig/kdump` or
- `/var/crash/`

Procedure

1. Log into the HPE Superdome Flex 280 Server as the root OS user, and enter the following commands to enable the kernel crash dump service, `kdump`.

   Make sure to log into the server, not the RMC.

   ```
   # systemctl enable kdump
   # systemctl start kdump
   ```

   The HPE Foundation Software package installation process enables `kdump` by default. The preceding commands ensure that `kdump` is enabled. You can enable `kdump` on your server at any time. `kdump` must be enabled to create a crash dump file.

2. To ensure that the `uv_nmi` default action is `kdump`, enter the following command:

   ```
   # echo kdump > /sys/module/uv_nmi/parameters/action
   ```

   As an alternative to this command, you could also boot the kernel with the following parameter:

   `uv_nmi.action=kdump`

3. Use one of the following methods to send a nonmaskable interrupt (NMI) signal to start the dump.

Method 1: When logged in directly to the RMC.

a. Use the `ssh` command to connect securely.

```
# ssh administrator@flex_rmc
```

b. To send the NMI signal, enter one of the following commands:

To send the NMI signal to an individual nPartition, enter the command:

`RMC cli>` **`power nmi`** ***`pnum=0`***

Where *pnum=0* indicates the partition where the NMI signal will be sent.

Method 2: From a remote connection.

```
# ipmitool -I lanplus -H HOST -U USER -P PASSWD chassis power diag
```

The `ipmitool` command uses the following specifiers:

HOST

The RMC host name.

USER

The RMC administrator account user name.

PASSWD

The RMC administrator account password.

NOTE: IPMI is disabled by default and must be enabled in the RMC by using the `enable ipmi` command.

Managing system performance with Firmware

HPE Superdome Flex 280 Server provides nPartition attributes to control the nPartition configuration, including the ability to modify many performance settings. For more information about configuring nPartition attributes and to view the supported list of Attributes, see **Configuring and Operating HPE Superdome Flex 280 Server**.

Managing system performance with HPE Foundation Software (HFS)

HFS includes automatic boot-time optimization utilities, reliability features, and technical support tools. Designed for high performance computing, these tools help maximize HPE Superdome Flex 280 Server system performance and availability.

NOTE: HFS is required on the server running Linux.

To install HFS, see **Installing Operating Systems on HPE Superdome Flex 280 Server**.

HPE Foundation Software can be downloaded at **https://www.hpe.com/support/superdomeflex280-software**.

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

Configuring CPU frequency scaling

CPU frequency scaling enables the operating system to scale the processor frequency automatically and dynamically. Hewlett Packard Enterprise configures the CPU frequency-scaling setting on all HPE Superdome Flex 280 Server systems before they leave the factory. The default setting is assumed to be correct for most implementations as it enables your system to take advantage of the Intel Turbo Boost technology built into each processor. Control freaks can control frequencies directly rather than relying on performance profiles.

- Enter the following command to see the available CPU governor settings, and study the output to determine which governor setting is appropriate for your site:

  ```
  #cpupower frequency-info -g
  ```

  Hewlett Packard Enterprise recommends verifying the CPU governor setting is `performance`. If some other setting is shown, change it to `performance`.

- Enter the following command to see the available CPU frequencies:

  ```
  #cpupower frequency-info
  ```

  Inspect the `frequencysteps` field, and choose a minimum and/or maximum frequency.

- Create a configuration file that includes the settings you configured in this procedure.

A file must be created that includes the command you ran in this procedure. Ensure that the file has execute permission.

```
/etc/hpe-auto-config/90_cpu_frequency.sh
          # chmod 744 /etc/hpe-auto-config/90_cpu_frequency.sh
```

When the system boots, the settings in this file override the default `hpe-auto-config` settings to ensure that the settings you configured in this procedure are included after the boot.

Changing the CPU governor setting and frequency setting

About this task

The default CPU frequency governor setting can inhibit system performance. The `hpe-auto-config` utility automatically sets the CPU frequency setting to `performance` mode and sets CPUs to maximum frequency.Previously it is explained how to use the `cpupower` command to adjust the frequency governor and c-states. The following procedure explains how to override the automatic CPU frequency setting.

Procedure

1. Enter the following command to view the available CPU governor settings, and study the output to determine which governor setting is appropriate for your site:

   ```
   # cpupower frequency-info -g
   ```

   Hewlett Packard Enterprise recommends that you verify that the CPU governor setting is `performance` and if some other setting is shown, change it to `performance`.

2. Enter the following command to display the available CPU frequencies:

   ```
   # cpupower frequency-info
   ```

   Inspect the `frequency steps` field, and choose a minimum and/or maximum frequency.

3. Enter one or more of the following commands to change the governor and/or frequency settings:

   - Enter the following command to change the governor setting:

     ```
     # cpupower frequency-set -g GOVERNOR
     ```

     For *GOVERNOR*, specify the setting you want.

   - Use the `cpupower frequency-set` command to change one of the following values:

     - Both the minimum frequency and the maximum frequency
     - The maximum frequency
     - The minimum frequency

     ```
     # cpupower frequency-set -u MAX -d min
     # cpupower frequency-set -u MAX
     # cpupower frequency-set -d MIN
     ```

     For *MAX* and *MIN*, specify a value in the following format: *VALUE*[*UNIT*]

     The default *UNIT* is KHz. You can also specify a *UNIT* of Hz, MHz, GHz, or THz.

4. Enter the following command and verify that the *GOVERNOR* setting you specified appears in the `cpupower` command output in the `current policy` field:

   ```
   # cpupower frequency-info
   ```

5. Create a configuration file that includes the settings you configured in this procedure.

   A file must be created that includes the command you ran in this procedure. Ensure that the file has execute permission.

   ```
   # echo "cpupower frequency-set -g performance -u 3000MHz -d 2000MHz" > \
   /etc/hpe-auto-config/90_cpu_frequency.sh
   # chmod 744 /etc/hpe-auto-config/90_cpu_frequency.sh
   ```

   When the system boots, the settings in this file override the default `hpe-auto-config` settings to ensure that the settings you configured in this procedure are included after the boot.

More information

`cpupower`

Configuring turbo mode

Procedure

1. Make sure that you configured a governor setting.
2. Use the `cat` command to retrieve the list of available frequencies.

```
# cat /sys/devices/system/cpu/cpu0/cpufreq/scaling_available_frequencies
3301000 3300000 3200000 3100000 3000000 2900000 2800000 2700000 2600000
2500000 2400000 2300000 2200000 2100000 2000000 1900000 1800000 1700000
1600000 1500000 1400000 1300000 1200000
```

   The preceding output shows the available frequencies. The output lists frequencies in order from the highest, 3,301,000 KHz, to the lowest, 1,200,000 KHz.

   The second frequency listed is always the processor nominal frequency. This processor is a 3.3 GHz processor, so 3,300,000 KHz is the nominal frequency.

   You can also obtain the nominal frequency by entering the following command and examining the information in the model name field.

```
# cat /proc/cpuinfo
```

3. Use the `cpupower` command to set the frequency to the nominal frequency of 3.3 GHz plus 1 MHz.

   That is, specify a frequency of 3,301 MHz.

```
# cpupower frequency-set -u 3301MHz
```

   Later, if you want to disable turbo mode, enter the following command to set the maximum frequency back to the nominal frequency:

```
# cpupower frequency-set -u 3300MHz
```

More information

Changing the CPU governor setting and frequency setting

Monitoring system performance

You can use Linux utilities, HPE Foundation Software (HFS) utilities, and open-source utilities to monitor system performance.

The Linux utilities include `w`, `ps`, `top`, `vmstat`, `iostat`, and `sar`.

The HFS utilities are **`gr_systat`**, **`nodeinfo`**, and **`topology`**.

Consistently naming network cards

About this task

You can use HPE Foundation Software to consistently name NICs (network cards) in the system based on their physical chassis location.

Hewlett Packard Enterprise recommends enabling this feature to ensure consistent NIC naming if a NIC fails, is moved or replaced, or when firmware is updated.

The naming scheme uses the *GEOID* of the chassis to identify the NIC.

For example, the NIC name with `UV_GEOID_NIC_NAMES=yes` and `UV_GEOID_NIC_SHORT_NAMES=no` is `r001u01p3i07p0`, where r=rack, u=rack unit, p=cpu, i=slot, and p=port.

With, `UV_GEOID_NIC_SHORT_NAMES=yes` will not contain the cpu information and the same NIC will be `r001u01i07p0`.

Procedure

1. Access the system using the RMC.

   NOTE: Accessing the system using the RMC is recommended as renaming NICs may result in invalidating existing network configuration.

2. Edit the `/etc/sysconfig/hpe-auto-config` file and change the `UV_GEOID_NIC_NAMES` entry to yes.
3. Confirm the changes by entering the `hpe-auto-config` command.
4. Restart the system.
5. Update your network settings as appropriate.

   NOTE: GeoID NIC names are implemented using `/etc/systemd/network/10-r[0-9][0-9][0-9]*.link` files. If you add or remove NICs in the chassis, remove those files and re-enter the `hpe-auto-config` command.

Activating an extended tuning script

About this task

Use HPE Superdome Flex 280 Server to select and activate an extended tuning script for your system. These scripts optimize performance for applications such as SAP HANA OS.

This document describes a general procedure for using tuning scripts. For more detailed information, see *Configuration Guide for HPE Superdome Flex Solutions for SAP HANA with 3PAR All Flash Storage*.

Procedure

1. Verify boot parameters needed for your system configuration, and make changes as necessary.
2. Create and set your parameters in the configuration script file.
   - For SLES, use the *HPE-Recommended_OS_settings.conf* configuration file located at `/etc/saptune/extra` directory. If the file does not exist, create the file.
   - For RHEL, use the *tuned.conf* configuration file located at `/etc/tuned/sap-hpe-hana` directory. If the file does not exist, create the file.
3. Verify that tuning settings are applied by using the `sysctl` command.

Additional HFS utilities

There are additional HFS commands and utilities available that typically require no user involvement. Hewlett Packard Enterprise technical support staff members might guide you in the use of these commands when troubleshooting or tuning.

- **hpe-auto-config**
- **hpe_irqbalance**

HPE Foundation Software (HFS) commands

HPE Foundation Software (HFS) includes automatic boot-time optimization utilities, reliability features, and technical support tools. These tools are initiated and managed through OS-level commands to the HFS interface.

Selected details for commonly used HFS commands are included in this guide.

More detailed descriptive and usage information is available in the manpage content for all HFS commands.

cpupower

`cpupower` is not a HFS command. The OS vendor (package cpupower on SLES, kernel-tools on RHEL) provides this command. `cpupower` is mentioned here as it is useful to set performance or power preferences.

Syntax

```
cpupower frequency-info [-g]
cpupower frequency-set [-u MAX] [-d MIN] [-g GOVERNOR]
```

Description

Enables viewing or changing the CPU operating frequency and power governor settings.

Options

`frequency-info`

Displays the available CPU operating frequencies

`frequency-info -g`

Displays the available CPU power governor settings

`frequency-set`

Changes the CPU operating frequency

`frequency-set -g`

Changes the CPU power governor setting

Specifiers

`-u MAX`

Specify the maximum CPU frequency in the following format: `value[unit]`. The default unit is KHz. To specify a frequency in a unit other than KHz, add **`Hz`**, **`MHz`**, **`GHz`**, or **`THz`** after the value.

`-d MIN`

Specify the minimum CPU frequency in the following format: `value[unit]`. The default unit is KHz. To specify a frequency in a unit other than KHz, add **`Hz`**, **`MHz`**, **`GHz`**, or **`THz`** after the value.

`-g GOVERNOR`

Specify the power governor setting. Possible power governor settings are:

- `ondemand` (default) dynamically switches between the available CPUs if at 95% of CPU load. HPE does not recommend this setting.
- `performance`. This governor setting runs the CPUs at the maximum frequency.

- `conservative`. This governor setting dynamically switches between the available CPUs if at 75% of CPU load.
- `powersave`. This governor setting runs the CPUs at the minimum frequency.
- `userspace`. This governor setting runs the CPUs at user-specified frequencies.

Usage

`cpupower frequency-info`

Displays the available CPU frequencies.

`cpupower frequency-info -g`

Displays the available CPU governor power settings.

`cpupower frequency-set -g` *`GOVERNOR`*

Changes the power governor setting, where *GOVERNOR* is the required setting.

`cpupower frequency-set -u` *`MAX`*

Changes the maximum CPU frequency.

`cpupower frequency-set -d` *`MIN`*

Changes the minimum CPU frequency.

`cpupower frequency-set -u` *`MAX`* `-d` *`MIN`*

Changes both the maximum and minimum CPU frequencies.

gr_systat

Syntax

`gr_systat`

Description

Generates information that includes the following:

- CPU and memory activity
- Input or output traffic statistics for each I/O device
- Other system statistics

Displays the following for the system as a whole and for each node:

- CPU utilization percentage
- I/O wait times
- Interrupt requests (IRQs)
- Memory utilization

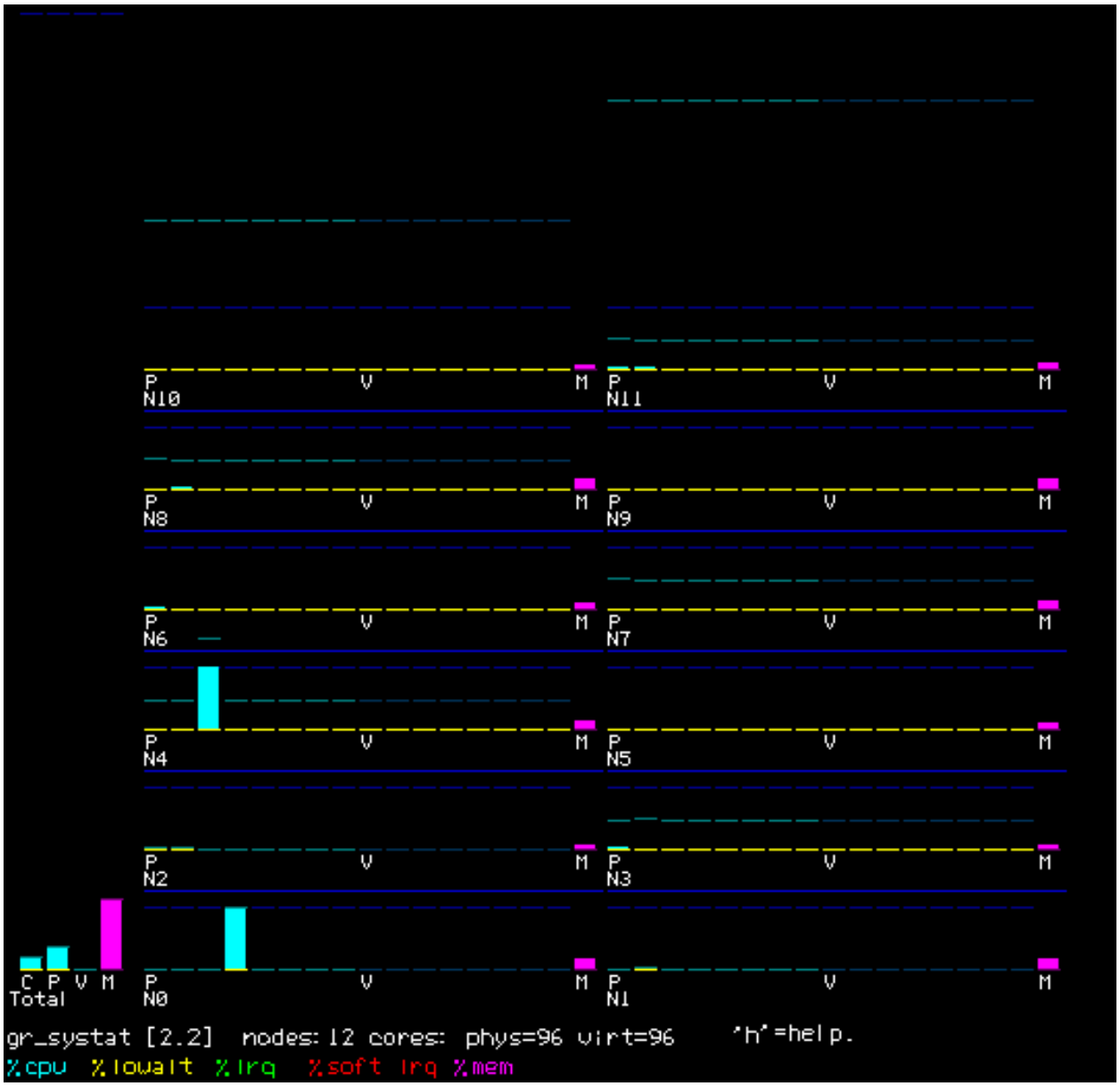
The `gr_systat` command is a useful performance monitoring tool that can help you to identify malfunctioning hardware.

Usage

The `gr_systat` command includes several command parameters that enables you to control the appearance of the `gr_systat` command output. You can save these parameters to a configuration file for future use. For more information, see the `gr_systat` manpage.

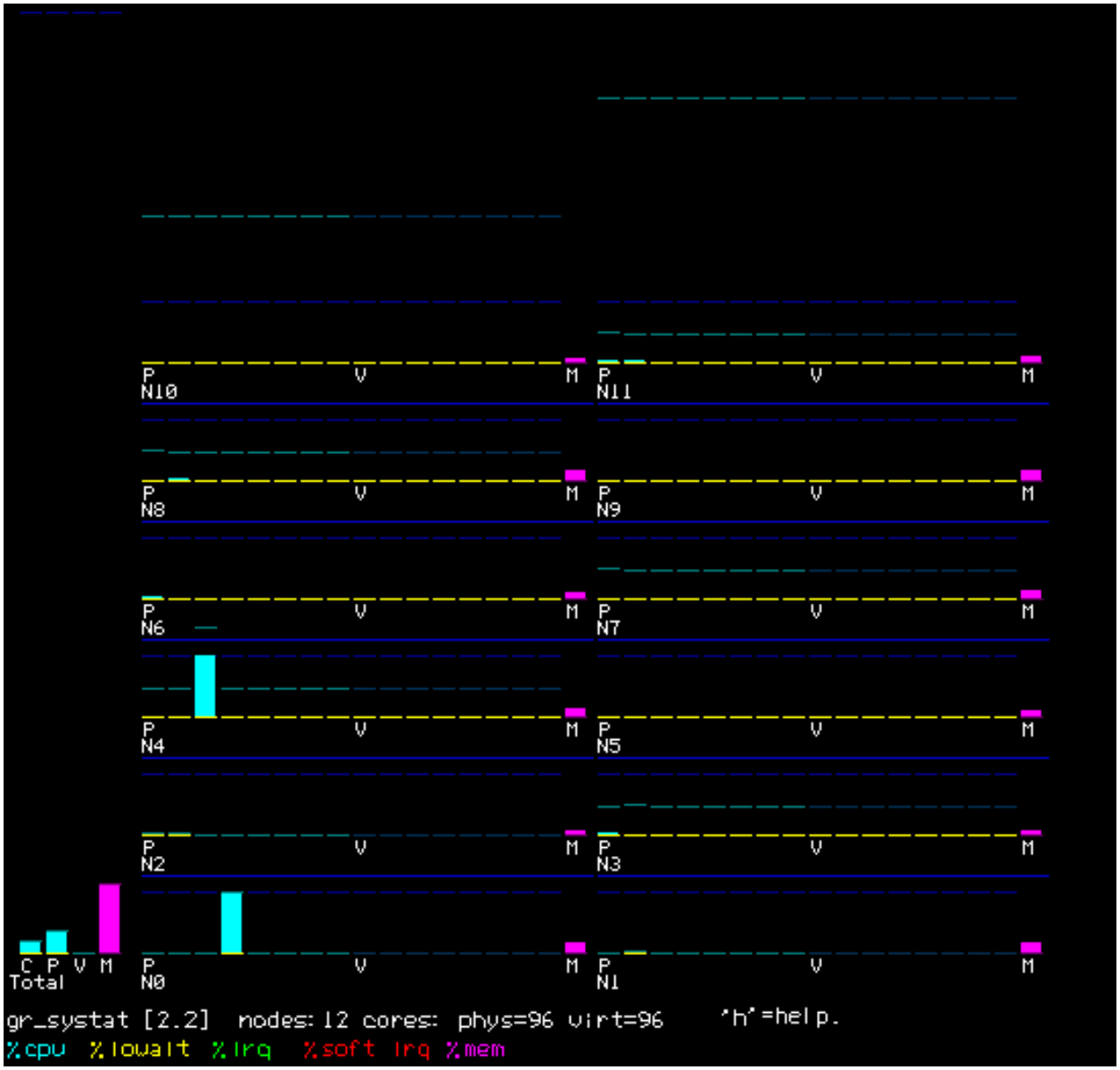
Example 1

Figure 3: CPU and memory utilization in real time



Example 2

Figure 4: I/O device use in real time



hpe-auto-config

Syntax

`hpe-auto-config`

`hpe-auto-config -n`

`hpe-auto-config -d`

Description

The `hpe-auto-config` package is a collection of configuration utilities and services. These utilities perform the following functions to ensure that systems are optimally configured:

- Monitor system attributes.
- Update configuration options and/or kernel parameters appropriately if an attribute changes.

