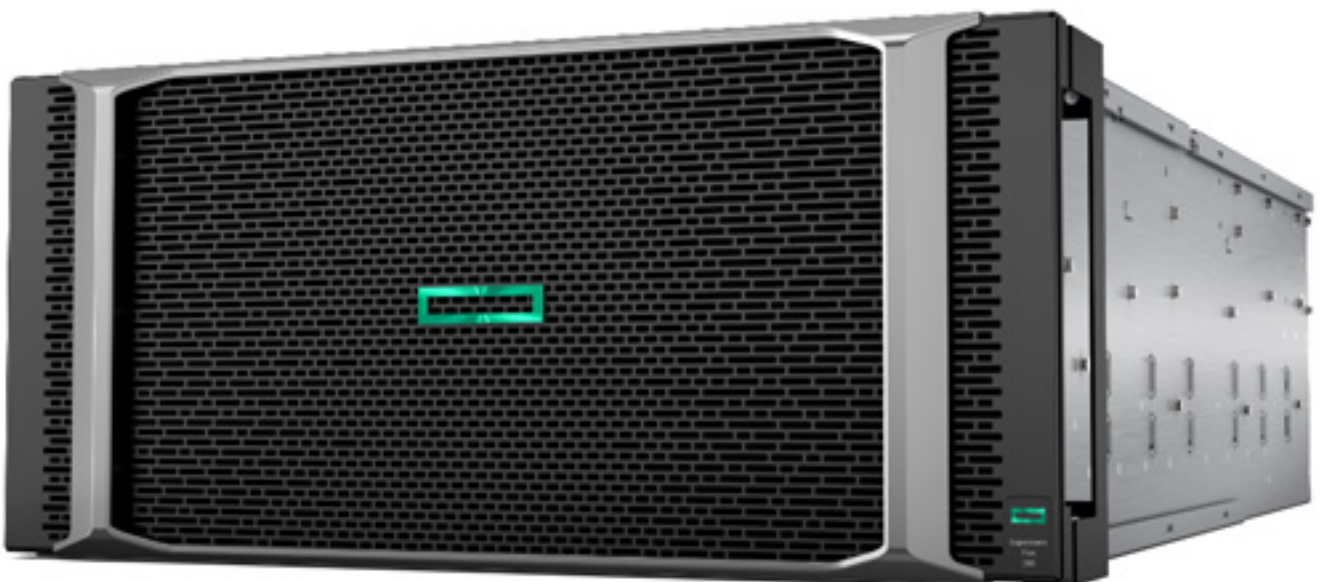




HPE SUPERDOME FLEX 280 SERVER MANAGEABILITY

Performance, reliability, and security for the most demanding workloads



CONTENTS

Introduction.....	3
Management components and tools.....	3
HPE Superdome Flex 280 embedded management	4
Foundation software.....	10
HPE OneView	13
HPE Remote Support	17
OpenStack for resource provisioning and management.....	17
OpenStack Ironic enablement for HPE Superdome Flex 280 systems	18
Managing an HPE Superdome Flex 280 Server	19
Monitoring.....	19
Firmware update	21
Security	21
Conclusion.....	23
Appendix 1: Redfish examples	24
Simple examples using Linux curl.....	24
Postman	25
Redfishtool.....	25
Python	25
Appendix 2: OpenStack Bare Metal Certification Matrix.....	26



INTRODUCTION

HPE Superdome Flex 280 is a highly reliable server that starts at two and scales up to eight 3rd generation Intel® Xeon® Scalable processors. Its modular architecture scales cost-efficiently to meet future growth. Six UPI links per processor result in higher bandwidth and faster data rates than prior generations. It is designed to provide 64 GB to 24 TB of shared memory using DRAM or in combination with persistent memory, it is an ideal choice for real-time analytics. Extreme HPE Superdome RAS features such as advanced memory resiliency, firmware-first approach, Analysis Engine, and self-healing provide increased system uptime. It also comes with superior security with Silicon Root of Trust from HPE, which protects your critical workloads, along with as-a-service consumption with HPE GreenLake, which provides flexibility while maintaining on-premises control.

HPE Superdome Flex 280 provides numerous management tools that work in concert to configure resources, monitor the system, and send alerts. These tools help identify issues and resolve problems through many interfaces—from intuitive and interactive GUIs to comprehensive CLIs that can be automated using a wide range of scripting languages.

HPE Superdome Flex 280 communicates management actions through industry-standard Redfish APIs, enabling many tools to operate, including industry-standard OpenStack cluster management. These APIs also enhance the built-in, mission-critical functionality of the HPE Superdome Flex 280 server, along with the standard environments using HPE OneView and HPE Insight Remote Support.