Options

`hpe-auto-config` functions are accessed through script files in the following directories:

`/etc/hpe-auto-config/*`

Executable files in this directory are executed by `hpe-auto-config` in lexical order. A number of scripts are included and custom scripts may be added. A configuration action may be disabled by removing execute permissions from the script that contains it.

`/etc/hpe-auto-config/boot_entry_blacklist`

List of regular expressions defining which boot entries `hpe-auto-config` are not edited. Any “rescue” boot entry is not edited by default.

`/etc/modprobe.d/hpe-auto-config.conf`

Destination for kernel module blacklist directives.

`/etc/sysconfig/hpe-auto-config`

Controls behavior of various HPE configuration actions.

`/usr/sbin/hpe-auto-config`

Main command for running `hpe-auto-config`.

`/var/log/hpe-auto-config.log`

Each script and shared library function logs its results to this file. Consult this log for a (partial) list of actions taken and for and warnings or errors.

`hpe-auto-config` can also use the following options:

`-n (--dry-run)`

Performs all processing but does not edit `bootloader_config`.

`-d (--verbose)`

Adds detailed output to `/var/log/hpe-auto-config.log`.

Usage

The `hpe-auto-config` package applies a number of required and suggested edits to the Linux command-line on top of default and user-defined parameters. Consult documentation for the installed `bootloader` program for instructions on adding or removing Linux boot parameters.

For best results, follow this procedure for changing Linux boot parameters:

1. Follow the documentation for your distribution for adding Linux boot parameters. For grub2 systems, it is recommended to add the `boot` option to */etc/default/grub*.
2. To remake the grub boot configuration, restart `hpe-auto-config`.

```
# systemctl restart hpe-auto-config
```

3. Check for cthonflicts and verify the boot configuration file, `/boot/grub2/grub.cfg (SLES)`, or `/boot/efi/EFI/redhat/grub.cfg (RHEL)`.

Read the kernel command-line in the `grub.cfg` and verify that it contains the option you specified. If any of your boot options conflict with HPE required options, it shows a `syslog` warning message calling out the offending parameters.

```
INFO: boot parameter X in /etc/default/grub conflicts with rule Y
```

To resolve this conflict, remove *X* from */etc/default/grub* and create a custom `hpe-auto-config` script to override the rule *Y*. For instructions and more information, see the examples in `hpe-auto-config(1)` manpage.

Overriding a required boot parameter example

1. Add `numa_balancing=enable` to the Linux command line.
2. Add `numa_balancing=enable` to `/etc/default/grub` and restart the `hpe-auto-config`.

```
# echo GRUB_CMDLINE_LINUX+=" numa_balancing=enable" >> /etc/default/grub
# systemctl restart hpe-auto-config
...
hpe-auto-config: 2022/10/05 21:23:42 20_sap_hana.sh: INFO: boot parameter
numa_balancing in /etc/default/grub conflicts with rule replace numa_balancing=disable
```

3. To override, create an executable file `/etc/hpe-auto-config/21_numa_balancing` with this content:

```
source /usr/lib64/hpe-auto-config/shlib
boot_option replace numa_balancing=enable
```

4. Restart `hpe-auto-config` and verify the command-line in the `grub.cfg` file.

   The conflict warning continues until `numa_balancing=enable` is removed from */etc/default/grub*.

5. Enter ***nano /etc/default/grub*** to update */etc/default/grub* before restarting `hpe-auto-config`.

```
# nano /etc/default/grub
# systemctl restart hpe-auto-config
```

hpe_irqbalance

Syntax

`hpe_irqbalance [`*OPTION*`]...`

Description

This utility controls interrupt request (IRQ) affinity. The daemon starts when a system boots. If a device generates IRQs, `hpe_irqbalance` attempts to distribute the interrupts to the CPUs that are on the same chassis (or node) upon which the interrupt originated.

Options

`-d`

Run interactively in debug mode.

`-o`

Run in one-shot mode. This mode distributes the currently existing IRQs once and exits rather than continually polling for new IRQs.

`-t`

Specifies the `sleeptime` in seconds between polling loops after which `hpe_irqbalance` polls for IRQs for which affinity has not been set. This option has no effect if `-o` is specified.

Specifiers

OPTION

`hpe_irqbalance_oneshot`

Same as the `-o` option.

hpe_irqbalance_sleeptime

Same as the `-t` option.

Usage

This utility starts in every two minutes by default.

1. To change the interval, set `HPE_IRQBALANCE_SLEEPTIME` in `/etc/sysconfig/hpe_irqbalance` to the desired number of seconds.
2. Restart `hpe_irqbalance` or reboot your system.

   The `hpe-auto-config` package automatically configures the `hpe_irqbalance` utility.

For more information, see the `hpe_irqbalance(8)` manpage.

nodeinfo

Syntax

```
nodeinfo [OPTION...]
```

Description

Monitors per-node memory statistics.

Options

-l

Print output line by line to stdout, instead of using the full screen display.

-s

Limit the number of data samples that `nodeinfo` outputs.

-i -t

Wait `i` seconds between printing each data sample.

-o

Sets the starting output options.

k

Show sizes in KB.

m

Show sizes in MB.

p

Show sizes in pages.

H

Show hugepage info.

-h

Show help message.

-v

Show verbose output.

Usage

`nodeinfo` is a tool for monitoring per-node Superdome Flex Grid memory statistics. The `nodeinfo` tool reads `/sys/devices/system/node/*/meminfo` and `/sys/devices/system/node/*/numastat` on the local system to gather Superdome Flex Grid memory statistics.

For more information on the `nodeinfo` command, see the NODEINFO(1) manpage.

From an interactive `nodeinfo` session, enter **h** for a help statement. For example:

```
Display memory statistics by node.
        q   quit
        +   Increase starting node number. Used only if more nodes than will
            fit in the current window.
        -   Decrease starting node number. Used only if more nodes than will
            fit in the current window.
        b   Start output with node 0.
        e   Show highest node number.
        k   show sizes in KB.
        m   show sizes in MB.
        p   show sizes in pages.
        t   Change refresh rate.
        A   Show/Hide memory policy stats.
        H   Show/Hide hugepage info.
        L   Show/Hide LRU Queue stats.
Field definitions:
        hit - page was allocated on the preferred node
        miss - preferred node was full. Allocation occurred on THIS node
               by a process running on another node that was full

        foreign - Preferred node was full. Had to allocate somewhere
                  else.

        interlv - allocation was for interleaved policy

        local - page allocated on THIS node by a process running on THIS node
        remote - page allocated on THIS node by a process running on ANOTHER node


  (press any key to exit from help screen)
```

Example

Sample memory statistics from the `nodeinfo` command are as follows:

```
# nodeinfo
Memory Statistics flex280-sys
        ------------ Per Node MB --------------------------   ------ Prefferred Alloc ------- -- Loc/Rem ---
node    Total   Free    Used    Dirty   Anon    Slab    Shmem   hit     miss    foreign interlv local   remote
0       385504  384375  1129    0       46      373     12      6       0       0       0       6       0
1       387063  386682  382     0       3       110     0       96      0       0       0       96      0
2       387063  386600  463     0       8       87      1       0       0       0       0       0       0
3       387063  386719  344     0       3       88      1       6       0       0       0       6       0
4       387063  386804  260     0       0       67      0       0       0       0       0       0       0
5       387029  386709  321     0       1       93      1       0       0       0       0       0       0
6       387063  386802  262     0       0       66      1       0       0       0       0       0       0
7       386543  386178  366     0       14      111     2       343     0       0       0       343     0
TOT     3094393 3090867 3526    0       75      995     18      451     0       0       0       451     0
```

topology

Syntax

```
topology [OPTION ...]
```

Description

Provides topology information about your system. Application programmers can use the `topology` command to help optimize execution layout for their applications.

Options

If none of the options are specified, then all information is displayed. Any combination of options may be specified to limit the amount of information displayed. Option names may be shortened to their unique values.

`--cpus`

Show detailed information for the CPUs.

`--cops`

Show detailed information for attached coprocessors.

`--disks`

Show detailed information for the disk controllers including SCSI and Serial Attached SCSI controllers.

`--gfx`

Show detailed information for graphics devices including both VGA (graphics) GPUs and GP (CUDA) GPUs.

`--io`

Displays information about I/O devices. (`--disks`, `--gfx`, `--networks`)

`--networks`

Show detailed information for the network devices including Ethernet, Fibre Channel, and InfiniBand controllers.

`--nodes`

Show detailed information for the system nodes. With verbose = 1, it will also show which CPUs are resident on this node (blade). With routered configurations, the blades may not be numbered the same as the physical ordering.

`--routers`

Show detailed information for the system routers.

`-s`

Display a system summary (default).

Other operational modifiers are:

`--affinity`

Show smp_affinity for each IRQ (implies arg --irqs). With verbose set, it will also show the current interrupt count for each IRQ.

`-d`

Increase the debug level.

`--debug=n`

Set the debug level to `n`.

--get_node=<device>

Returns the lowest local node associated with where the device is installed. This information is useful for placing an application on the same node as the device, often improving DMA performance. With verbose set, it will return all nodes that are local to the device.

--get_cpus=<device>

Returns a list of cpus associated with where the device is installed. Normally returns a cpulist (cpuJ-cpuK,cpuM-cpuN). If verbose, returns a comma-separated list of individual cpus (cpuJ,cpuJ+1,...).

--noheaders

Do not display the column headers. For those cases where multiple devices are on the same node, this option causes the node info to be displayed on every line. This output is useful for parsing the output by other programs. The format of the data may change and the user is advised to use the `--version` option to maintain compatibility with each new version.

--irqs

Shows which IRQs are assigned to the devices. With verbose set, it will also show the current interrupt count for each IRQ. Implies arg `--io` if none of "`--disks`, `--gfx`, or `--networks`" set.

--nox

Do not display the X Server Display column when displaying I/O. This output is implied if `--gfx` is not present or if there is only the BASE I/O VGA installed on the system and it is not configured in the xorg configuration file.

-tt

Forces use /var/run/sgi_uv/topology if available to obtain system topology information.

--lspci=file

Use file to obtain PCI device information. The file will contain output from the lspci command in machine-readable format.

-v

Increase the verbosity.

--verbose=n

Set the verbosity to 'n'.

--version

Display topology version.

--xorgconf=file

Use file to obtain X display information instead of the standard `/etc/X11/xorg.conf` file.

Specifiers

gfxtopology

Same as the `gfx` option to `topology`.

For more information about the `topology` command, see the TOPOLOGY(1) manpage content.

Example 1

The `topology` command includes many options. For more information, type `topology --help` on the command line.

The following `topology` command shows the system summary:

```
# topology
System type: Superdome Flex 280
System name: flex280-rmc-009.example.com
Serial number: 5UF9511900
       2 Chassis
     288 CPUs (online: 0-287)
       8 Nodes
    3021 GB Memory Total
      16 PCIe Slots
       2 PCIe Cards
       1 Co-processor
       2 Fibre Channel Controllers
       4 Network Controllers
       1 SATA Storage Controller
       1 USB Controller
       1 VGA GPU
       1 RAID Controller
```

Example 2

The following `topology` command explicitly requests the system summary and also shows node and CPU information:

```
# topology --summary --nodes --cpus
System type: Superdome Flex 280
System name: flex280-rmc-009.example.com
Serial number: 5UF9511900
       2 Chassis
     288 CPUs (online: 0-287)
       8 Nodes
    3021 GB Memory Total
      16 PCIe Slots
       2 PCIe Cards
       1 Co-processor
       2 Fibre Channel Controllers
       4 Network Controllers
       1 SATA Storage Controller
       1 USB Controller
       1 VGA GPU
       1 RAID Controller

 Node    Location    Threads     Memory
---------------------------------------
    0   r001u01p0         36     376 GB
    1   r001u01p1         36     377 GB
    2   r001u01p2         36     377 GB
    3   r001u01p3         36     377 GB
    4   r001u06p0         36     377 GB
    5   r001u06p1         36     377 GB
    6   r001u06p2         36     377 GB
    7   r001u06p3         36     377 GB

CPU       Location PhysID CoreID APIC-ID Family Model Speed L1(KiB) L2(KiB) L3(KiB)
-------------------------------------------------------------------------------------
  0 r001u01p0c00t0      0      0       0      6    85  1598 32d/32i    1024   25344
  1 r001u01p0c01t0      0      1       2      6    85  3440 32d/32i    1024   25344
  2 r001u01p0c02t0      0      2       4      6    85  2037 32d/32i    1024   25344
  3 r001u01p0c03t0      0      3       6      6    85  2047 32d/32i    1024   25344
.
.
.
```

Example 3

The following `topology` command shows the interrupt requests that are assigned to devices:

```
# topology --irq
Index Location    NASID  PCI Address           IRQ(s)    Device
-------------------------------------------------------------------
    0 r001u01s00   0002  0000:00:11.5             30   Intel Lewisburg SSATA Controller [AHCI]
    .          .      .  0000:00:14.0             29   Intel Lewisburg USB 3.0 xHCI Controller
    .          .      .  0000:00:17.0             31   Intel C600/X79 SATA RAID Controller
    .          .      .  0000:00:1f.5              0   Intel Lewisburg SPI Controller
    .          .      .  0000:01:00.0             19   Emulex x1 PCIe Gen2 Bridge[Pilot4]
    .          .      .  0000:02:00.0             19   Matrox MGA G200e [Pilot] ServerEngines (SEP1)
    .          .      .  0000:02:01.0            255   Emulex ServerView iRMC HTI
    .          .      .  0000:c3:00.0    33-39,42-111   Intel Ethernet Connection X722 for 10GBASE-T
    .          .      .  0000:c3:00.1      28,163-291   Intel Ethernet Connection X722 for 10GBASE-T
    .          .      .  0000:c3:00.2      28,292-420   Intel Ethernet Connection X722 for 10GBASE-T
    .          .      .  0000:c3:00.3      28,421-549   Intel Ethernet Connection X722 for 10GBASE-T
```

Example 4

The following `topology` command uses the `-v` option, which includes interrupt count information:

```
# topology --irq -v
Index Location    NASID  PCI Address           IRQ(s)     INTCNT     Device
-------------------------------------------------------------------------------
    0 r001u01s00   0002  0000:00:11.5             30       1941    Intel Lewisburg SSATA Controller [AHCI]
    .          .      .  0000:00:14.0             29        795    Intel Lewisburg USB 3.0 xHCI Controller
    .          .      .  0000:00:17.0             31          0    Intel C600/X79 SATA RAID Controller
    .          .      .  0000:00:1f.5              0          0    Intel Lewisburg SPI Controller
    .          .      .  0000:01:00.0             19          0    Emulex x1 PCIe Gen2 Bridge[Pilot4]
    .          .      .  0000:02:00.0             19          0    Matrox MGA G200e [Pilot] ServerEngines (SEP1)
    .          .      .  0000:02:01.0            255          0    Emulex ServerView iRMC HTI
    .          .      .  0000:c3:00.0    33-39,42-111       1856    Intel Ethernet Connection X722 for 10GBASE-T
    .          .      .  0000:c3:00.1      28,163-291          0    Intel Ethernet Connection X722 for 10GBASE-T
    .          .      .  0000:c3:00.2      28,292-420          0    Intel Ethernet Connection X722 for 10GBASE-T
    .          .      .  0000:c3:00.3      28,421-549          0    Intel Ethernet Connection X722 for 10GBASE-T
```

Example 5

The following `topology` command shows local CPU and node information for each device. You can use the output from this command to help you place applications close to their I/O device for better direct memory access performance.

```
# topology --io -v --nox
 Location       PCI Address        Local CPUS    Device
 ------------------------------------------------------------------
 r001u01p0i00  0000:00:11.5     0-17,144-161    Intel Lewisburg SSATA Controller [AHCI]
             .  0000:00:14.0     0-17,144-161    Intel USB controller device a22f [*]
             .  0000:00:16.3     0-17,144-161    Intel Serial controller device a23d [*]
             .  0000:00:17.0     0-17,144-161    Intel C600/X79 SATA RAID Controller
             .  0000:00:1f.5     0-17,144-161    Intel Lewisburg SPI Controller
             .  0000:01:00.0     0-17,144-161    Intel I210 Gigabit Network Connection
             .  0000:02:00.0     0-17,144-161    Intel I210 Gigabit Network Connection
             .  0000:03:00.0     0-17,144-161    Emulex x1 PCIe Gen2 Bridge[Pilot4]
             .  0000:04:00.0     0-17,144-161    Matrox MGA G200e [Pilot] ServerEngines (SEP1)
             .  0000:04:01.0     0-17,144-161    Emulex ServerView iRMC HTI
 r001u01p1i08  0000:58:00.0    18-35,162-179    QLogic ISP2722-based 16/32Gb Fibre to PCIe Adapter
             .  0000:58:00.1    18-35,162-179    QLogic ISP2722-based 16/32Gb Fibre to PCIe Adapter
 r001u01p3i07  0000:ed:00.0    54-71,198-215    QLogic FastLinQ QL41000 10/25/40/50GbE Controller
             .  0000:ed:00.1    54-71,198-215    QLogic FastLinQ QL41000 10/25/40/50GbE Controller
```

Rack management controller (RMC) commands

This chapter explains the RMC commands that are available to you when you log in as the `administrator` user.

The remote management commands use the following terminology:

- The term **HPE Superdome Flex 280 Server system** includes the server, RMC, and the Baseboard Management Controllers.
- The term **HPE Superdome Flex 280 Server** refers only to the server component of the system. The server is enclosed within each chassis. The RMC and the BMCs are not part of the server itself.

The following RMC commands provide command information from the RMC command line:

- `apropos` *`command`*

  The `apropos` command helps you search for RMC commands, by displaying a list of all commands that include a text string you specify, either in a command name or in command syntax.

  For example, to retrieve command information that pertains to SNMP traps, enter the following:

  ```
  RMC cli> apropos snmp

  add snmp forward_address=FORWARD_ADDRESS [port=FORWARD_PORT] [protocol=PROTOCOL]
  clear snmp_forwarding
  remove snmp forward_address=FORWARD_ADDRESS
  set snmp forward_address=FORWARD_ADDRESS [port=FORWARD_PORT] [protocol=PROTOCOL]
  show snmp
  show snmp forward_address
  ```

- `help` *`command`* or *`command`*

  When you enter an incomplete command at the RMC command prompt, the system returns the correct syntax and options for the command. For *command*, specify the name of any RMC command.

  For example, to display information about the `enable` command, enter either of the following commands at the prompt:

  ```
  RMC cli> enable

  Usage: enable
         enable autopower
         enable cert_checking
         enable cli_session_timeout
         enable http
         enable https
         enable ipmi
         enable ldap
         enable ler vendor_id=VENDOR_ID device_id=DEVICE_ID
         enable pcie_error_isolation chassis=GEOID (all | io_slot=IO_SLOT [IO_SLOT ...])
         enable predictive_mem_health
         enable power_redundancy
         enable script_mode
         enable ssh
         enable tpm [pnum=0]
         enable zeroconf

  RMC cli> help enable
  Usage: enable
         enable autopower
         enable cert_checking
         enable cli_session_timeout
         enable http
         enable https
  ```

```
      enable ipmi
      enable ldap
      enable ler vendor_id=VENDOR_ID device_id=DEVICE_ID
      enable pcie_error_isolation chassis=GEOID (all | io_slot=IO_SLOT [IO_SLOT ...])
      enable predictive_mem_health
      enable power_redundancy
      enable script_mode
      enable ssh
      enable tpm [pnum=0]
      enable zeroconf
```

acquit

Syntax

```
acquit [physloc=PHYSLOC_STR | chassis=GEOID | pnum=0 | all]
```

Description

Releases the indicted and deconfigured status of a specified component manually in the following situations:

- After you examine the log files and replace the indicted hardware.
- When you suspect that the hardware is indicted erroneously.

Specifiers

PHYSLOC_STR

Specify short form string.

GEOID

Specify the ID number of a chassis.

Usage

- The `acquit physloc=`**PHYSLOC_STR** command acquits all indicted or deconfigured hardware at the specified physical location.
- The `acquit chassis=`***GEOID*** command acquits all indicted or deconfigured hardware in the specified chassis.
- The `acquit pnum=`**0** command acquits all indicted or deconfigured hardware in the specified nPartition.
- The `acquit all` command acquits all indicted or deconfigured hardware in the complex.

Example

The following example shows how to retrieve a list of indictments and how to acquit an indictment:

```
RMC cli> show indict


==== r001u01b ====

  FFFF040101FFFF63 rack1/chassis_u1/chassis_fan4

    Indicted: Yes
                2021-08-17T19:24:58Z  Reason ID: 302
            Summary: Fan reported to be running slowly or stopped
            Cause: A fan is not running at normal speed.  There may be
                something obstructing the airflow, a blocked fan or a
```

```
                fan failure.
            Action: Check the enclosure for obstructions to airflow
                and ensure the fans are installed properly.  If the
                problem persists, replace the fan. After replacing the
                faulty fan, perform an acquittal from the RMC command
                line.

RMC cli> acquit physloc=FFFF040101FFFF63
```

add

Syntax

`add certificate`

`add certificate ca file=`*`FILENAME`*

`add certificate signed [chassis=`*`GEOID`*`]`

`add dns [ipaddress=`*`IPADDRESS`*` | search=SEARCH_NAME]`

`add host name=`*`NAME`*` ipaddress=`*`IPADDRESS`*

`add ldap_group name=`*`GROUP_NAME`*` role={administrator,monitor,operator}`

`add location [rack=`*`RACK`*`] [bmc_id=`*`BMC_ID`*`] [module={rmc,bmc}] upos=`*`UPOS`*

`add snmp forward_address=`*`FORWARD_ADDRESS`*` [port=`*`FORWARD_PORT`*`] [protocol=`*`PROTOCOL`*`]`

`add sshkey key=`*`PUBLIC KEY`*

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

Description

Specifies system characteristics or users to the system.

Specifiers

FILENAME

Specify the name of the file that provides the Certificate Authority.

IPADDRESS

Specify the IP address of a DNS server at your site.

FORWARD_ADDRESS

Specify the IP address of a local computer or device to receive SNMP alerts.

GEOID

Specify the ID number of the chassis to receive the signed certificate.

GROUP_NAME

Specify the LDAP directory group.

PUBLIC KEY

Specify the `ssh` public key.

USERNAME

Specify the name of a new user that you want to add to the system. The following are rules regarding the *USERNAME* specification:

- You can add a maximum of 30 users.
- *USERNAME* must begin with a letter and is case-sensitive.
- *USERNAME* must be unique to all other user names and group names.
- *USERNAME* can be 2 to 20 characters long and can include all alphanumeric characters, the dash, and the underscore.
- Certain user names are reserved for the RMC. The reserved user names are as follows:

User name	Reserved on RMC
adminstrator	X
backup	
bin	
daemon	X
dbus	
ftp	
haldaemon	
logger	X
mail	
nobody	
ntp	X
operator	
proxy	
root	X
sshd	X
sys	
sysadmin	X
sync	
www-data	

When you create a user, the system also prompts you to create a password. The password can be from 6 to 64 characters long (default minimum is 8 characters) and can include all printable characters.

Usage

- The `add certificate ca file=`*`FILENAME`* command adds a specified Certificate Authority file for a signed certificate.
- The `add certificate signed` command adds a default-generated signed security certificate to the RMC.
- The `add certificate signed [chassis=`*`GEOID`*`]` command adds a signed security certificate to the specified chassis.
- The `add dns ipaddress=`*`DNS_IPADDRESS`* command specifies your site domain name service to the RMC.

- The `add host name=NAME ipaddress=IPADDRESS` command specifies the host name for the RMC.
- The `add ldap_group name=GROUP_NAME role={administrator,monitor,operator}` command specifies the LDAP group for the RMC and the user role for the RMC.
- The `add location [rack=RACK] [bmc_id=BMC_ID] [module={rmc,bmc}] upos=UPOS` command specifies the physical location of the RMC.
- The `add snmp forward_address=FWD_IPADDRESS` command specifies an IP address of the device to which you want the RMC to send SNMP alerts.
- The `add sshkey key=PUBLIC_KEY` command adds the provided SSH public key to the RMC.
- The `add user name=USERNAME` command adds a user to the RMC.

apropos

Syntax

`apropos STRING_TO_MATCH [STRING_TO_MATCH ...]`

Description

Retrieves a list of commands that include the string you specify.

Specifiers

STRING

Specify a topic area, a command name, or another word for which you want the *apropos* command to display information.

Example 1

```
RMC cli> apropos snmp
add snmp forward_address=FORWARD_ADDRESS [port=FORWARD_PORT] [protocol=PROTOCOL]
clear snmp_forwarding
remove snmp forward_address=FORWARD_ADDRESS
set snmp forward_address=FORWARD_ADDRESS [port=FORWARD_PORT] [protocol=PROTOCOL]
show snmp
show snmp forward_address
```

Example 2

```
RMC cli> apropos disable
disable
disable autopower
disable cert_checking
disable cli_session_timeout
disable http
disable https
disable ipmi
disable ipmi all
disable ipmi bt
disable ipmi lan
disable ipv6
disable ldap
disable ler vendor_id=VENDOR_ID device_id=DEVICE_ID
disable pcie_error_isolation chassis=GEOID (all | io_slot=IO_SLOT [IO_SLOT ...])
disable power_redundancy
disable predictive_mem_health
disable script_mode
disable ssh
disable tpm [pnum=0]
disable zeroconf
modify npar [pnum=0] [secure_boot={on,off}] [dcpmm_security={enabled,disabled}] [dcpmm_passphrase]
```

```
set ipmi_watchdog (disabled | os_managed)
show ler [enable] [disable]
RMC cli>
```

backup

Syntax

```
backup firmware [chassis=CHASSIS]
```

Description

Back up the current firmware.

Specifiers

CHASSIS

Specify the GEOID identifier of one chassis on which to do the backup action. Default: all chassis.

Usage

For the sake of resiliency, different firmware "silos" exists. If for some reason the firmware gets corrupted, another silo can boot if needed. This command provides a way to back up the currently active firmware to the other silos. If the backup silos have firmware older than current active firmware, run this command to update them.

For more information about firmware silos, see, `show firmware silos` command.

Example

```
RMC cli> backup firmware

Chassis r001u01b: Checking preconditions ........
Chassis r001u06b: Checking preconditions .......
Chassis r001u01b: Backup to silo #3 (Recovery) .......
Chassis r001u06b: Backup to silo #1 (Secondary) ......
Chassis r001u06b: Backup to silo #3 (Recovery) ......

RMC cli>
```

baseiolist

Syntax

```
baseiolist
```

Description

Returns the IP address and the MAC address of the BaseIO BMC.

Usage

The IP address is needed as input to the JViewer software. You can use JViewer to install an operating system on an HPE Superdome Flex 280 Server from a remote location.

Example

```
RMC cli> baseiolist

P000 [r001u01b]:   192.168.1.1     [01:01:01:01:01:01]
                   fddd:6775:1110:93:a00:69ff:fe17:a1e1/64 Scope:Global
                   fe80::a00:69ff:fe17:a1e1/64 Scope:Link
                   fddd:6775:1110:93:1::1c8/64 Scope:Global
```

cancel autopower

Syntax

```
cancel autopower
```

Description

Prevents the HPE Superdome Flex 280 Server from applying power to the server components after a power off.

Usage

When power is restored after a power outage, the power to the RMCs and the BMCs is restored automatically. If the autopower capability is enabled, the system restores power to the servers automatically, too. If you use this command to cancel the autopower capability, the system does not restore power to the servers automatically after the power is restored.

clear

Syntax

```
clear cae (all | complex | pnum=0)

clear dns

clear host

clear ldap [server] [port] [login] [binddn] [bindpw] [sid] [basedn]
[userfilter] [userdn] [groupfilter] [groupdn]

clear logs

clear logs console target={BMC_GEOID |P0}

clear logs debug

clear logs error type=SEVERITY [pnum=0]

clear logs rcu [file=FILENAME]

clear logs hel [target=TARGET]

clear logs iel [pnum=0]

clear logs sel [target=TARGET]

clear ntp
```

```
clear remote_log_server
clear rmc [product_data] [verbose]
clear snmp_forwarding
clear sshkey
```

Description

Removes or erases settings, files, or other entities.

Specifiers

FILENAME

Specify the name of the file to remove.

TARGET

Specify the identifier for one of the system RMCs. The `show complex` command returns system information that includes BMC identifiers.

SEVERITY

Specify one of the following severities: `MCA`, `CMC`, or `ALL`.

GEOID

Specify the identifier of the log.

Usage

- The `clear dns` command removes the domain name service (DNS) setting on the RMC.
- The `clear ldap` command clears LDAP configuration attributes.
- The `clear logs console` command removes the console logs.
- The `clear logs debug` command removes files generated by the `collect debug` command.
- The `clear logs hel` command removes the hardware error logs (HEL).

  If you specify the `target=`*`target`* argument, the command removes the logs on the specified BMC. For example:

  ```
  RMC cli> clear logs hel target=r001u01b
  ```

- The `clear logs iel` command removes the integrated event log (IEL).
- The `clear logs sel` command removes the system event log (SEL).

  If you specify the `target=`*`TARGET`* argument, the command removes the system event log on the specified BMC.
- The `clear logs error type=`*`SEVERITY`* `[pnum=0]` command removes errors of the specified severity. If a partition number is specified, only errors for the specified partition of the specified severity are removed.

  NOTE: HPE does not recommend clearing logs to ensure that failure information is available for diagnostic purposes.
- The `clear logs rcu [file=FILENAME]` command removes the specified *rcu* file.
- The `clear ntp` command removes the network time protocol (NTP) setting on the RMC.
- The `clear remote_log_server` command clears the configured remote log server settings and disables sending system log to the remote log server. RMC reboot is required after the clear command to disable logging to the remote server.

- The `clear rmc [product_data] [verbose]` command is not used on Superdome Flex 280 server.
- The `clear snmp_forwarding` command removes the simple network management protocol (SNMP) forwarding address setting on the RMC.
- The `clear sshkey` command removes the `ssh` key.

  To clear the key, first use the `show sshkey` command to display the key, and then use the `clear sshkey` command to remove the key.

collect

Syntax

```
collect debug
collect idc
```

Description

Gathers debugging data or the IDC logs into an archive file.

Usage

- You can use the `upload debug` command to transfer the file to another system at your site for eventual analysis.
- The approximate time it takes to create the archive file is as follows:
  - Allow up to 90 minutes for the RMC .
  - Allow up to 5 minutes per BMC.
- The `collect idc` command is used to collect and archive IDC logs. You can use `upload idc` command to transfer the file. It takes approximately 10 minutes to create the archive file.

commands

Syntax

```
commands
```

Description

Retrieves the list of valid RMC commands and the command formats.

Example output

```
RMC cli> commands
acquit
acquit [physloc=PHYSLOC_STR | chassis=GEOID | pnum=0 | all]
add
add certificate
add certificate ca file=FILENAME
add certificate signed [chassis=GEOID]
add dns [ipaddress=IPADDRESS | search=SEARCH_NAME]
add host name=NAME ipaddress=IPADDRESS
add ldap_group name=GROUP_NAME role={administrator,monitor,operator}
add location [rack=RACK] [bmc_id=BMC_ID] [module={rmc,bmc}] upos=UPOS
add snmp forward_address=FORWARD_ADDRESS [port=FORWARD_PORT] [protocol=PROTOCOL]
add sshkey key=PUBLIC_KEY
add user name=USERNAME role={administrator,monitor,operator}
apropos
backup
backup firmware [chassis=CHASSIS]
```

```
cancel
cancel autopower
clear
clear cae (all | complex | pnum=0)
clear dns
clear host
clear ldap [server] [port] [login] [binddn] [bindpw] [sid] [basedn] [userfilter] [userdn] [groupfilter] [groupdn]
clear logs
.
.
.
```

connect

Syntax

`connect npar [pnum=0] [clear] [full][nocache] [notty] [kill] [spy | steal]`

Description

Opens a console session to the partition. To exit the console session, type CTRL-`]` and enter `q`.

Usage

- `connect npar pnum=`*`0`* connects you to the partition in a console window.
- `connect npar pnum=`*`0`* `clear` removes cached console data.
- `connect npar pnum=`*`0`* `full` dumps out the entire console data cache and then goes to a live console.
- `connect npar pnum=`*`0`* `nocache` suppresses the display of cached data.
- `connect npar pnum=`*`0`* `notty` suppresses the interactive console capability.
- `connect npar pnum=`*`0`* `kill` terminates all existing console connections except for the console at which this command is entered.
- `connect npar pnum=`*`0`* `spy` enables you to watch another console in read-only mode.
- `connect npar pnum=`*`0`* `steal` assumes control of the console by force.

You can specify zero or more of the `clear`, `full`, `nocache`, `notty`, or `kill` parameters. You can specify either `spy` or `steal`.

deallocate

Syntax

`deallocate physloc=`*`PHYSLOC_STR`*

Description

Manually deallocate hardware.

Specifiers

`PHYSLOC_STR`

Specify the short form string of the hardware resource you want to deallocate. For example, `rack1/chassis_u1/cpu0/io_slot5`. The string you specify must appear in the output from the `show chassis info` command.

Usage

After you deallocate the hardware resource, the resource will not be available for use by the nPartition. Ensure that the power is off before you deallocate resources.

Example

```
RMC cli> deallocate
physloc=rack1/chassis_u1/cpu0/io_slot5
Deallocating rack1/chassis_u1/cpu0/io_slot5
RMC cli> deallocate physloc=rack1/chassis_u1/cpu0/io_slot5
Deallocating rack1/chassis_u1/cpu0/io_slot5
```

deconfig

Syntax

`deconfig physloc=`*`PHYSLOC_STR`*

Description

Manually removes a hardware component from the configuration.

Specifiers

PHYSLOC_STR

Specify the short form string. For example:

rack1/chassis_u1/cpu2/dimmQ0

The string you specify must appear in the output from the `show chassis info` command.

disable

Syntax

```
disable autopower
disable cert_checking
disable cli_session_timeout
disable http
disable https
disable ipmi
disable ipmi all
disable ipmi bt
disable ipmi lan
disable ipv6
disable ldap
disable ler vendor_id=VENDOR_ID device_id=DEVICE_ID
disable pcie_error_isolation chassis=GEOID (all | io_slot=IO_SLOT
[IO_SLOT ...])
```

```
disable power_redundancy
disable predictive_mem_health
disable script_mode
disable ssh
disable tpm [pnum=0]
disable zeroconf
```

Usage

- The `disable autopower` command prevents the system from applying power to the server components after a power off.
- The `disable cert_checking` command disables certificate checking for TLS connections.
- The `disable http` and `disable https` commands disable HTTP or HTTPS access to the RMC.

  NOTE: HTTP is also disabled after performing a factory reset.
- The disable `cli_session_timeout` disables `CLI Session Timeout`.
- The `disable ipmi all` command disables IPMI Block Transfer (BT) and IPMI LAN interfaces.
- The `disable ipmi bt` command disables IPMI Block Transfer (BT) interface.
- The `disable ipmi lan` command disables IPMI over LAN interface.
- The `disable ipv6` command disables ipv6 network interface.
- The `disable ipmi` command disables IPMI over LAN interface.

  NOTE: The IPMI Block Transfer (BT) interface is enabled and IPMI over LAN interface is disabled by default and are set to defaults on factory reset command.
- The `disable ldap` command disables LDAP management of the RMC.
- The `disable ler` command disables PCIe Live Error Recovery for the specified HPE supported I/O card.

  NOTE: Disabling LER is only recommended for those cases where FPGA cards are reprogrammed under an OS.
- The `disable script_mode` command returns the command-line interface to interactive mode.
- The `disable ssh` command disables SSH access to the RMC.
- The `disable power_redundancy` command disables reporting of power redundancy conditions.
- The `disable predictive_mem_health` command disables reporting of predictive memory failures on the system.
- The `disable tpm [pnum=0]` command disables the Trusted Platform Module (TPM) on the next boot.
- The `disable zeroconf` disables `zeroconf` protocol.

download

Syntax

`download certificate ca url=`*`URL`*

`download certificate crl url=`*`URL`*

`download certificate signed url=`*`URL`* `[chassis=`*`GEOID`*`]`

`download config (url=`*`URL`* `| file=`*`FILENAME`*`)`

`download npar config (url=`*`URL`* `| file=`*`FILENAME`*`)`

`download npar attributes (url=`*`URL`* `| file=`*`FILENAME`*`) [pnum=0]`

Description

Downloads a certificate, configuration or nPartition configuration to the RMC.

Specifiers

URL

Specify the full path to the source location on a local computer. Accepted transfer methods are `https`, `sftp` and `scp`.

The following examples show the supported formats:

- `https://`*`user@localhost/path`*
- `sftp://`*`user@localhost/path`*
- `scp://`*`user@localhost/path`*

The command prompts you for the password to the local host computer.

FILENAME

Specify the name of the file.

GEOID

Specify the identifier of the server chassis where you want to download the certificate. The *GEOID* identifies the rack number and the chassis U position within the rack. To retrieve a *GEOID*, enter `show complex` at the RMC prompt.

For example, *GEOID* `r001u06b` pertains to the chassis in rack number 1 with U position 6.

Usage

- The `download certificate ca url=`*`URL`* command downloads a certificate authority from the specified URL.
- The `download certificate crl url=`*`URL`* command downloads a certificate revocation list from the specified URL.
- The `download certificate signed url=`*`URL`* `[chassis=`*`GEOID`*`]` command downloads a signed certificate to the specified chassis. If a chassis is not specified, the command downloads a signed certificate to the RMC.

- The `download config (url=URL | file=FILENAME)` command downloads a configuration file at the specified URL to the RMC.
- The `download npar config (url=URL | file=FILENAME)` downloads the nPartition configuration file at the specified URL to the RMC.

enable

Syntax

```
enable autopower
enable cert_checking
enable cli_session_timeout
enable http
enable https
enable ipmi
enable ipmi all
enable ipmi bt
enable ipmi lan
enable ipv6
enable ldap
enable ler vendor_id=VENDOR_ID device_id=DEVICE_ID
enable pcie_error_isolation chassis=GEOID (all | io_slot=IO_SLOT
[IO_SLOT ...])
enable power_redundancy
enable predictive_mem_health
enable script_mode
enable ssh
enable tpm [pnum=0]
enable zeroconf
```

Usage

- The `enable autopower` command lets the system apply power to the server components after a power off.
- The `enable cert_checking` command enables certificate checking for TLS connections.
- The `enable http` and `enable https` commands enable HTTP or HTTPS access to the RMC.