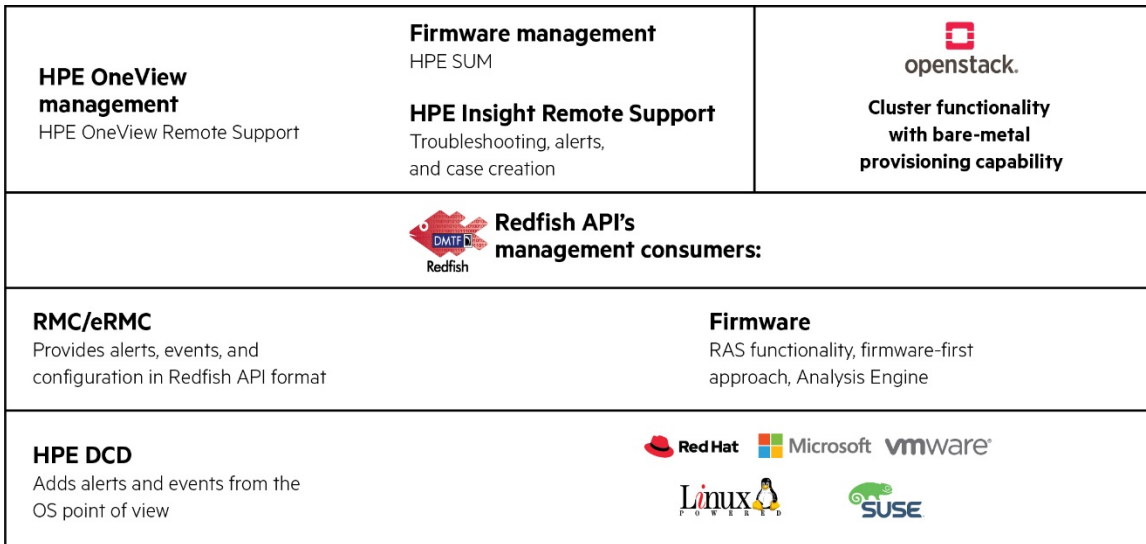


FIGURE 1. Simplified management experience on HPE Superdome Flex 280

This technical white paper describes the rich management ecosystem of the HPE Superdome Flex 280 servers and how to set up the right combination of tools for your unique IT environment.

MANAGEMENT COMPONENTS AND TOOLS

Extensive management and RAS capabilities built into HPE Superdome Flex 280 hardware and firmware architecture ensure the platform has a minimum level of always-on functionality before installing additional manageability tools to the platform. The primary component of the management system is the rack management controller (RMC). This management interface controls configuration, monitoring, and alerting of the HPE Superdome Flex 280, regardless of the number of chassis in a system. Each chassis has its own built-in baseboard management controller (BMC), which communicates the current status and alerts to the RMC.



HPE Superdome Flex 280 embedded management

Rack management controller

HPE Superdome Flex 280 uses the embedded rack management controller (RMC) management configuration where RMC functionality runs within the base chassis BMC. For a two-chassis HPE Superdome Flex 280, connect the peer network cables between the base chassis and expansion chassis to connect the two BMCs. The base chassis provides the RMC LAN connection to your data center's management network.

Below is a block diagram of a two-chassis HPE Superdome Flex 280 system with embedded RMC showing the LAN connections required.

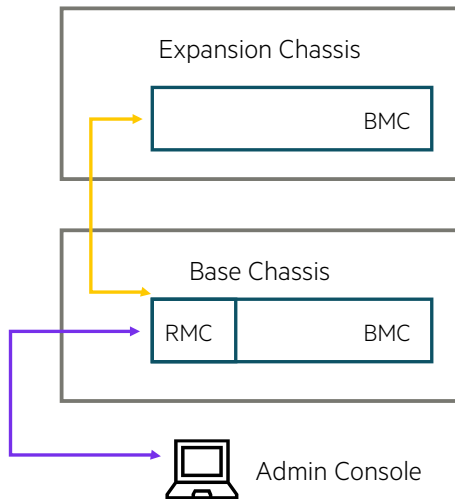


FIGURE 2. Embedded RMC managing a 2-chassis HPE Superdome Flex 280 system

Within the HPE Superdome Flex 280, the RMC provides:

- Analysis Engine
- Firmware manager
- Secure shell (SSH)-based CLI
- SSL-based web GUI
- System power, boot sequencing, and control
- Environmental control and monitoring
- Fault and error message information
- Alerting capability using Redfish events and alerts, Remote Support, or simple network management protocol (SNMP)
- Remote access to the UEFI and host serial console (available via SSH)
- Virtual media and web console for the host system
- Industry-standard Redfish interface for scripting access and tool support



Chassis types

HPE Superdome Flex 280 has two chassis types:

- Base chassis—the first chassis purchased in a system, containing the system information for warranty tracking; the base chassis is installed below the expansion chassis if it is a two-chassis system.
- Expansion chassis—the second chassis for the HPE Superdome Flex 280 systems larger than 4 sockets.