  NOTE: HTTP is also disabled after performing a factory reset.

- The `enable ipmi` command enables IPMI over LAN interface.

  NOTE: The IPMI Block Transfer (BT) interface is enabled and IPMI over LAN interface is disabled by default and are set to defaults on factory reset command.

- The `enable ipmi all` command enables IPMI Block Transfer (BT) and IPMI LAN interfaces.
- The `enable ipmi bt` command enables IPMI Block Transfer (BT) interface.
- The `enable ipmi lan` command enables IPMI over LAN interface.
- The `enable ipv6` command enables ipv6 network interface.
- The `enable ldap` command enables LDAP management of the RMC.
- The `enable ler` command enables PCIe Live Error Recovery for the specified HPE supported I/O card.
- The `enable predictive_mem_health` command enables reporting of predictive memory failures on the system.
- The `enable script_mode` command turns off the console interactive mode. In script mode, when the command line prompts you to enter `y` or `n` in answer to a question, the system assumes a `y` and continues.
- The `enable ssh` command enables SSH access to the RMC.
- The `enable tpm [pnum=0]` command enables the Trusted Platform Module (TPM) on the next boot.
- The `enable zeroconf` enables `zeroconf` protocol.

exit

Syntax

```
exit
```

Description

Closes the RMC CLI session from where the command is entered.

generate certificate

Syntax

```
generate certificate
generate certificate request [chassis=GEOID]
generate certificate selfsigned [chassis=GEOID]
```

Description

Generates a certificate for the RMC/eRMC or the BMC of the specified chassis.

Specifiers

GEOID

Specify the chassis for which to generate the certificate.

Usage

The `generate certificate request` command generates a CSR certificate for the RMC/eRMC.

The `generate certificate request chassis=`*`GEOID`* requests a CSR certificate for the BMC of the specified chassis.

The `generate certificate selfsigned` command generates a self-signed certificate for the RMC/eRMC.

The `generate certificate selfsigned chassis=`*`GEOID`* command generates a self-signed certificate for the BMC of the specified chassis.

help

Syntax

`help` *`COMMAND`* `[`*`OPTION`*`]`

Description

Returns information about an RMC command. Adding a command *OPTION* returns information about that option.

Specifiers

COMMAND

Any of the RMC commands.

OPTION

Any valid option for the RMC command.

Example

The following example uses the `apropos` and `help` commands together.

```
RMC cli> apropos snmp

add snmp forward_address=FORWARD_ADDRESS [port=FORWARD_PORT] [protocol=PROTOCOL]
clear snmp_forwarding
remove snmp forward_address=FORWARD_ADDRESS
set snmp forward_address=FORWARD_ADDRESS [port=FORWARD_PORT] [protocol=PROTOCOL]
show snmp
show snmp forward_address

RMC cli> help show snmp

Usage: show snmp
       show snmp forward_address

RMC cli> help show snmp forward_address

Shows SNMP forwarding addresses.
Usage: show snmp forward_address
```

indict

Syntax

`indict physloc=`*`PHYSLOC_STR`*

Description

Manually marks a hardware component as failed.

Specifiers

PHYSLOC_STR

Should be a string. For example:

rack1/chassis_u1/cpu2/dimmQ0

The command does not accept short form strings.

Usage

After you replace the failed component, run the `acquit` command to clear the indictment. The string you specify must appear in the output of the `show chassis info` command for the affected component.

ipmi

Syntax

`ipmi command=`*`CMD_STRING`*

Description

Lets you run industry standard `ipmi` commands on the HPE Superdome Flex 280 Server.

Specifiers

CMD_STRING

Specifies one or more `ipmi` commands. To retrieve a list of possible commands, enter the following at the RMC command prompt:

```
ipmi command=help
```

Enclose the *CMD_STRING* in quotation marks (" ") if you specify more than one command. If the *CMD_STRING* contains spaces, you must enclose it in quotation marks.

Example

```
RMC cli> ipmi command=help

Commands:
        raw           Send a RAW IPMI request and print response
        i2c           Send an I2C Master Write-Read command and print response
        spd           Print SPD info from remote I2C device
        lan           Configure LAN Channels
        chassis       Get chassis status and set power state
        power         Shortcut to chassis power commands
        event         Send pre-defined events to MC
        mc            Management Controller status and global enables
        sdr           Print Sensor Data Repository entries and readings
.
.
.
RMC cli> ipmi command="chassis power status"

Chassis Power is off
```

More information

Management with `ipmitool`

modify

Syntax

```
modify chassis target=GEOID [serial=SERIAL_NUMBER] [{type={31-34}} |
{part_num=PRODUCT_ID model=PRODUCT_NAME}] [verbose]
```

```
modify ldap_group name=GROUP_NAME role={administrator, monitor,operator}
```

```
modify npar [pnum=0] [secure_boot={on,off}]
[dcpmm_security={enabled,disabled}] [dcpmm_passphrase]
```

```
modify npar attributes [pnum=0] [attribute1=VALUE] [attribute2=VALUE] ...
[attributeN=VALUE]
```

Description

Lets you change the hardware features on a specified partition.

Specifiers

GROUP_NAME

Specify the LDAP directory group.

GEOID

Specify the identifier of the server chassis for which you want to disable or enable a unit identification number (UID). The *GEOID* identifies the rack number and the chassis U position within the rack. To retrieve a *GEOID*, enter `show complex` at the RMC prompt.

For example, *GEOID* `r001u06b` pertains to the chassis in rack number 1 with U position 6.

Usage

- The `modify ldap_group name=GROUP_NAME role={administrator, monitor,operator}` command changes the LDAP directory group or role for the RMC.
- The `modify npar [pnum=0 [secure_boot={on,off}]` command enables or disables secure boot.

  CAUTION: Hewlett Packard Enterprise strongly recommends using the `ras=on` specification to enable memory RAS features (ADDDC mode). HPE RAS features provide higher resiliency to DIMM faults versus standard memory error-correcting code (ECC).

  The `ras=hpc` specification disables memory RAS features and therefore could result in compromised system resiliency and a potential server outage.

  You will experience high failure rates of DIMMs using the `ras=hpc` specification.

  To check the memory RAS setting, enter the `show npar verbose` RMC command.

- The `modify npar [pnum=0]` attributes command enables users to modify a large number of settings on a per-nPar basis. You must reboot the nPar to apply pending changes.
- The `modify npar [pnum=0] attributes workloadprofile={mc,hpc,imdb,virtualization,custom}` command affects multiple attributes simultaneously, including power consumption and RAS features.

NOTE: Hewlett Packard Enterprise strongly recommends using the `workloadprofile=mc` specification to enable memory RAS features (ADDDC mode). HPE RAS features provide higher resiliency to DIMM faults versus standard memory error-correcting code (ECC).

The `workloadprofile=hpc` specification disables memory RAS features and therefore could result in compromised system resiliency and a potential server outage.

You may experience higher failure rates of DIMMs using the `hpc` profile.

To check the memory `AdvancedMemProtection` setting, enter the `show npar verbose` RMC command.

- The `modify npar attributes [pnum=0] bootslots=`*`n`* `[,`*`n`* `[ ,`*`n`* `]]` command adjusts which PCI slot numbers are enabled for boot devices and for option ROM execution.
- The `modify chassis` command is used only by service personnel.

ping

Syntax

```
ping [-LRUbdfnqrvVaADO] [-c count] [-i interval] [-w deadline]
            [-p pattern] [-s packetsize] [-t ttl] [-I interface]
            [-M pmtudisc-hint] [-m mark] [-S sndbuf]
            [-T tstamp-options] [-Q tos] [hop1 ...] destination
```

Description

Sends an echo request to a server on an IPv4 network to test reachability.

ping6

Syntax

```
ping6 [-LUdfnqrvVaADO] [-c count] [-i interval] [-w deadline]
            [-p pattern] [-s packetsize] [-t ttl] [-I interface]
            [-M pmtudisc-hint] [-S sndbuf] [-F flowlabel] [-Q tclass]
            [-N nodeinfo-suboptions]
            [hop1 ...] destination
```

Description

Sends an echo request to a server on an IPv6 network to test reachability.

power

Syntax

```
power
power cycle [force]
power cycle bmc
power cycle npar [pnum=0] [bootopt=BOOTOPT] [force]
power off [force]
```

```
power off npar [pnum=0] [force]
power on
power on npar [pnum=0] [bootopt=BOOTOPT] [secure_erase_dcpmms]
power reset [force]
power reset bmc
power reset npar [pnum=0] [bootopt=BOOTOPT] [force]
```

Description

Enables you to control power to the following:

- The HPE Superdome Flex 280 Server system
- Specific components of the HPE Superdome Flex 280 Server system

Specifiers

BOOTOPT

Specify the boot option.

Usage

- `power` displays the quantity of chassis in each power mode.
- If power is on, the `power cycle npar [pnum=0] [bootopt=BOOTOPT] [force]` command performs an OS immediate (non-graceful) shutdown and the momentarily removes power from the specified nPartition. Then the command turns on partition power and starts the nPartition. If `force` is specified, no user confirmation occurs.
- The `power cycle [force]` command functions the same as `power cycle npar` if a single nPartition is configured. This command is invalid if multiple nPartitions are configured. If `force` is specified, no user confirmation occurs.
- The `power cycle bmc` command removes auxiliary power from all BMCs in an nPartition and then turns on auxiliary power.

  NOTE: All chassis in the nPartition are powered off when this command is used.

- The `power off npar pnum=0][force]` command performs a graceful OS shutdown and then removes power from the specified nPartition with no user confirmation. If `force` is specified, the command performs an OS immediate (non-graceful) shutdown instead.
- The `power off [force]` command functions the same as `power off npar` if a single nPartition is configured. This command is invalid if multiple nPartitions are configured.
- The `power on npar [pnum=0] [bootopt=BOOTOPT] [secure_erase_dcpmms]` command turns on power to the specified nPartition and starts the nPartition power.
- The `power on` command functions the same as `power on npar` if a single nPartition is configured. This command is invalid if multiple nPartitions are configured. If `force` is specified, no user confirmation occurs.
- If power is on, the `power reset npar [pnum=0] [bootopt=BOOTOPT] [force]` command performs a graceful OS shutdown then restarts the specified nPartition. If `force` is specified, it performs an OS immediate (non-graceful) shutdown instead. This command is invalid if power is off; you must use `power on` instead.
- The `power reset [force]` command functions the same as `power reset npar` if a single nPartition is configured. This command is invalid if multiple nPartitions are configured.

- The `power reset bmc` command restarts all BMCs in the specified nPartition after user confirmation.
- The RMC and the BMCs are always powered up if the RMC and BMCs are connected to an AC power source. You cannot power off the RMC or the BMCs, however you can power cycle the BMCs.

More information

Partition boot options

reallocate

Syntax

```
reallocate (physloc=PHYSLOC_STR | all)
```

Description

Reallocate deallocated hardware.

Specifiers

`PHYSLOC_STR`

Specify the short form string of the hardware resource you want to reallocate. For example, `rack1/chassis_u1/cpu0/io_slot5`. The string you specify must appear in the output from the show chassis info command.

Usage

- The `reallocate physloc` command reallocates only the one hardware resource specified by the physical location.
- The reallocate all command reallocates all deallocated hardware in the complex.

Example

```
RMC cli> reallocate all

==== r001u01b ====

Reallocating rack1/chassis_u1/cpu0/io_slot5
Reallocating rack1/chassis_u1/cpu2/dimmT1

RMC cli>
```

reboot

Syntax

```
reboot

reboot bmc (all | target=GEOID [GEOID ...])

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

reboot rmc

reboot validate_fw
```

Description

Reboots the RMC or the HPE Superdome Flex 280 Server.

Specifiers

GEOID

Identifies the specific BMC.

BOOTOPT

Specify the boot option.

Usage

- If power is on, the `reboot npar [pnum=0] [bootopt=BOOTOPT] [force] [secure_erase_dcpmms]` command performs an OS graceful shutdown, then restarts the nPartition. If `force` is specified, the command instead performs an OS immediate (non-graceful) shutdown. This command is invalid if power is off. Use the `power on` command instead.
- The `reboot` command functions the same as the `reboot npar` command when a single nPartition is configured. This command is invalid if multiple nPartitions are configured. No `force` option is supported for this command; use the `reboot npar` command instead.
- The `reboot rmc` command prompts the user that this action may disrupt operations, and then after confirmation restarts the RMC, disconnecting all current user sessions.
- The `reboot bmc target=`*`GEOID`* command prompts the user that this action may disrupt operations, and then after confirmation restarts the specified BMC, which may be in any chassis in the complex.
- The `reboot validate_fw` initiates a reboot of every chassis and performs Silicon Root of Trust (SiROT) validation.

More information

Partition boot options

remove

Syntax

```
remove certificate ca (file=FILENAME | all)
remove certificate crl (file=FILENAME | all)
remove config (file=FILENAME | all)
remove debug [file=FILENAME]
remove dns [ipaddress=DNS_IPADDRESS | search=SEARCH_NAME]
remove ermc
remove host [name=NAME | ipaddress=IPADDRESS]
remove idc [file=FILE]
remove ldap_group name=GROUP_NAME
remove ldap_user_data
remove location [module={rmc,bmc}] bmc_id=BMC_ID
remove redfish event_subscription (id=ID | all)
```

`remove snmp forward_address=FORWARD_ADDRESS`

`remove sshkey key=PUBLIC_KEY`

`remove user name=USERNAME`

Description

Specifies system characteristics or users to be removed from the HPE Superdome Flex 280 Server .

Specifiers

DNS_IPADDRESS

Specify the IP address of the DNS server at your site.

FORWARD_ADDRESS

Specify the IP address of a local computer or device to receive SNMP alerts.

PUBLIC_KEY

Specify the SSH public key. The `show sshkey` command returns they key values.

USERNAME

Specify the name of the user that you want to delete from the system.

FILENAME

Specify the name of the file you want to delete from the system.

Usage

The `remove certificate ca (file=FILENAME | all)` command removes the specified certificate authority file or all certificate authority files.

The `remove certificate crl (file=FILENAME | all)` command removes the specified certificate revocation list file or all certificate revocation list files.

The `remove config file=FILENAME` command removes the specified configuration file.

The `remove config all` command removes all configuration files present in the RMC/eRMC. To see configuration file details, enter the command `show config list`.

The `remove debug [file=FILE]` command removes the specified debug file. To see the debug file details, enter the command `show debug`.

The `remove dns [ipaddress=DNS_IPADDRESS | search=SEARCH_NAME]` command removes the specified DNS server address or the DNS server matching the specified search name.

The `remove ermc` command removes the active eRMC. This command effectively converts the eRMC to a BMC. For use cases and examples, enter the command `help add location`.

The `remove host [name=NAME | ipaddress=IPADDRESS]` command removes the specified host.

The `remove idc [file=FILE]` command removes all the IDC logs archive files or only the specified IDC logs archive.

The `remove ldap_group name=GROUP_NAME` command removes the specified LDAP group.

The `remove ldap_user_data` command removes all LDAP user data.

The `remove location [module={rmc,bmc}] bmc_id=BMC_ID` command removes a BMC entry or the eRMC from the configuration.

The `remove redfish event_subscription (id=ID | all)` command removes the specified or all Redfish event subscription(s).

The `remove sshkey key=PUBLIC_KEY` command removes the specified SSH public key.

The `remove snmp forward_address=FORWARD_ADDRESS` command removes the specified SNMP forwarding IP address.

The `remove user name=USERNAME` command removes the specified user.

NOTE: All existing CLI sessions for the user are logged off when the user is removed.

restore

Syntax

```
restore config (url=URL | file=FILENAME)
restore npar attributes (url=URL | file=FILENAME) [pnum=0]
restore npar config (url=URL | file=FILENAME)
```

Description

Download and then execute a previously saved configuration script file produced by a `save` command. This restores user configurable settings on the complex.

Descriptors

URL

Specify the full path to the source location on a local computer. Accepted transfer methods are `https`, `sftp`, and `scp`.

The following examples show the supported formats:

- `https://user@localhost/path`
- `sftp://user@localhost/path`
- `scp://user@localhost/path`

The command prompts you for the password to the local host computer.

FILENAME

Specify the name of the file.

Usage

- The `restore config (url=URL | file=FILENAME)` command restores RMC configuration using the specified configuration file at the specified URL.
- The `restore npar config (url=URL | file=FILENAME)` restores nPartition configuration from the specified file at the specified URL.

save

Syntax

```
save config (url=URL | file=FILENAME)
save npar config (url=URL | file=FILENAME)
```

Description

Upload a configuration script file of all user configurable settings to a server or RMC local file. You can use the resulting file with the restore command.

Descriptors

URL

Specify the full path to the source location on a local computer. Accepted transfer methods are `https`, `sftp`, and `scp`.

The following examples show the supported formats:

- `https://user@localhost/path`
- `sftp://user@localhost/path`
- `scp://user@localhost/path`

The command prompts you for the password to the local host computer.

FILENAME

Specify the name of the file.

Usage

- The `save config (url=URL | file=FILENAME)` command saves the specified RMC configuration file at the specified URL.
- The `save npar config (url=URL | file=FILENAME)` saves the specified nPartition configuration file at the specified URL.

`search` and `searchevents`

Syntax

```
search logs iel [begin=BEGIN_TIME] [end=END_TIME] [alert=ALERT_THRESHOLD]
[str=SEARCH_STRING] [excl=EXCLUDE_STRING] [pnum=0]
```

```
 searchevents [-B begin_time] [-E end_time] [-e stringA]...[-e stringB] [-v
stringY]...[-v stringZ] [-A alert_threshold] [-p partition] [-x] [-?] [-h]
   -B  : beginning of search time           (default: "last boot" associated
with partition number)
   -E  : ending of search time              (default: "now")
   -e  : search string  (case-insensitive)  (default: no search filters)
   -v  : exclude string (case-insensitive)  (default: no exclude filters)
   -A  : alert threshold                    (default: 0)
   -p  : partition number                   (default: unspecified)
   -x  : eXhaustive search (entire file)    (default: Not exhaustive.
Assumes all events are in chronological order.

-? -h  : this help
```

Description

The `search` command examines log files for one or more characteristics that you specify and returns events that match your search criteria.

The `searchevents -h` command shows additional information and examples on how to specify search criteria.

Specifiers

BEGIN_TIME

Specify a time. Use one of the formats that the `searchevents -h` command returns.

END_TIME

Specify a time. Use one of the formats that the `searchevents -h` command returns.

ALERT_THRESHOLD

Specify one of the following alert levels: 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.

SEARCH_STRING

Specify a string of your choice. The string cannot include space characters.

EXCLUDE_STRING

Specify a string of your choice. The string cannot include space characters.

Example

```
RMC cli> searchevents -h

Usage: searchevents [-B begin_time] [-E end_time] [-e stringA]...[-e
stringB] [-v stringY]...[-v stringZ] [-A alert_threshold] [-p partition] [-
x] [-?] [-h]
   -B  : beginning of search time           (default: "last boot" associated
with partition number)
   -E  : ending of search time              (default: "now")
   -e  : search string  (case-insensitive)  (default: no search filters)
   -v  : exclude string (case-insensitive)  (default: no exclude filters)
   -A  : alert threshold                    (default: 0)
   -p  : partition number                   (default: unspecified)
   -x  : eXhaustive search (entire file)    (default: Not exhaustive.
Assumes all events are in chronological order.

-? -h  : this help

All times are assumed to be UTC. Unrecognized/extraneous strings may be
silently ignored.
Example formats for Begin/End search times:
  -B/-E "09/05/2017 20:16:15"  ->  fully specified date/time
  -B/-E "2017-09-05 20:16:15Z" ->  ISO standard date/time (trailing Z
optional)
  -B/-E "09/05      20:16:15"  ->  if year is omitted, current year will be
used
  -B/-E "9/5        20:16"     ->  if seconds are omitted, seconds will
be :00
  -B/-E 22:00                  ->  today at the specified time
  -B/-E "XX sec ago"           ->  current time minus specified quantity
  -B/-E "XX min ago"           ->  current time minus specified quantity
  -B/-E "XX hour ago"          ->  current time minus specified quantity
  -B/-E "XX day ago"           ->  current time minus specified quantity
  -B/-E "XX week ago"          ->  current time minus specified quantity
  -B/-E "XX month ago"         ->  current time minus specified quantity
  -B/-E "XX year ago"          ->  current time minus specified quantity
  -B/-E "XX day ago 17:00"     ->  combine the above with a specific time
  -B/-E yesterday              ->  prior date at 00:00:00
  -B/-E "yesterday 22:00"      ->  prior date at specified time
  -B/-E today                  ->  today at 00:00:00
  -B/-E "today 7:30"           ->  today at the specified time
  -B/-E now                    ->  current time
  -B/-E epoch                  ->  01/01/1970 00:00:00   (search entire log)
  -B/-E IEL_EVENT_KEYWORD      ->  last IEL_EVENT_KEYWORD (case insensitive)
```

```
Additional options for Begin search times:
  -B "last poweron"         ->  last CHASSIS_POWERED_ON event
  -B "last efi reset"       ->  last 'EFI reset'
  -B "last os reboot"       ->  last 'OS reboot'
  -B "last boot"            ->  last 'poweron' OR 'efi reset' OR 'os reboot'
event
```

set

Syntax

`set autopower delay=SECONDS`

`set date [yr=YEAR] [mo=MONTH] [day=DAY] [hr=HOUR] [min=MINUTE] | [str=DATE_STRING]`

`set factory [initialize | npar]`

`set failed_login delay=SECONDS`

`set hostname [name=HOST_NAME | default]`

`set ipmi_watchdog (disabled | os_managed)`

`set ipmi restricted={on,off}`

`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 network [baseio=GEOID] [addressing={dhcp,static,default}] [gateway=GATEWAY] [hostname=HOST] [ipaddress=IPADDRESS] [netmask=NETMASK]`

`set network internal [bmc_subnet=BMC_SUBNET] [cmc_subnet=CMC_SUBNET] [ermc_subnet=ERMC_SUBNET]`

`set network internal default`

`set network ipv6 [addressing={dhcp,static}] [ipaddress=IPV6_ADDRESS/PREFIX_LENGTH] [gateway=GATEWAY]`

`set network ipv6 aux [addressing={static,default}] [ipaddress=IPV6_ADDRESS/PREFIX_LENGTH]`

`set network ipv6 baseio [chassis=GEOID] [addressing={dhcp,static}] [ipaddress=IPV6_ADDRESS/PREFIX_LENGTH] [gateway=GATEWAY]`

`set npar default [pnum=0] (attributes | efi_variables | all)`

`set ntp server=SERVER`

`set password [username=USERNAME | minimum_length=MINIMUM_LENGTH]`

`show password minimum_length`

`set password default`

`set prompt [string=STRING | default]`

`set remote_log_server server_address=SERVER_ADDRESS [port=PORT] [protocol=PROTOCOL] [severity_level=SEVERITY_LEVEL]`

`set session [hr=HOUR] [min=MINUTE] [sec=SECOND]`

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

```
set telemetry (on | off)
set timezone str=TIMEZONE_SPEC
]
set tpm cancel_clear [pnum=0]
set tpm clear [pnum=0]
set tpm ppi (accept | deny) action={clear} [minutes=MINUTES] [pnum=0]
set uid off [chassis=GEOID] [drive=ID]
set uid on [chassis=GEOID] [drive=ID
```

Description

Specifies system characteristics.

Specifiers

DATE_STRING

Specify the date in a quoted string. For example:

```
set date str="2021-01-25 13:27"
```

To retrieve the date in a format that you can use as input to the `set date` command, enter the following command on a local Linux or UNIX system:

```
date "+%Y-%m-%d %H:%M"
```

DAY

Specify the day as a two-digit integer. For example, `02` or `31`.

FORWARD_PORT

Specify a network port to receive SNMP notifications.

GATEWAY

Specify a network gateway.

GEOID

Specify the identifier of the server chassis for which you want to disable or enable a unit identification number (UID). The *GEOID* identifies the rack number and the chassis U position within the rack. To retrieve a *GEOID*, enter `show complex` at the RMC prompt.

For example, *GEOID* `r001u06b` pertains to the chassis in rack number 1 with U position 6.

HOST_NAME

Specify a hostname for the RMC. If you specify the keyword of `default`, the RMC displays the default prompt, which is the RMC *geoid*.

HOUR

Specify the hour as a two-digit integer against a 24-hour clock. For example, `08` or `14`

MINUTES

Specify the minutes as a two-digit integer.

MONTH

Specify the month as a two-digit integer. For example, `06` or `12`.

NETMASK

Specify the network mask.

NUMBER

Specify the number of the rack in which the RMC resides.

PORT

Specify a network port in the remote log server to receive the system events.

PROTOCOL

Specify the network protocol used to transfer the system events to remote log server. The supported protocols are `UDP` and `TCP`. Default protocol is `UDP`.

SECONDS

- `set autopower delay=`*`SECONDS`*—Specify the number of seconds in the you want to elapse between power being applied to the HPE Superdome Flex 280 Server and the server powering up. When power is reapplied to the system, the RMCs and BMCs power up automatically. You can delay the server power-up by the number of seconds specified.

  For example, after a power outage, all servers power up at the same default time interval after power is restored. To stagger each server to power up at a slightly different time, you can specify a different number of *SECONDS* for each server. This practice avoids having all servers power up at the same time, which can lead to a blown circuit breaker in the computer center.
- `set failed_login delay=SECONDS`—Specify the delay for a failed login in seconds, allowed values are 0 to 240.

SERVER

Specify an appropriate IP address or host name.

STRING

Specify the command prompt you want on the RMC. If *STRING* contains space characters, enclose *STRING* in quotation marks. For example:

```
RMC cli> set prompt string="my rmc"
RMC cli> set prompt string=flex-rmc
```

Severity_level

The severity level can optionally be provided for selecting the severity level. Default severity level is `info`. The supported input values can be:

- `debug`
- `info`
- `warn`
- `critical`
- `fatal`

TIMEZONE_SPEC

Specify one of the time zone codes. For example, `EST` or `Canada/Central`. For the complete time zone code list, log into the RMC and enter the following command:

```
RMC cli> help set timezone
```

UPOS

Specify the U position of the RMC. In the rack, the U positions are numbered from bottom to top. The bottom-most U position is 1.

YEAR

Specify the year as a four-digit integer. For example, `2018`.

Usage

- The `set autopower delay=`*`SECONDS`* command sets the delay in seconds before the system powers on after applying power.
- The `set date` command sets the date using the specified parameters.
- The `set factory [initialize]` command resets the system to factory default settings and optionally initializes the system.
- The `set failed_login delay=SECONDS` command sets the login delay value in seconds for a failed login. Login is restricted till the configured delay is reached. This delay value is in seconds. Valid values are 0 to 240 seconds. Default value 0 indicates failed login is disabled. This feature is applicable only for local users but not for remote users such as LDAP users.
- The `set hostname [name=`*`HOST_NAME`*` | default]` command sets the system hostname to the specified name or a default-generated value.
- The `set ipmi_watchdog (disabled | os_managed)` command disables or enables the IPMI watchdog functionality to be managed by the OS. The default is disabled.
- The `set ldap` command sets the LDAP server using the specified parameters.
- The `set network` command sets the primary external networking using the specified parameters or to default generated values.
- The `set network aux` sets the auxiliary external networking using the specified parameters or to default generated values.
- The `set network internal` command sets the internal networking subnet using the specified parameters or to default generated values.
- The `set network ipv6` command sets primary IPv6 networking to the specified parameters.
- The `set network ipv6 baseio` command sets the IPv6 networking for the BaseIO.
- The `set ntp SERVER=`*`SERVER`* command sets the NTP server to the specified IP address or server host name.
- The `set password [username=USERNAME | minimum_length=MINIMUM_LENGTH]` command sets the user password for the specified user account. Passwords must meet the following requirements:
  - Passwords may include combinations of these types of characters:
    - Upper case letters
    - Lower case letters
    - Numbers
    - Special characters - including `!@#$%^&*()!@`
    - The default RMC password can be configured for a length of 6 to 64 characters.
  - 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 minimum length can be modified with

administrator account privileges using the `Password` command. Below are the absolute minimum lengths that can be configured and the current default minimum lengths in parentheses.

  - Passwords only containing one type of character must be at least 12 (default 14) characters.
  - Passwords containing two types of character must be at least 10 (default 12) characters.
  - Passwords containing three types of character must be at least 8 (default 10) characters.
  - Passwords containing all four types of characters must be at least 6 (default 8) characters.

- The `set prompt` command sets the CLI prompt to the specified string or to the default value. If you want to use a prompt character such as > or `:`, it must be included in the string. The prompt string is stripped of leading and trailing spaces.
- The `set remote_log_server server_address=`*`SERVER_ADDRESS`* `[port=`*`PORT`*`] [protocol=`*`PROTOCOL`*`] [severity_level=`*`SEVERITY_LEVEL`*`]` command sets the IP address or hostname of remote log server and enables remote logging. The port number and protocol can optionally be provided for connecting to the remote log server. The supported protocols are `UDP` and `TCP`. Default protocol is `UDP`. Default `severity_level` is `info`. The supported input values for `severity_level` can be:
  - `debug`
  - `info`
  - `warn`
  - `critical`
  - `fatal`
- The `set snmp forward_address=`*`FORWARD_ADDRESS`* `[port=`*`FORWARD_PORT`*`] [protocol=`*`PROTOCOL`*`]` command sets SNMP forwarding to the specified IP address, optionally using the port and protocol specified.
- The `set timezone str=`*`TIMEZONE_SPEC`* command sets the RMC to the specified time zone.
- The `set uid` command turns on or turns off the UID locator light on the specified chassis.
- The `set session [hr=`*`HOUR`*`] [min=`*`MINUTE`*`] [sec=`*`SECOND`*`]` would set the session timeout for CLI, eRS, GUI, and Redfish interfaces. The setting range can be from 1 minute to 24 hours.
- The `set telemetry (on | off)` command sets the telemetry control configuration.
- The `set tpm ppi (accept | deny) action={clear} [minutes=`*`MINUTES`*`] [pnum=0]` command sets Physical Presence Indication to either acceptor deny PPI requests for the specified action.
- The `set tpm cancel_clear [pnum=0]` command cancels previously requested Trusted Platform Module (TPM) clear.
- The `set tpm clear [pnum=0]` command clears the Trusted Platform Module (TPM) during the next boot.

show

Syntax

```
show all
show analysis id=BUNDLE_ID [summary]
show autopower
```

```
show bios [target=TARGET]

show bios revision [target=TARGET]

show bios state [target=TARGET]

show bios uptime [target=TARGET]

show cae [list] [id=EVENT_ID] [severity=SEVERITY num or text] [pnum=0]
[offset=OFFSET] [count=NUMBER] [dump=INDEX num or "all"]

show cert_checking

show certificate [chassis=GEOID]

show certificate request [chassis=GEOID]

show certificate ca [file=FILENAME]

show certificate crl [file=FILENAME]

show certificate request [chassis=GEOID]

show chassis

show chassis info [chassis=GEOID]

show chassis list

show complex

show config [list | file=FILENAME]

show date

show deallocate [chassis=GEOID | pnum=0]

show debug

show deconfig [chassis=GEOID | pnum=0]

show dns

show failed_login

show firmware [verbose]

show firmware bundle [url=BUNDLE_URL]

show firmware silos [chassis=CHASSIS]

show health [chassis=GEOID | pnum=0 | verbose]

show host

show hostname

show hwcfg

show idc

show indict [chassis=GEOID | pnum=0]

show ipmi_watchdog

show ipmi config

show ipmi restricted

show ldap

show ldap_group

show ler [enable] [disable]
```

```
show livelogs
show location
show logs
show logs audit
show logs console target={BMC_GEOID | P0 | PROC_GEOID} [socket={0-3}] [full]
show logs dmesg [target=TARGET]
show logs error [mca | cmc | type=SEVERITY | id=BUNDLE_ID | pnum=0]
show logs hel [all] [hex] [target=TARGET]
show logs iel [live]
show logs sel [target=TARGET]
show logs support [ieldepth=DAYS]
show logs syshist [verbosity={0,1,2} | raw]
show network
show npar [pnum=0] [verbose]
show npar attributes [pnum=0]
show ntp
show password
show password default
show password minimum_length
show pcie_error_isolation
show power
show power npar [pnum=0]
show power_redundancy
show predictive_mem_health
show privileges [role={administrator, monitor,operator}]
show rcu [list | id=HEX_ID | file=FILENAME] [verbose]
show redfish [uri=URI] [walk]
show redfish event_subscription
show remote_log_server
show rmc
show rmc usb [all | path=PATH]
show sdr [target=TARGET]
show sensor [target=TARGET]
show snmp
show snmp forward_address
show sshkey
show telemetry
show timezone
```

```
show tpm [pnum=0]
show uid chassis=GEOID[drive=ID]
show user
show user list
```

Specifiers

EVENT_ID

Specify one or more event identifiers. Use a comma to separate each *EVENT_ID*. The `show cae` command returns information for each specified *EVENT_ID*.

FILENAME

Specify the name of the file that you want to view.

OFFSET

Specify an offset value. When you specify an *OFFSET* value, the `show cae` command displays events starting from a particular *INDEX* with *OFFSET* value.

NUMBER

Specify an integer number of events that you want the command to display. You can specify a *NUMBER* and an *offset* to scroll through the entire set of events that are available.

INDEX

Specify an `Index` value from the list.

To retrieve a list of index values, enter `show cae list`.

SEVERITY

Specify one of the following:

- 0 or `Unknown`
- 1 or `Other`
- 2 or `Informational`
- 3 or `Degraded` or `Warning`
- `4` or `Minor Fault`
- `5` or `Major Alert`
- `6` or `Critical`
- `7` or `Fatal`

When you specify a *SEVERITY*, the `show cae` command returns information for events at that severity threshold and above.

BUNDLE_ID

Specify the identifier that is associated with the log file that you want to examine. For example: `0x2110000000000001`.

TARGET

Specify the BMC *geoid*.

GEOID

Specify the identifier of the server chassis for which you want to display a unit identification number (UID). The *GEOID* identifies the rack number and the chassis U position within the rack. To retrieve a *GEOID*, enter `show complex` at the RMC prompt.

For example, a *GEOID* of `r001u06b` pertains to the chassis in rack number 1 with U position 6.

Usage

- The `show all` command runs the following commands in sequence (in a noninteractive mode):
  - `show failed_login`
  - `show firmware verbose`
  - `show hwcfg`
  - `show health`
  - `show health verbose`
  - `show host`
  - `show hostname`
  - `show idc`
  - `show indict`
  - `show ipmi_watchdog`
  - `show ldap`
  - `show ldap_group`
  - `show ler [enable] [disable]`
  - `show logs audit`
  - `show logs dmesg`
  - `show logs hel`
  - `show logs sel`
  - `show logs rcu`
  - `show deconfig`
  - `show network`
  - `show npar`
  - `show chassis list`
  - `show ntp`
  - `show power`
  - `show predictive_mem_health`
  - `show redfish event_subscription`
  - `show remote_log_server`

- show sdr
- show sensor
- show session
- show sshkey
- show snmp
- show uid chassis=r001u01b
- show uid chassis=r001u06b
- show user
- show user list

Example1

The `show indict` command returns a list of indictments.

```
RMC cli> show indict

r001u01b

  FFFF000101FFFF64 rack1/chassis_u1/harp_fan0

    Indicted: Yes
        2017-10-31T17:05:42Z  Reason ID: 302
            Summary: Fan reported to be running slowly or stopped
            Cause: A fan is not running at normal speed.  There may be
something obstructing the airflow, a blocked fan or a fan failure.
            Action: Check the enclosure for obstructions to airflow and
ensure the fans are installed properly.  If the problem persists, replace
the fan. After replacing the faulty fan, perform an acquitall from the RMC
command line.
```

This example shows that the fan with resource ID `rack1/chassis_u1/harp_fan0` in the chassis with GEOID `r001u01b` in the physical location `FFFF000101FFFF64` has been indicted with an error.

Example 2

The following command displays errors in the machine check architecture (MCA) log files and corrected machine check (CMC) log files:

```
show logs error [mca | cmc | type=SEVERITY | id=BUNDLE_ID]
```

The command returns information to the console. Because the amount of returned information can be large, use your terminal emulation program tools to capture this information. Plan to analyze this program on a host computer other than the RMC.

In a CMC dump, you can, for example, find one or more headers that resemble the following:

```
***** CMC (Corrected Machine Check) Error Log ( 0x2110000000000001 )

============================================================
CPER Record 0x0000000000000000   Timestamp 2017/09/29 19:45:34
============================================================
```

The `0x2110000000000001` string is the log identifier that you supply as the *bundle_id* to the show logs error command. For example:

```
RMC cli> show logs error cmc
============================================================
CPER Record 0x0000000000000000   Timestamp 2017/09/29 19:45:34
============================================================
Signature Start         0x52455043 (REPC)
Revision                0x0101
Signature End           0xffffffff
Section Count           0x0009 (9 Sections)
Error Severity          0x00000002 (Corrected)
Validation Bits         0x00000002
Record Length           0x00000a58 (2648 Bytes)
Timestamp               0x2017092900194534 (2017/09/29 19:45:34)
Platform ID             00000000-0000-0000-0000000000000000
                        (Invalid)
Partition ID            00000000-0000-0000-0000000000000000
                        (Invalid)
Creator ID              00000000-0000-0000-0000000000000000
                        (Invalid)
Notification Type       2dce8bb1-bdd7-450e-b9ad9cf4ebd4f890
                        (CMC)
Record ID               0x0000000000000000
Flags                   0x00000000
Persistence Information 0x0000000000000000

============================================================
CPER Section Descriptor -  number 0x0001 (1)
============================================================
Section Offset          0x00000308 (776 Bytes)
Section Length          0x00000048 (72 Bytes
.
.
.
```

Example 3

The `show network` command displays network information.

```
RMC cli> show network
-- Network Configuration --

IPv4 Addressing: dhcp
IPv4 Address: 192.168.1.1
IPv4 Netmask: 255.255.255.0
IPv4 Gateway: 137.38.91.1
Hostname: uv4test14-rmc
IPv6 Addressing: dhcp
IPv6 Address: 1111:1111:1111:11:111:1111:1111:1111/64 Scope:Global
IPv6 Address: 1111:1111:1111:11:1::1111/64 Scope:Global
IPv6 Address: 1111::111:1111:1111:1111/64 Scope:Link

-- AUX Network Configuration --

IPv4 Addressing: static
IPv4 Address: 192.168.1.2
IPv4 Netmask: 255.255.0.0
IPv4 Gateway:
IPv6 Addressing: default

-- Network Information --

eth0      Link encap:Ethernet  HWaddr 00:00:00:00:00:00
          inet addr:192.168.1.3  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: 1234::567:89ab:cdef:0123/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
```

```
          RX packets:2209650 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1950104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:414470219 (395.2 MiB)  TX bytes:233440163 (222.6 MiB)
          Base address:0xc000

eth1      Link encap:Ethernet  HWaddr 01:23:45:67:89:ab
          inet addr:192.168.1.3  Bcast:192.168.1.4  Mask:255.255.255.0
          inet6 addr: abcd:ef0:1234:56:789:abcd:ef0:1234/64 Scope:Global
          inet6 addr: 0123::456:789a:bcde:f012/64 Scope:Link
          inet6 addr: 1234:5678:9abc:de:f::0123/64 Scope:Global
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:1610866 errors:0 dropped:43 overruns:0 frame:0
          TX packets:757013 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:249314737 (237.7 MiB)  TX bytes:134176764 (127.9 MiB)
          Base address:0xe000


-- BaseIO --

P000 [r001u01b]:   192.168.1.5      [ab:cd:ef:01:23:45]
                   2345::678:9abc:def0:1234/64 Scope:Link
                   bcde:f0123:4567:89:a::bcd/64 Scope:Global
                   cdef:0123:4567:89:abc:def0:1234:5678/64 Scope:Global


Network Configuration:
==== r001u01b ====
IPv4 Addressing: dhcp


-- Network protocols --

HTTP:     Enabled
HTTPS:    Enabled
IPMI:     Enabled
IPV6:     Enabled
SSH:      Enabled

-- Internal Network Configuration --

Internal BMC Subnet: 172.30.50.0
Internal CMC Subnet: 172.16.0.0
Internal eRMC Subnet: 172.30.60.0
```

Example 4

The `show remote_log_server` command displays the remote log server information.

```
RMC cli> show remote_log_server
-- Remote log server Information --
Server: 10.11.12.135
Port: 514
Protocol: udp
Severity_level: info
```

Example 5

The `show predictive_mem_health` command displays the current status of predictive memory failures reporting on the system.

```
RMC cli> show predictive_mem_health
Predictive Memory health is enabled
```

test

Syntax

`test`

`test ldap [username=`*`USERNAME`*`] [verbose]`

`test remote_log`

`test upi [pnum=0] [verbose]`

Description

Tests the UPI cables, LDAP configurations, or remote log server settings.

Specifiers

USERNAME

Specify the LDAP username you want to test. LDAP username can be case-insensitive.

Example output

```
RMC cli> test upi

Running basic cable placement check...
No errors detected.
Checking UPI port connections and basic link health...

==== r001u01b ====
No errors detected.
Checking link status of UPI ports...

==== r001u01b ====
No errors detected.
Done
RMC cli>
```

```
RMC cli> test ldap

Beginning test...

Ping Test
---------

# ping -c2 fddd:6777:123:234:aabb:5678:ccdd:cac4
# ping6 -c2 fddd:6777:123:234:aabb:5678:ccdd:cac4

Ping Test was successful.


Group Search Test
-----------------
```

```
Attempting LDAP search for group3 in cn=Users,dc=ad1,dc=dmn01 DN scope...

# LDAPTLS_REQCERT=allow
# ldapsearch -LLL -v -x -l 90 -d 4 -H ldaps://
[fddd:6777:123:234:aabb:5678:ccdd:cac4]:636 -b "cn=Users,dc=ad1,dc=dmn01" -D
"cn=ldapAdmin,cn=Users,dc=ad1,dc=dmn01" -W "(&(objectClass=group)
(cn=group3))" cn

Entry for group3 was found.

Attempting LDAP search for group2 in cn=Users,dc=ad1,dc=dmn01 DN scope...

# LDAPTLS_REQCERT=allow
# ldapsearch -LLL -v -x -l 90 -d 4 -H ldaps://
[fddd:6777:123:234:aabb:5678:ccdd:cac4]:636 -b "cn=Users,dc=ad1,dc=dmn01" -D
"cn=ldapAdmin,cn=Users,dc=ad1,dc=dmn01" -W "(&(objectClass=group)
(cn=group2))" cn

Entry for group2 was found.

Attempting LDAP search for group1 in cn=Users,dc=ad1,dc=dmn01 DN scope...

# LDAPTLS_REQCERT=allow
# ldapsearch -LLL -v -x -l 90 -d 4 -H ldaps://
[fddd:6777:123:234:aabb:5678:ccdd:cac4]:636 -b "cn=Users,dc=ad1,dc=dmn01" -D
"cn=ldapAdmin,cn=Users,dc=ad1,dc=dmn01" -W "(&(objectClass=group)
(cn=group1))" cn

Entry for group1 was found.

Group Search Test was successful.


Domain SID Test
---------------

Attempting LDAP search for group3 in cn=Users,dc=ad1,dc=dmn01 DN scope...

# LDAPTLS_REQCERT=allow
# ldapsearch -LLL -v -x -l 90 -d 4 -H ldaps://
[fddd:6777:123:234:aabb:5678:ccdd:cac4]:636 -b "cn=Users,dc=ad1,dc=dmn01" -D
"cn=ldapAdmin,cn=Users,dc=ad1,dc=dmn01" -W "(&(objectClass=group)
(cn=group3))" objectsid cn

 decoded Object SID: S-1-5-21-652678-1122334455-1122334455-1111
settings Domain SID: S-1-5-21-652678-1122334455-1122334455

Domain SID Test was successful.

INFO: Optional USERNAME not provided for test. Skipping User Search test.

LDAP Client Test
----------------

# nslcd --check
NSLCD is running.

LDAP Client Test was successful.

Test is complete.
```

```
RMC cli> test remote_log
```

```
ping test:
----------

# ping -c2 10.100.10.100
Ping Test was successful.

A test log message has been sent to the system log.
Verify remote server for test message.
```

update firmware

Syntax

`update firmware url=`*`PATH_TO_FIRMWARE`* `[dry_run] [reinstall] [exclude_npar_fw]`

`update firmware (saved | url=BUNDLE_URL) [dry_run] [reinstall] [exclude_npar_fw] [chassis=CHASSIS] [pca={bmc,mlb,power}]`

Description

Updates the system firmware.

Specifiers

PATH_TO_FIRMWARE

Specify the path to the firmware. This command assumes the following:

- You downloaded the firmware update bundle from the HPE Support Center.
- The bundle resides on a local computer at your site.

Accepted access methods are `https`, `sftp`, and `scp`.

The firmware also accepts nonstandard ports for `https`, `sftp`, and `scp`.

For example:

```
scp://<user>@<host>:<port>/<path to FW>
https://[<user>@]<host>[:<port>]<https path to FW>
```

Options

`dry_run`

Specify if you want to test the firmware installation.

`reinstall`

Specify if you want to force an installation when the firmware already matches the complex firmware. The complex firmware includes all firmware on the system except the UEFI drivers for IO. You may update the drivers either through the OS online, or offline from a DVD-booted version using the Smart Update Manager tool.

`[exclude_npar_fw]`

Specify if you do not want to update any firmware running on an nPartition, such as BIOS.

upload

Syntax

`upload config (url=URL | file=`*`FILENAME`*`)`

`upload debug url=URL [file=FILENAME]`

`upload idc url=URL [file=FILE]`

`upload npar config (url=URL | file=FILENAME)`

`upload syshist url=URL`

`upload rcu [id=HEX_ID | file=FILENAME] url=URL`

`upload npar attributes (url=URL | file=FILENAME) [pnum=0]`

Description

Transfers a `tar` file that contains files to a different, local computer at your site. The command compresses the `tar` file automatically.

Specifiers

URL

Specify the full path to the target location on a local computer. Accepted transfer methods are `sftp` and `scp`.

The following examples show the supported formats:

- `sftp://user@localhost/path`
- `scp://user@localhost/path`

The command prompts you for the password to the local host computer.

FILENAME

Specify the name of the file. If you do not specify a *FILENAME* name, the system creates and then uploads a debugging or configuration file.

Usage

The `upload config (url=URL | file=FILENAME)` command uploads the configuration file to the specified URL.

The `upload debug url=URL [file=FILENAME]` command uploads the debugging file to the specified URL.

The `upload idc url=URL [file=FILE]` command uploads the archive file to a target system or uploads the specified IDC logs archive file to a target system.

The `upload npar config (url=URL | file=FILENAME)` command uploads the nPartition configuration file to the specified URL.

The `upload syshist url=URL` command uploads the system history file to the specified URL.

The `upload rcu [id=HEX_ID | file=FILENAME] url=URL` command uploads a dump file to the specified URL.

The `upload npar attributes (url=URL | file=FILENAME) [pnum=0]`.

Partition boot options

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.

Administering with HPE OneView GUI

You can administer the HPE Superdome Flex 280 Server using any of the GUI applications:

- HPE OneView
- RMC GUI

HPE OneView is a unified management platform used to administer HPE servers, storage, and networking components. OneView supports the industry standard Redfish APIs that are used for communication with managed systems such as Superdome Flex servers. Using a single instance of HPE OneView, you can administer multiple HPE Superdome Flex servers at a time.

Rack Management Controller (RMC) GUI of a given HPE Superdome Flex 280 Server offers an interface to monitor and manage that server. You cannot administer multiple servers or other elements in your data center using the RMC UI.

HPE OneView

HPE OneView is a converged infrastructure management software product that provides a unified interface for the administration of systems in a data center. Through a single GUI, administrators can automate management and maintenance tasks that have traditionally been performed manually and required several different tools. Within the data center, HPE OneView can manage systems such as the Superdome Flex, storage arrays, and network connectivity.

HPE OneView uses the Redfish interface, an industry-standard RESTful API to administer Superdome Flex 280 server. OneView can manage or monitor up to 80 HPE Superdome Flex 280 servers and HPE Superdome Flex systems.

Advantages of HPE OneView

You can consider using HPE OneView if you have any of the following requirements:

- To administer multiple Superdome Flex and Superdome Flex 280 servers in your data center using a single GUI.
- To administer other compute, storage, and network devices that are supported by HPE OneView.
- To avail the Redfish interface and standard information models to organize the physical and logical elements of your devices.
- To bring standardization into the administration of your servers by using configuration templates.
- To minimize time and improve efficiency in server administration.
- To integrate remote support and view details of the cases filed.

Installing HPE OneView

You can install OneView on any server hardware that meets the requirements described in the *HPE OneView Support Matrix* or see the **table**. For information on the prerequisites, procedure to obtain and install OneView in different virtual machine environments, see *HPE OneView Installation Guide* at **https://www.hpe.com/support/OneView-IG**. HPE releases new versions of OneView more than twice a year. They include new features and updates. You must update to the required versions to avail the new features.

HPE OneView features

HPE OneView includes many features that facilitate the administration of managed devices. It includes the administrative interface called **Global Dashboard** and a **Map View**. You can use the interface to understand the relationships of various physical and logical elements. It also provides capabilities to monitor and manage your infrastructure and integration with **OneView Remote Support**.

Global Dashboard

Use the single-pane-of-glass administrative interface to monitor and manage the HPE Superdome Flex 280 Server.

Map View

Use the **Map View** to configure and view the relationships between logical and physical resources in your data center. The **Map View** provides a complete view of your infrastructure, the associations of various elements and helps you understand the impact of different actions.

Smart Search

Use the **Smart Search** option to search for resources in real time.

Server hardware inventory

When a server is added or refreshed, either as monitored or managed, HPE OneView collects inventory information about that server and the devices inside the server. Any inventory information that is required for applying server profiles is collected during the actual add or refresh operation. Other inventory information that is not required for profiles is collected a short time after, using a low priority background process to conserve system resources.

Some inventory items cannot be collected unless the server is powered on. In such cases, a notification explaining why the inventory collection is not collected is visible at the top of individual inventory pages.

Inventory information collected while adding or refreshing a server

General server hardware information

Includes model name, product ID, and serial number.

Firmware and driver inventory

A list of all the devices in the server that have firmware and the version of firmware installed on that device.

Network adapters and ports

A list of the network adapters in the server, and all ports in the adapter. The port information includes MAC and WWPN numbers.

Other inventory information collected using the background process

The following information is available for HPE Superdome Flex 280 Server.

PCI device inventory

A list of all the PCI devices installed in that server that are not already inventoried, with detailed information about each discovered device.

System memory

A list of all the memory slots in that server, with detailed information about any DIMMs installed in those slots.

Standard and Managed modes of HPE OneView

- Standard or Monitor mode is provided as an appliance when deployed. Standard mode enables:

- The discovery of servers
- A detailed inventory of physical and logical resources
- Comprehensive health monitoring, activities/alerts, and reporting

- With Managed or Advanced mode, you can perform functions such as changing the BIOS settings on a server and defining a server profile for efficiently standing up and deploying servers in the future.

HPE OneView will automatically enable the license for Managed mode if HPE OneView version is 5.0 or newer and HPE Superdome Flex 280 firmware version is 1.0.x and newer.

HPE OneView user guides, support matrixes that include supported features, and other manuals are available on the **Enterprise Information Library**.

To view help in the HPE OneView appliance, click  .

Add a rack manager

Prerequisites

Privileges: Infrastructure administrator or Server administrator.

About this task

HPE OneView supports adding rack managers with IPv4, IPv6, or both IPv4 and IPv6 addresses depending on the network configuration.

You can also use the hostname to add the rack manager. If the hostname resolves to both IPv4 and IPv6 addresses, the rack manager is added using only the IPv4 address as IPv4 address is preferred.

After the rack manager is added, communication with the rack manager happens through the IP address that was used to add the rack manager. If the IP address is not reachable, HPE OneView does not fall back to the other IP addresses that are associated with the added rack manager.

You can add rack managers as managed or monitored. HPE OneView automatically applies either the HPE OneView Standard license or the HPE OneView Advanced license to the rack manager based on the firmware version installed. HPE OneView discovers and monitors the hardware subcomponents of the rack manager.

HPE OneView supports adding rack managers with IPv4, IPv6, or both IPv4 and IPv6 addresses depending on the network configuration in HPE OneView. You can add the rack manager using the IPv4 address, IPv6 address or with the hostname.

When you add a rack manager, you can select the already uploaded firmware bundle from the firmware baseline option. Once selected, HPE OneView updates the server with the firmware that matches the specified baseline. The baseline is set for each of the rack manager platform components such as chassis, systems (nPartitions), and Rack Management Controller (RMC). You can also choose to manage the firmware update of the rack manager platform components manually.

Procedure

1. From the main menu, select **SERVERS** > **Rack Managers**, and do one of the following:
   - Click **+ Add rack manager** in the master pane.
   - Select **Actions** > **Add**.
2. Enter the **IP address or host name**.

3. Enter the **Credentials**.

   NOTE: Users with **Create** permissions that are restricted by scope must assign resources to one or more restrictive scopes to be able to manage a resource. Users with **Create** permissions that are not restricted by scope are not required to assign resources to a scope to be able to manage a resource. Users with no scope restrictions can assign any resource to any scope.

4. Select the **Firmware baseline** options.
5. Click **Add** to add the rack manager or click **Add+** to add more rack managers.
6. Verify that the rack manager has been added by confirming it is listed in the master pane.

More information

- **Enable remote support for a rack manager**
- **Adding and monitoring rack managers**
- **Superdome Flex firmware bundle**

Remote support for rack manager

Once remote support is enabled for the rack manager, you can configure and edit the remote support settings for that rack manager.

The support identifier is based on the rack manager serial number and product number. HPE OneView Remote Support performs entitlement against the new product number and serial number. Entitlement is checked again by the support center agent who handles new support cases.

NOTE: To refresh contract and warranty information, select **Actions** > **Update contract and warranty**.

Configure remote support for a rack manager

Prerequisites

- Privileges: Infrastructure administrator or Server administrator.
- You have **enabled remote support** for the rack manager.

Procedure

1. From the main menu, select **SERVERS** > **Rack Managers**.
2. Select the rack manager you want to register with Hewlett Packard Enterprise support services.
3. Select **Actions** > **Edit remote support settings**.
4. In the **Edit Remote Support Settings** dialog box, select **Enable remote support**.
5. Set the properties for **Contacts**, **Channel Partners**, and **Warranty and Contract**.
6. Click **OK**.
7. Verify the remote support settings by selecting **Remote Support** from the view selector in the details pane.

Collect remote support data for rack managers

Prerequisites

- Privileges: Infrastructure administrator or Server administrator.
- You have **enabled remote support** for the rack manager.

About this task

You can collect remote support data that is automatically sent to Hewlett Packard Enterprise for analysis. You can collect only basic information from a rack manager.

Procedure

1. From the main menu, select **SERVERS** > **Rack Managers**.
2. Select the rack manager you want to collect remote support data.
3. Select **Actions** > **Collect remote support data**.
4. In the **Collect Remote Support Data** dialog box, click **Yes, collect data**.
5. Verify the data collection status in the details pane or the **Activity** page.

Edit a rack manager

Prerequisites

Privileges: Infrastructure administrator or Server administrator.

About this task

You can edit a rack manager to change its name.

Procedure

1. From the main menu, select **SERVERS** > **Rack Managers** and do one of the following:
   - In the master pane, select the rack manager you want to edit, and select **Actions** > **Edit**.
   - Hover your pointer in the details pane, and click the **Edit** icon.
2. Edit the values shown on the screen.
3. Confirm your changes and click **OK** to apply them.
4. Verify the changes by checking the rack manager information in the details pane.

Reset a rack manager

Prerequisites

- Privileges: Infrastructure administrator or Server administrator.
- The rack manager is successfully added and is managed by the HPE OneView appliance.
- Ensure that there are no ongoing operations on the rack manager.

About this task

You can reset a Rack Management Controller (RMC) from HPE OneView. Resetting a Rack Management Controller does not affect any of the running partitions. Resetting a Rack Management Controller will cause a loss of connectivity between the rack manager and HPE OneView. Once the reset operation completes, connectivity is restored automatically.

Procedure

1. From the main menu, select **SERVERS** > **Rack Managers**.
2. Select the rack manager you want to reset.
3. Select **Actions** > **Reset**.

   If the selected rack manager is in `Unmanaged` state, the **Reset** option is disabled.

   All the other rack manager actions will not be allowed when the reset action is in progress and an error message is displayed if you trigger any other action.
4. Review the confirmation message, and then click **Yes, reset**.

   An error message is displayed if:

   - Any operations are ongoing on the rack manager.
   - The reset operation is not supported by the firmware running on the HPE Superdome Flex.
5. To verify the progress of the reset action, check the general state of the rack manager. The state is displayed as follows:

   - **Resetting RMC:** This state is displayed when the resetting is in progress.
   - **Monitored:** This state is displayed once the reset action is completed and the rack manager is reachable.

Utilization metrics

HPE OneView supports CPU, Memory, Power and Temperature utilization metrics for HPE Superdome Flex Server and HPE Superdome Flex 280 Server. For more information see, HPE OneView documentation.

When to use a server profile

A server profile allows you to do the following tasks:

- Manage the server hardware configuration separately from the actual server hardware. Capture significant portions of the server configuration in one place to simplify server configuration.
- Reapply the configuration to the server hardware if the server hardware is serviced or replaced.
- Define the server configuration before the server hardware is installed.

Depending on the hardware environment, you can configure the following settings:

- **Firmware** (optional):
  - Specify a firmware baseline to update the server BIOS firmware as well as firmware on the Rack Management Controller (RMC) and Board Management Controller (BMC). The firmware settings in server profile is supported for only Superdome Flex 280 servers.

    You can use the HPE OneView server profile to manage the I/O firmware of an HPE Superdome Flex 280 Server and HPE Superdome Flex Server in the offline mode.
- **BIOS settings** (optional):
  - Specify the BIOS settings to apply on the selected server hardware.
- **Connections** (required for Virtual Connect):
  - Describes which Fibre Channel SANs are accessible by the server hardware.
- **Storage Attachments:**
  - Lists the storage volumes that are accessible by the server hardware, and supports creation of storage volumes. Supports HPE 3PAR and HPE Primera storage systems and Brocade FOS switches. Storage volumes cannot be configured for boot on HPE Superdome Flex Server and HPE Superdome Flex 280 Server.

When to use a server profile template

A server profile template allows you to do the following tasks:

- Update many server profiles with the same configuration.
- Easily generate new server profiles from one template.
- Control configuration changes for multiple servers at once. HPE OneView checks compliance in all the server profiles that are referenced to the template.
- Automatically resolve the compliance issues using the **Update from Template** action. The server profile configuration is adjusted to match the server profile template for most changes. Some changes to volumes and volume attachments are not automatically updated with the **Update from Template** action. You may have to manually configure volume attachments in the server profile.

NOTE: Some of the values in the **Update from Template** screen can be edited even when the server power is on. **Update from Template** is able to determine and indicate when the user needs to power off the server while changing the values.

The conditions applicable to edit the server profile settings while the server hardware is powered on or powered off, are also applicable when you are editing values in the **Update from Template** screen.

OneView capabilities supported on HPE Superdome Flex family of servers

Table 2: HPE OneView Monitoring and Management Capabilities supported on HPE Superdome Flex and on HPE Superdome Flex 280

OneView feature	HPE Superdome Flex		HPE Superdome Flex 280	
	Min OneView version	Min firmware version	Min OneView version	Min firmware version
Monitor mode				
RMC, partition and chassis inventory	4.1	3.0.x	5.5	1.0
Events (Health alerts)	4.1	3.0.x	5.5	1.0
Fan and Power supply inventory	4.2	3.0.x	5.5	1.0
Events (lifecycle)	4.2	3.0.x	5.5	1.0
Remote Support	4.2	3.0.x	5.5	1.0
Power controls (on/off nPar)	4.2	3.0.x	5.5	1.0
IPv6 support	5.2	3.0.x	5.5	1.0
RMC connectivity monitoring and event subscription monitoring	5.2	3.0.x	5.5	1.0
Launch RMC web interface from OneView UI	5.2	3.0.x	5.5	1.0
Reset RMC from OneView UI	5.2	3.0.x	5.5	1.0
Notify when a Superdome Flex server is forcibly added to another OneView appliance	5.2	3.0.x	5.5	1.0
OneView Remote Support for Superdome Flex with IPv6	5.3	3.0.x	5.5	1.0
Testing systems connectivity to the HPE Remote Support Data Center from Superdome Flex	5.4	3.0.x	5.5	1.0
Device Inventory	5.5	3.0.x	5.5	1.0

Table Continued

OneView feature	HPE Superdome Flex		HPE Superdome Flex 280	
Firmware upgrade when Superdome Flex is added to OneView appliance	5.5	3.0.x	5.5	1.0
Rack manager Inventory reports	6.00	3.0.x	6.00	1.0
Port inventory	6.00	3.30.x	6.00	1.0
Launch nPar remote web console from OneView UI	6.2	3.30.x	6.2	1.0
Power and thermal utilization metrics	6.2	3.30.x	6.2	1.0
Cooling fan speed information	6.2	3.30.x	6.2	1.0
System memory (DIMMs) inventory	6.3	3.0.x	6.3	1.0
Storage inventory (internal disks)	6.3	3.10.x	5.5	1.0
Notifications for new server firmware updates	7.1	3.55.8	7.1	1.35.12
Managed mode				
Firmware update	5.0	3.0.x	5.5	1.0
One-Time Boot settings for nPar	5.0	3.0.x	5.5	1.0
Firmware update while adding Rack manager	5.5	3.0.x	5.5	1.0
Edit the name of a Rack manager	5.5	3.0.x	5.5	1.0
Create, edit, and remove partitions	7.2	3.40.x	NA	NA
Managed mode (via Server profile)				
BIOS settings via server profile	5.0	3.0.x	5.5	1.0
Secure Boot settings[1]	5.2	3.0.x	5.5	1.0
Server firmware update	NA	NA	6.20	1.0
I/O firmware update	7.0	3.50.x	6.5	1.2
			7.2	1.3
Connections and SAN storage management	6.30	3.0.x	6.30	1.0

[1] Secure boot keys are restored to defaults when ‘set npar default all’ or equivalent operations are executed. This means that any customizations to the Secure Boot settings such as update DBX settings will lost and must be reapplied.

Remote management with Redfish

The Redfish standard integrates easily with commonly used tools by specifying a `RESTful` interface. Redfish uses `JSON` and `OData` constructs to facilitate scripting and organization of server management data. Redfish is the main API to manage the HPE Superdome Flex 280 Server through the RMC. Tools like OpenStack and HPE OneView use it to get information about the system, control it, and get Redfish events, and alerts to monitor the system. These tasks also be done, using `Redfishtool` or your own scripting methods.

To learn more about Redfish, start at the **Redfish Standard Site**.

NOTE: HPE OneView version 5.5 or later is supported (and recommended) for monitoring the HPE Superdome Flex 280 Server system.

As an alternative to the procedure in this topic, use the `ssh` command to connect with an RMC. Log in as the administrator user, or any other user you have configured.

Redfish can be used without any particular tool. Simple `curl` commands, or `perl` , `python`, or PowerShell scripting that sends the right `JSON` data over `https` works well. However, the Distributed Management Task Force (DMTF) has built a specific scripting tool for interacting with systems that support the standard, called `Redfishtool`. `Redfishtool` is able to walk the tree, and complete common tasks. These tasks include gathering the health of objects within the system, and performing actions.

For more information about `Redfishtool`, see **https://github.com/DMTF/Redfishtool**.

You can use the `Redfishtool` commands remotely from a laptop or other computer that is on the same local network as the rack management controller (RMC). The `Redfishtool` commands rely on Python 3.4 or later, which is commonly included in Linux distributions. Python 3.4 can be downloaded for Windows and Linux from **https://www.python.org/**. You can manage a system in the following ways:

The remote management commands use the following terminology:

- The term **HPE Superdome Flex 280 Server system** includes the server, RMC, and the board management controllers (BMCs).
- The term **HPE Superdome Flex 280 Server** refers only to the server component of the system. The server is enclosed within each chassis. The RMC and the BMCs are not part of the server itself.

The RMCs and BMCs have no power on or power off capability. When power is applied to the HPE Superdome Flex 280 Server, the RMC has power, and the BMCs have power. You can issue `Redfishtool` commands to the RMC and to the BMCs as long as power is applied to the system.

NOTE: This documentation shows `Redfishtool` command output. Depending on the revision level of the `Redfishtool` command you use on your remote console, the command output you see can differ from the output shown in this documentation.

Out-of-Band management with Redfishtool - general procedure

About this task

The `Redfishtool` is a Redfish client that has to be installed on a computer with network connectivity to the RMC. The tool then can be used to power on or off the HPE Superdome Flex 280 Server and obtain status information.

Procedure

1. Ensure that the computer running the `Redfishtool` has `https` connectivity to the managed RMC.
2. Ensure that Python 3.4 or later is installed, and working correctly on the workstation running `Redfishtool`.
3. Follow the instructions for downloading all the files for `Redfishtool` from **https://github.com/DMTF/Redfishtool**.

NOTE: The implementation of Redfish on the server only uses `https`. One command argument to include, that is not in all the DMTF `Redfishtool` examples (but is a valid option), is `-S Always` to always use `https`.

Use the following command to get the `root` of the Redfish tree with RMC target `hostname=flex_rmc`, and the default administrator account and password:

```
$> python3 ~/Redfishtool/redfishtool.py -r flex_rmc -u <RMC login> -p
<Password> -S Always root
```

where *`RMC login`* is the user name, for example `Administrator`, and *`Password`* is the password for that account. For the rest of this chapter, we will use `Administrator` and `DummyPwd` for the user password.

IMPORTANT: Use your own unique password on your RMC for security purposes.

In some network environments, you may need to override a proxy to make things work correctly.

For example, from a Linux workstation the following command overrides the proxy server once and then retrieves the root properties of the remote RMC:

```
$> https_proxy='' python3 ~/Redfishtool/redfishtool.py -r flex_rmc -u
Administrator -p DummyPwd -S Always root
```

You can override the proxy server during an entire interactive session with:

```
$> export https_proxy=''
```

Some subsystems have built in help in the `examples` command. In this Bash shell example, the following command displays all the subcommands available to get or set the `systems` subsystem properties:

```
$> python3 redfishtool.py -r flex_rmc -u Administrator -p DummyPwd -S
Always Systems examples
redfishtool -r<ip> Systems                                  # shows the systems collection
redfishtool -r<ip> Systems list                             # lists Id, Uri, AssetTag for all systems
redfishtool -r<ip> Systems -I <id>                          # gets the system with Id=<d>
redfishtool -r<ip> Systems -M AssetTag:12345                # gets the system with AssetTag=12345
redfishtool -r<ip> Systems -L <sysUrl>                      # gets the system at URI=<systemUrl
redfishtool -r<ip> Systems -F                               # get the First system returned (for debug)
redfishtool -r<ip> Systems -1                               # get the first system and verify that there
is only one system
redfishtool -r<ip> Systems -I <id> patch {A: B,C: D,...}    # patch the json-formatted {prop: value...}
data to the object
redfishtool -r<ip> Systems -I <id> reset <resetType>        # reset a system.  <resetType>=the redfish-defined
values: On, Off, gracefulOff...
redfishtool -r<ip> Systems -I <id> setAssetTag <assetTag>   # set the system's asset tag
redfishtool -r<ip> Systems -I <id> setIndicatorLed  <state>  # set the indicator LED.
<state>=redfish defined values: Off, Lit, Blinking
redfishtool -r<ip> Systems -I <id> setBootOverride <enabledVal> <targetVal> #-- set Boot Override properties.
<enabledVal>=Disabled|Once|Continuous
redfishtool -r<ip> Systems -I<Id> Processors                # get the processors Collection
redfishtool -r<ip> Systems -I<Id> Processors list           # lists Id, Uri, and Socket for all
processors in system with Id=<Id>
redfishtool -r<ip> Systems -I<Id> Processors -i 1           # get the processor with id=1 in
system with Id=<Id>
redfishtool -r<ip> Systems -L <sysUrl> Processors -m Socket:CPU_1  # get processor with property
Socket=CPU_1, on system at url <sysUrl>
```

To list the partitions:

```
$> python3 redfishtool.py -r flex_rmc -u administrator -p DummyPwd -S Always Systems
{
    "Name": "Computer System Collection",
    "@odata.id": "/redfish/v1/Systems",
    "@odata.context": "/redfish/v1/$metadata#ComputerSystemCollection.ComputerSystemCollection",
    "@odata.type": "#ComputerSystemCollection.ComputerSystemCollection",
    "Members": [
        {
            "@odata.id": "/redfish/v1/Systems/Partition0"
        }
    ],
    "Members@odata.count": 1
}
```

To get the top-level model for a partition, in this case number 0:

```
{
    "Body": {
        "@odata.id": "/redfish/v1/Systems/Partition0",
        "@odata.type": "#ComputerSystem.v1_15_0.ComputerSystem",
        "Actions": {
            "#ComputerSystem.Reset": {
                "ResetType@Redfish.AllowableValues": [
                    "On",
                    "ForceOff",
                    "ForceRestart",
                    "GracefulRestart",
                    "GracefulShutdown",
                    "PowerCycle"
                ],
                "target": "/redfish/v1/Systems/Partition0/Actions/ComputerSystem.Reset"
            }
        },
        "Bios": {
            "@odata.id": "/redfish/v1/Systems/Partition0/Bios"
        },
        "BiosVersion": "1.20.190",
        "Boot": {
            "BootNext": null,
            "BootOptions": {
                "@odata.id": "/redfish/v1/Systems/Partition0/BootOptions"
            },
            "BootOrder": [
                "Boot0013",
                "Boot0001",
                "Boot0002",
                "Boot0003",
                "Boot0004",
                "Boot0005",
                "Boot0006",
                "Boot0007",
                "Boot0008",
                "Boot0009",
                "Boot000A",
                "Boot000B",
                "Boot000C",
                "Boot000D",
                "Boot000E",
                "Boot000F",
                "Boot0010",
                "Boot0011"
            ],
            "BootSourceOverrideEnabled": "Disabled",
            "BootSourceOverrideEnabled@Redfish.AllowableValues": [
                "Continuous",
                "Disabled",
                "Once"
```

```
    ],
    "BootSourceOverrideMode": "UEFI",
    "BootSourceOverrideMode@Redfish.AllowableValues": [
        "UEFI"
    ],
    "BootSourceOverrideTarget": "None",
    "BootSourceOverrideTarget@Redfish.AllowableValues": [
        "None",
        "BiosSetup",
        "Cd",
        "Hdd",
        "Pxe",
        "RemoteDrive",
        "SDCard",
        "UefiBootNext",
        "UefiHttp",
        "UefiShell",
        "Usb"
    ],
    "HttpBootUri": null
},
"EthernetInterfaces": {
    "@odata.id": "/redfish/v1/Systems/Partition0/EthernetInterfaces"
},
"HostName": "hostname",
"Id": "Partition0",
"LastResetTime": "2021-10-18T18:29:39Z",
"Links": {
    "Chassis": [
        {
            "@odata.id": "/redfish/v1/Chassis/r001u01b"
        },
        {
            "@odata.id": "/redfish/v1/Chassis/r001u06b"
        }
    ],
    "Chassis@odata.count": 2,
    "ManagedBy": [
        {
            "@odata.id": "/redfish/v1/Managers/RMC"
        }
    ],
    "ResourceBlocks": [
        {
            "@odata.id": "/redfish/v1/CompositionService/ResourceBlocks/r001u01b"
        },
        {
            "@odata.id": "/redfish/v1/CompositionService/ResourceBlocks/r001u06b"
        }
    ],
    "ResourceBlocks@odata.count": 2
},
"Memory": {
    "@odata.id": "/redfish/v1/Systems/Partition0/Memory"
},
"MemorySummary": {
    "Metrics": {
        "@odata.id": "/redfish/v1/Systems/Partition0/MemorySummary/MemoryMetrics"
    },
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    },
    "TotalSystemMemoryGiB": 3071,
    "TotalSystemPersistentMemoryGiB": 0
},
"Name": "Npar 0",
"NetworkInterfaces": {
    "@odata.id": "/redfish/v1/Systems/Partition0/NetworkInterfaces"
```

```
},
"Oem": {
    "Hpe": {
        "@odata.type": "#HpeNpar.v1_0_0.HpeNpar",
        "DCD": {},
        "IPv4Addresses": [
            {
                "Address": "10.11.12.135"
            }
        ],
        "OSType": "85",
        "OSVersion": "15-SP2",
        "OV": {},
        "ProductId": "1590PID02020001",
        "SystemUsage": {}
    }
},
"PCIeDevices": [
    {
        "@odata.id": "/redfish/v1/Chassis/r001u01b/PCIeDevices/7"
    },
    {
        "@odata.id": "/redfish/v1/Chassis/r001u01b/PCIeDevices/8"
    }
],
"PCIeDevices@odata.count": 2,
"PCIeFunctions": [],
"PCIeFunctions@odata.count": 0,
"PowerState": "Off",
"ProcessorSummary": {
    "Count": 8,
    "LogicalProcessorCount": 144,
    "Metrics": {
        "@odata.id": "/redfish/v1/Systems/Partition0/ProcessorSummary/ProcessorMetrics"
    },
    "Model": "Intel(R) Xeon(R) Platinum 8353H CPU",
    "Status": {
        "Health": "OK",
        "State": "Enabled"
    }
},
"Processors": {
    "@odata.id": "/redfish/v1/Systems/Partition0/Processors"
},
"SecureBoot": {
    "@odata.id": "/redfish/v1/Systems/Partition0/SecureBoot"
},
"SerialConsole": {
    "MaxConcurrentSessions": 30,
    "SSH": {
        "ConsoleEntryCommand": "connect npar pnum=p0 nocache steal",
        "HotKeySequenceDisplay": "ctrl-] q",
        "Port": 22,
        "ServiceEnabled": true,
        "SharedWithManagerCLI": true
    }
},
"Status": {
    "Health": "OK",
    "HealthRollup": "OK",
    "State": "Enabled"
},
"Storage": {
    "@odata.id": "/redfish/v1/Systems/Partition0/Storage"
},
"SystemType": "PhysicallyPartitioned",
"TrustedModules": [
    {
        "FirmwareVersion": "0x00490040",
```

```
                "FirmwareVersion2": "0x44a01a03",
                "InterfaceType": "TPM2_0",
                "Status": {
                    "State": "Enabled"
                }
            }
        ],
        "UUID": "9003367f-1409-584f-a371-632a9d1110cd",
        "VirtualMedia": {
            "@odata.id": "/redfish/v1/Systems/Partition0/VirtualMedia"
        },
        "VirtualMediaConfig": {
            "ServiceEnabled": true
        }
    },
    "Metadata": {
        "_Collection": "/redfish/v1/Systems",
        "_DescribedBy": "http://redfish.dmtf.org/schemas/ComputerSystem.v1_15_0.json",
        "_ETag": "\"26a9e52b305c4d6a09818b60c6101701\"",
        "_LastChangeTime": 1634642932.3270605,
        "_Uri": "/redfish/v1/Systems/Partition0"
    }
}
```


Note that the health of that partition is a property in the preceding list:


```
$> python3 redfishtool.py -r flex_rmc -u administrator -p DummyPwd -S Always Systems -I Partition0 -P Status
{
    "Status": {
        "State": "Enabled",
        "Health": "OK"
    }
}
```


The tool also includes the ability to set up alert monitoring, and can walk the Redfish tree to pull all the health status.

For more information, see:

- **Redfish Standard Site** – hosted by the Distributed Management Task Force
- **Redfish - Simple, Modern and Secure Management for Multi-Vendor Cloud and Web-Based Infrastructures** – Technical note
- **DSP2044: Redfish White Paper** – more white papers available at: **https://www.dmtf.org/standards/redfish**

Management with ipmitool

This section describes HPE Superdome Flex 280 Server support for the Intelligent Platform Management Interface (IPMI) protocol. HPE Superdome Flex 280 Server also supports the Redfish manageability standard for out-of-band management. Redfish is a newer, modern method for interfacing with management processors, using RESTful HTTPS and JSON protocols for greater flexibility and security.

The default IPMI user name on RMC is ADMIN and the default IPMI user name for eRMC is admin (note the all UPPER vs. all lower case). Default IPMI user password is the same as the default administrator password which is printed on the pull tab label.

NOTE: IPMI is disabled by default and must be enabled in the RMC by using the enable ipmi command. IPMI is also disabled after performing firmware updates or using the reset factory command.

NOTE: IPMI is only supported for use to remotely interact and control the system through the RMC when all the chassis in the system are included in one large nPartition. Any other configuration is outside the scope of the IPMI standard.

Therefore if a partition definition exists that does not contain all chassis in the complex, or if two or more partitions are defined, use Redfish to control and manage it instead of IPMI. Redfish is supported for operation in all server configurations.

For details about the industry standard release of Redfish, see **https://redfish.dmtf.org**. To download Redfishtool, go to **https://github.com/DMTF/Redfishtool**.

Redfish can be used for gathering status, inventory, and health information. Redfish can also be used to subscribe to alerts, controlling power on the server. Redfish is the interface used by software such as HPE OneView.

Redfish can also be used directly without Redfishtool, using simple Python, Perl, or other scripts. Redfish also supports properly formed Linux URL commands and some browser-based JSON web add-ons. Redfishtool is designed for people to get information and manage systems explicitly using Redfish, rather than generically using HTTPS and JSON.

The HPE Superdome Flex 280 Server supports IPMI. You can access the IPMI v1.5/v2.0 interface through the ipmi command. IPMI management software is included in most Linux distributions and in IPMI-compliant management applications. For more information about the ipmitool command, see the **https://github.com/ipmitool/ipmitool**.

NOTE: IPMI is not recommended for interactive sessions.

You can use the ipmitool commands remotely from a laptop or other computer that is on the same local network as the RMC.

More information

Remote management with Redfish

Create a new IPMI user

1. To create a new IPMI user, set the user name and password using **ipmitool** or **RMC CLI**.
2. After the user is created, provide the right privileges and enable the user.

Creating an IPMI user using ipmitool through IPMI LAN

Procedure

1. Create an IPMI user. In this example, the chosen user name is "ipmiuser" and user ID is 6.

   ```
   remotehost% ipmitool -I lanplus -H flex-rmc -U ADMIN -P PASSWORD user set name 6
   ipmiuser
   ```

2. Set the password for user ID 6.

   ```
   remotehost% ipmitool -I lanplus -H flex-rmc -U ADMIN -P PASSWORD user set password 6
   Password for user 6:
   Password for user 6:
   Set User Password command successful (user 6)
   ```

3. Set the channel access and privileges.

   NOTE: The channel number for IPMI LAN must be 1 for the RMC and 8 for the eRMC. The channel number used in this example is 1 and the privilege level is 4 (administrator).

   ```
   remotehost% ipmitool -I lanplus -H flex-rmc -U ADMIN -P PASSWORD channel setaccess
   1 6 ipmi=on privilege=4
   ```

4. Enable the new user.

   ```
   remotehost% ipmitool -I lanplus -H flex-rmc -U ADMIN -P PASSWORD user enable 6
   ```

Creating an IPMI user using RMC CLI

Procedure

1. Create an IPMI user with user name "ipmiuser" and user ID 6.

   ```
   RMC cli> ipmi command="user set name 6 ipmiuser"
   ```

2. Set a password for user ID 6.

   ```
   RMC cli> ipmi command="user set password 6"
            Password for user 6:
            Password for user 6:
            Set User Password command successful (user 6)
   ```

3. Set the channel access and privileges.

   The channel number used in this example is 1, and the privilege level is 4 (administrator).

   ```
   RMC cli> ipmi command="channel setaccess 1 6 ipmi=on privilege=4"
   ```

4. Enable the new user.

   ```
   RMC cli> ipmi command="user enable 6"
   ```

Retrieving ipmi help output

About this task

The following procedure explains how to retrieve ipmi help output.

Procedure

1. Log into the rack management controller (RMC) as the `administrator` user.
2. Enter the following command:

   ```
   RMC cli> ipmi command=help
   ```

3. Press `q` to exit the help display.

Running IPMI commands on the rack management controller (RMC) - general procedure

About this task

The RMC supports a limited set of IPMI commands that you can use to power on and power off the system, or obtain RMC status information. When you run an IPMI command on the RMC, it returns information about the RMC only.

Use the `ssh` command to connect with an RMC, and log in as the `administrator` user. Enter your `ipmi` commands.

```
RMC cli> bmc exec "ipmi chassis power status" bmc_id
```

Out-of-band management with ipmitool

Procedure

1. Make sure that your local computer is on the same network as the RMC.
2. Enter an `ipmitool` command in the following format.

   ```
   local_computer% ipmitool -I lanplus -H host -U admin -P password cmd
   ```

   The parameters are as follows:

   - For *host*, specify the hostname (preferred) or IP address of the RMC you want to target.
   - The `admin` user name.
   - For *password*, specify the RMC `ipmi` password.

     Use the password that is in effect at this time. The initial installation instructions that explained how to attach the system to your site network directed you to change the factory default `ipmi` password. If you changed the `ipmi` password at that time, provide the new `ipmi` password.

     If you did not specify a site-specific `ipmi` password, use the factory-default RMC password. The factory-default RMC password appears on the password sticker. The password sticker is a bar coded sticker that appears on your system.

     For more information about the placement of the password sticker, see the following:

     Configuring HPE Superdome Flex 280 Server

   - For *cmd*, specify the specific command you want to run.

Running an ipmi command against a baseboard management controller (BMC) - general procedure

Procedure

1. Use the ssh command to connect to the rack management controller (RMC).

   Log into the RMC as the administrator user.

   This is necessary if you want to run ipmi commands on the system BMCs.

2. Specify the command that targets a specific BMC.

   To target a BMC, provide BMC credentials on the ipmi command. The user name is admin.

   Use the password that is in effect at this time. The initial installation instructions that explained how to attach the system to your site network directed you to change the factory default ipmi password. If you changed the ipmi password at that time, provide the new ipmi password.

   If you did not specify a site-specific ipmi password, use the factory-default RMC password. The factory-default RMC password appears on the password sticker. The password sticker is a bar coded sticker that appears on your system.

   For more information about the placement of the password sticker, see the following:

   Configuring HPE Superdome Flex 280 Server

Running an ipmi command against one BMC

About this task

The following procedure explains how to log into an RMC and then target an ipmi command to one BMC.

NOTE: The user name is different for RMC and eRMC. For example, **ADMIN** and **admin** respectively for ipmitool.

eRMC and RMC have the same set of commands for ipmitool.

To run an ipmi command on one BMC

Procedure

1. To log into the RMC, use the ssh command in the following format.

   ```
   remotehost% ssh administrator@host
   ```

   For *host*, specify the hostname (preferred) or IP address of the RMC.

   For example:

   ```
   remotehost% ssh administrator@flex-rmc
   ```

2. Enter the RMC password when prompted.

3. Use the following command to target the BMC.

   ```
   RMC cli> bmc "ipmi cmd" bmc_id
   ```

   The variables in this command are as follows.

- For *cmd*, specify one of the `ipmitool` commands. You cannot specify the `exec` or `shell` commands, but all other commands are accepted.
- For *bmc_id*, specify the ID of a specific BMC.

Running an `ipmi` command against all BMCs

About this task

The following procedure explains how to log into an RMC and then target an `ipmi` command to all BMCs.

To run an `ipmi` command on all BMCs

Procedure

1. Use the `ssh` command in the following format to log into the RMC.

   ```
   remotehost% ssh administrator@host
   ```

   For *host*, specify the hostname (preferred) or IP address of the RMC.

   For example

   ```
   remotehost% ssh administrator@flex-rmc
   ```

2. Enter the RMC password when prompted.
3. Use the following command to target the BMCs.

   ```
   RMC cli> bmc ipmi cmd
   ```

   For *cmd*, specify one of the `ipmi` commands. You cannot specify the `exec` or `shell` commands, but all other commands are accepted.

Retrieving RMC or BMC power status information

Assume the following:

- You are logged into a Linux computer as a regular user, not the root user or the administrator user.
- The hostname of the RMC is `flex-rmc`.
- The chassis BMC IDs are `r001u01b` and `r001u06b`.

Example 1: You can use the following command to obtain information about the power status on the RMC.

```
remotehost% ipmitool -I lanplus -H flex-rmc -U ADMIN -P PASSWORD \
power status
Chassis Power is on
```

In this example, assume that the user already added a user with the name `administrator` to IPMI user.

Example 2: You can use the following commands to obtain information about the power status on chassis BMC `r001u01b`.

```
remotehost% ssh administrator@flex-rmc
password:######
```

```
RMC cli> bmc exec "ipmi power status" r1u1b
Chassis Power is on
```

In this example, assume that the user supplied the `administrator` password for the RMC when prompted.

Issuing power cycle commands

The following command sends power control requests to the entire HPE Superdome Flex Server system.

```
remotehost% ipmitool -I lanplus -H host -U ADMIN -P password \
chassis power action
```

For *host*, specify the hostname (preferred) or IP address of the RMC.

For *action*, specify `status`, `on`, `off`, `cycle`, `reset`, `diag`, or `soft`.

If you want to watch the server boot process, use the `ipmitool sol activate` command to open up a serial console. For information about the `sol activate` command.

NOTE: The `ipmitool` power command in this topic addresses the entire server, not any of the individual chassis. Hewlett Packard Enterprise recommends that you do not attempt to issue power commands to any individual server chassis.

The RMC `power on` command is an alternative to the `ipmitool power` command. For more information about the RMC `power` commands, see command.

The `ipmitool` power command does not work when there are two or more partitions.

More information

Opening a serial console

Sending a nonmaskable interrupt (NMI) signal to write a crash dump

You can send a nonmaskable interrupt (NMI) signal to the entire HPE Superdome Flex 280 Server system, which responds by writing a system crash dump.

```
remotehost# ipmitool -I lanplus -H flex-rmc -U ADMIN -P password \
chassis power diag
```

Listing information for field replaceable units (FRUs)

The `fru list` command lists information about each FRU.

NOTE: The remote host will not be running the same version of `ipmitool` as runs on the server RMC, and may display less FRU information. For additional details, such as network card addresses, run `ipmitool` on the RMC.

The following commands list FRUs for a specific chassis BMC.

```
remotehost% ssh administrator@flex-rmc
password: #####
flex-rmc eRMC:r001u01c cli> bmc exec "ipmi fru list" r1u1b

==== r001u01b ====
FRU Device Description : Builtin FRU Device (ID 0)
 Board Mfg Date        : Mon Oct 14 08:53:00 2019
 Board Mfg             : HPE_PRMO
 Board Product         : CH_BASEIO
```

```
 Board Serial          : PR19412345
 Board Part Number     : P22654_001
 Board Revision        : _A03
 Encryption Key P      : 00001234
 Encryption Key G      : 00000001
 Encryption Key Y      : 00005678
 Board Spare Part Num  : 000000_000
 Board Auth Ser Num    : ABC123
 OEM (Hewlett Packard Enterprise) MAC Address Record
  Ethernet 1           : 94:40:C9:12:34:51
  Ethernet 2           : 94:40:C9:12:34:52
  Ethernet 3           : 94:40:C9:12:34:53
  Ethernet 4           : 94:40:C9:12:34:54

FRU Device Description : NODE_EEPROM (ID 1)
 Board Mfg Date        : Thu Oct 31 09:24:00 2019
 Board Mfg             : HPE_PRMO
 Board Product         : CH_MLB
 Board Serial          : PR19498765
 Board Part Number     : P22643_001
 Board Revision        : _A03
 Encryption Key P      : 00004321
 Encryption Key G      : 00000001
 Encryption Key Y      : 00008765
 Board Spare Part Num  : 000000_000
 Board Auth Ser Num    : CBA321

FRU Device Description : PWR_EEPROM (ID 2)
.
.
.
```

Listing the local area network (LAN) configuration

The `lan print 1` command lists the LAN configuration.

Example: The following command lists the LAN configuration for the BMC.

```
remotehost% ipmitool -I lanplus -H flex-rmc -U ADMIN -P password lan print 1
Set in Progress         : Set Complete
Auth Type Support       :
Auth Type Enable        : Callback : MD5
                        : User     : MD5
                        : Operator : MD5
                        : Admin    : MD5
                        : OEM      : MD5
IP Address Source       : DHCP Address
IP Address              : 192.168.1.22
Subnet Mask             : 255.255.255.0
MAC Address             : 94:40:c9:12:34:51
SNMP Community String   : hpe
IP Header               : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
BMC ARP Control         : ARP Responses Enabled, Gratuitous ARP Disabled
Gratituous ARP Intrvl   : 0.0 seconds
```

Listing environmental sensors and values

The `sdr list` command retrieves a list of the system's environmental sensors and shows their values.

The following commands target a specific BMC:

```
remotehost% ssh administrator@flex-rmc
password: #####
RMC cli> bmc exec "ipmi sdr list" r1u1b
BMC_DIE_TEMP      | 47 degrees C      | ok
BIO_BMC_INLET     | 26 degrees C      | ok
BIO_BMC_OUTLET    | 25 degrees C      | ok
NODE_INLET        | 24 degrees C      | ok
NODE_OUTLET       | 28 degrees C      | ok
NODE_TEMP_3       | 27 degrees C      | ok
NODE_TEMP_4       | 26 degrees C      | ok
P0_THROT_OFFSET   | -60 degrees C     | ok
P1_THROT_OFFSET   | -68 degrees C     | ok
P2_THROT_OFFSET   | -63 degrees C     | ok
P3_THROT_OFFSET   | -65 degrees C     | ok
P0-DIMMA0         | 30 degrees C      | ok
P0-DIMMA1         | no reading        | ns
P0-DIMMB0         | 29 degrees C      | ok
P0-DIMMB1         | no reading        | ns
P0-DIMMC0         | 28 degrees C      | ok
P0-DIMMC1         | no reading        | ns
P0-DIMMD0         | 30 degrees C      | ok
P0-DIMMD1         | no reading        | ns
P0-DIMME0         | 29 degrees C      | ok
P0-DIMME1         | no reading        | ns
.
.
.
```

Retrieving the system event log (SEL)

The `sel list` command retrieves the system event log (SEL).

Example 1: The following command targets the RMC:

```
remotehost% ipmitool -I lanplus -H flex-rmc -U administrator -P password sel list
   1 | 07/10/2021 | 12:11:20 | Temperature #0x01 | Upper Non-critical going low  | Asserted
   2 | 07/10/2021 | 12:11:20 | Temperature #0x01 | Upper Critical going low  | Asserted
   3 | 07/10/2021 | 12:11:20 | Temperature #0x01 | Upper Non-recoverable going low  | Asserted
   4 | 07/10/2021 | 12:11:20 | Temperature #0x02 | Upper Non-critical going low  | Asserted
   5 | 07/10/2021 | 12:11:20 | Temperature #0x02 | Upper Critical going low  | Asserted
   6 | 07/10/2021 | 12:11:20 | Temperature #0x02 | Upper Non-recoverable going low  | Asserted
   7 | 07/10/2021 | 12:16:53 | Voltage #0x0a | Upper Non-critical going high | Asserted
   8 | 07/10/2021 | 12:16:53 | Voltage #0x0a | Upper Critical going high | Asserted
   9 | 07/10/2021 | 12:16:53 | Voltage #0x0a | Upper Non-recoverable going high | Asserted
   a | 07/10/2021 | 12:16:56 | Voltage #0x0a | Upper Non-critical going high | Deasserted
   b | 07/10/2021 | 12:16:56 | Voltage #0x0a | Upper Critical going high | Deasserted
   c | 07/10/2021 | 12:16:56 | Voltage #0x0a | Upper Non-recoverable going high | Deasserted
   d | 07/10/2021 | 12:23:50 | Voltage #0x0a | Lower Non-critical going low  | Asserted
   e | 07/10/2021 | 12:23:50 | Voltage #0x0a | Lower Critical going low  | Asserted
   f | 07/10/2021 | 12:23:50 | Voltage #0x0a | Lower Non-recoverable going low  | Asserted
  10 | 07/10/2021 | 12:23:53 | Voltage #0x0a | Lower Non-critical going low  | Deasserted
  11 | 07/10/2021 | 12:23:53 | Voltage #0x0a | Lower Critical going low  | Deasserted
  12 | 07/10/2021 | 12:23:53 | Voltage #0x0a | Lower Non-recoverable going low  | Deasserted
  13 | 07/10/2021 | 12:34:50 | Voltage #0x0a | Upper Non-critical going high | Asserted
...
```

Example 2: The following commands target a specific chassis BMC:

```
remotehost% ssh administrator@flex-rmc
password: #####
RMC cli> bmc exec "ipmi sel list" r1u1b
SEL has no entries
```

Opening a serial console

The `sol activate` command opens a serial console to the server. You might want to issue this command, for example, if you want to observe system messages during a boot.

```
remotehost% ipmitool -I lanplus -H flex-rmc -U ADMIN -P password \
sol activate
```

Restricting the `ipmi` commands

You can disable the `ipmi` interface used by the OS to communicate with the BMC. You can choose to allow only the allowlist set of `ipmi` commands or allow all the commands. The solution supports extensibility by providing a means to add to the allowlist without the need for a new firmware version. The default settings allow the same usage that exists in the released versions of CH firmware.

NOTE: Changing `ipmi` to enable or disable the BT interface should not be made while the OS is booted. Gracefully shut down the OS before changing the `ipmi` BT to enable or disable state.

Blocking all `ipmi` commands

About this task

You can block all the `ipmi` commands from the nPartition operating system. Blocking `ipmi` commands blocks all the `ipmi` commands over the BT interface.

NOTE: Blocking or disabling the `ipmi` commands over the BT interface is not recommended. When in-band BT IPMI interface is disabled, the Data Collection Deamon (DCD) will not operate. HPE support depends on DCD operation. Various OS level events are communicated through the inband `ipmi` and these events will be blocked.

Procedure

Enter the following command:

```
RMC cli> disable ipmi bt
```

Enabling all the `ipmi` commands

Procedure

Enter the following command:

```
RMC cli> enable ipmi bt
```

disabling the Linux `ipmi_si` driver

About this task

Procedure

1. On RHEL, log into the OS console and complete the following steps.

a. `# echo "blacklist ipmi_si">>/etc/modprobe.d/blacklist.conf`

b. `# echo “install ipmi_si /bin/true”>> /etc/modprobe.d/blacklist.conf`

c. `# reboot`

2. On SLES, log into the OS console and complete the following steps.

a. `# echo "blacklist ipmi_si">>/etc/modprobe.d/50-blacklist.conf`

b. `# echo “install ipmi_si /bin/true”>>/ etc/modprobe.d/50-blacklist.conf`

c. `# mkinitrd && reboot`

Running restricted `ipmi` commands

About this task

You can create a restricted allowlist of `ipmi` commands. Running restricted `ipmi` commands allows only those `ipmi` commands added in the IPMI allowlist. A restricted list minimizes the risk of `ipmi` commands being exploited by external entities. You can run these restricted list of `ipmi` commands from the nPartition operating system, LAN interface, and from RMC CLI.

Procedure

Enter the following command:

```
RMC cli> set ipmi restricted on
```

Turning off restricted `ipmi` commands

About this task

You can turn off the restricted `ipmi` commands which you have enabled on your system.

Procedure

Enter the following command:

```
RMC cli> set ipmi restricted off
```

Adding an `ipmi` command to the restricted list

About this task

You can add `ipmi` commands to the restricted allowlist.

Procedure

Enter the following command:

```
RMC cli> add ipmi restricted fn=<FN> cc=<CC> desc=<DESCRIPTOIN>
```

Deleting an ipmi command from the restricted list

About this task

You can delete the ipmi commands that you added to the restricted allowlist.

Procedure

Enter the following command:

```
RMC cli> remove ipmi restricted fn=<FN> cc=<CC> desc=<DESCRIPTOIN>
```

Viewing ipmi configuration

Procedure

Enter the following command:

```
RMC cli> show ipmi config
```

Viewing ipmi restricted allowlist

Procedure

Enter the following command:

```
RMC cli> show ipmi restricted
```

Disaster recovery with HPE Serviceguard for Linux (SGLX)

HPE Serviceguard for Linux provides disaster recovery and failover options for HPE Superdome Flex 280 Server.

HPE Serviceguard for Linux user guides and manuals can be found at **http://www.hpe.com/info/Linux-serviceguard-docs**.

HPE Persistent Memory on HPE Superdome Flex 280 Server

Hewlett Packard Enterprise supports HPE Persistent Memory on HPE Superdome Flex 280 Server.

For details on supported PMM configurations and related administration and maintenance tasks, see **HPE Persistent Memory Guide for HPE Superdome Flex 280 Server**.

Websites

HPE Superdome Flex 280 Server websites

- Product page

  www.hpe.com/support/superdomeflex280-product
- Customer documentation

  www.hpe.com/support/superdomeflex280-docs
- Software

  www.hpe.com/support/superdomeflex280-software
- HPE Foundation Software

  https://downloads.linux.hpe.com/SDR/project/hpe-foundation/
- Hewlett Packard Enterprise server operating systems and virtualization software

  www.hpe.com/us/en/servers/server-operating-systems.html
- HPE Superdome Flex 280 Server QuickSpecs

  www.hpe.com/support/superdomeflex280-quickspecs
- HPE Foundation Software (HFS) and Linux version support matrix

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

  www.hpe.com/support/superdomeflex280-customer-advisories
- Spare parts list

  www.hpe.com/support/superdomeflex280-spareparts
- Release sets (support matrix)

  www.hpe.com/support/superdomeflex280-release-sets
- Safety and regulatory information

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

  www.hpe.com/recycle
- Visio templates

  www.visiocafe.com/hpe.htm

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

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

HPE Superdome Flex 280 Server support documentation

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

Support and other resources

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/completecare

Customer self repair

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

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.