RMC web GUI

The HPE Superdome Flex Server 280 RMC has a web GUI interface providing most frequently used features, as well as providing help and additional information on related expert-level functionality that may only be in the RMC CLI. The web GUI shows system inventory, health, and detailed information about all components in the system. Remote power control, virtual media, and a remote view of the graphical console for the host system are also available. Refer to the [HPE Superdome Flex 280 QuickSpecs](#), which details browser compatibility.

This web console provides an HTML5 browser view of the system output sent to the embedded graphics on the base I/O of the base chassis. Virtual media on this interface provides one connection at a time. For two simultaneous virtual media connections, an embedded Java application can be launched from the browser.

Also, note that the RMC web GUI runs entirely off the Redfish API. So, if you see a feature in the RMC web GUI, you know it is obtainable and controllable by tools and scripts that use Redfish.

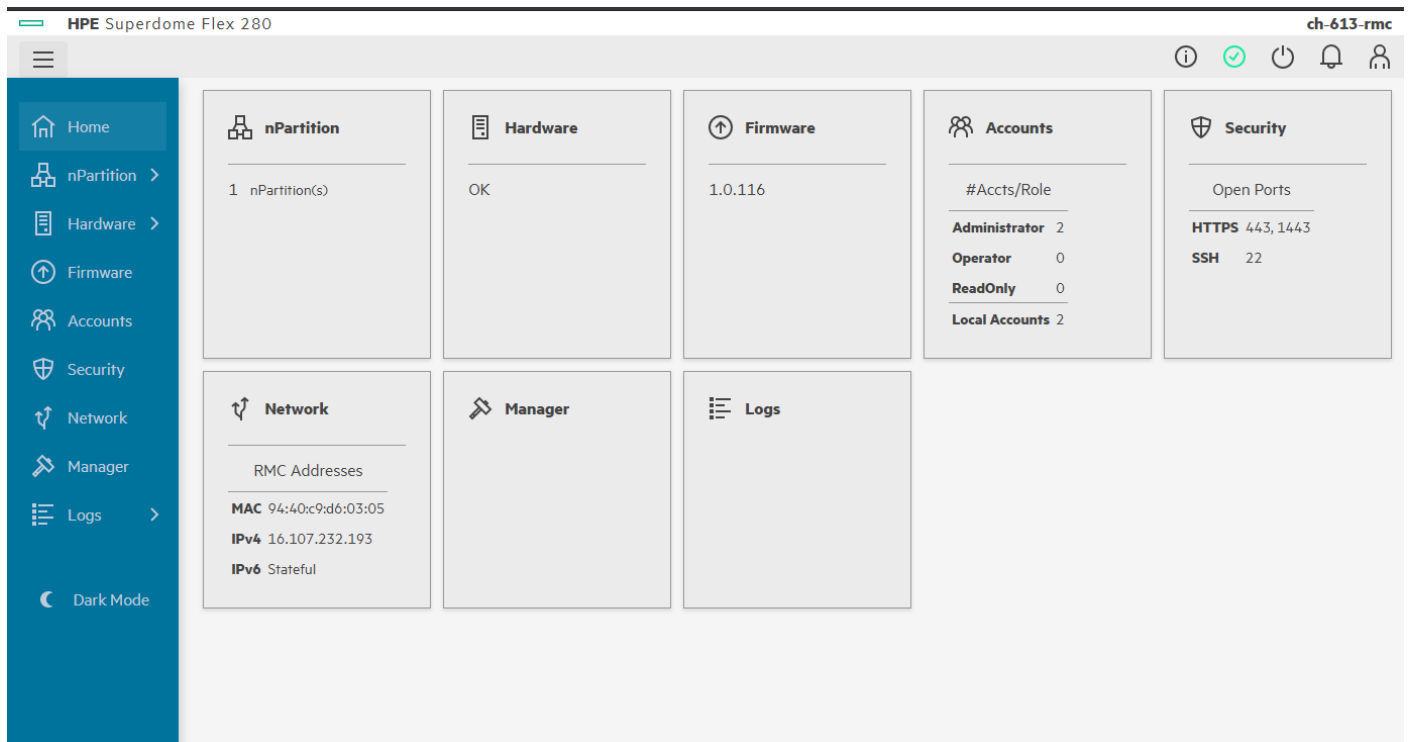


FIGURE 3. HPE Superdome Flex 280 GUI



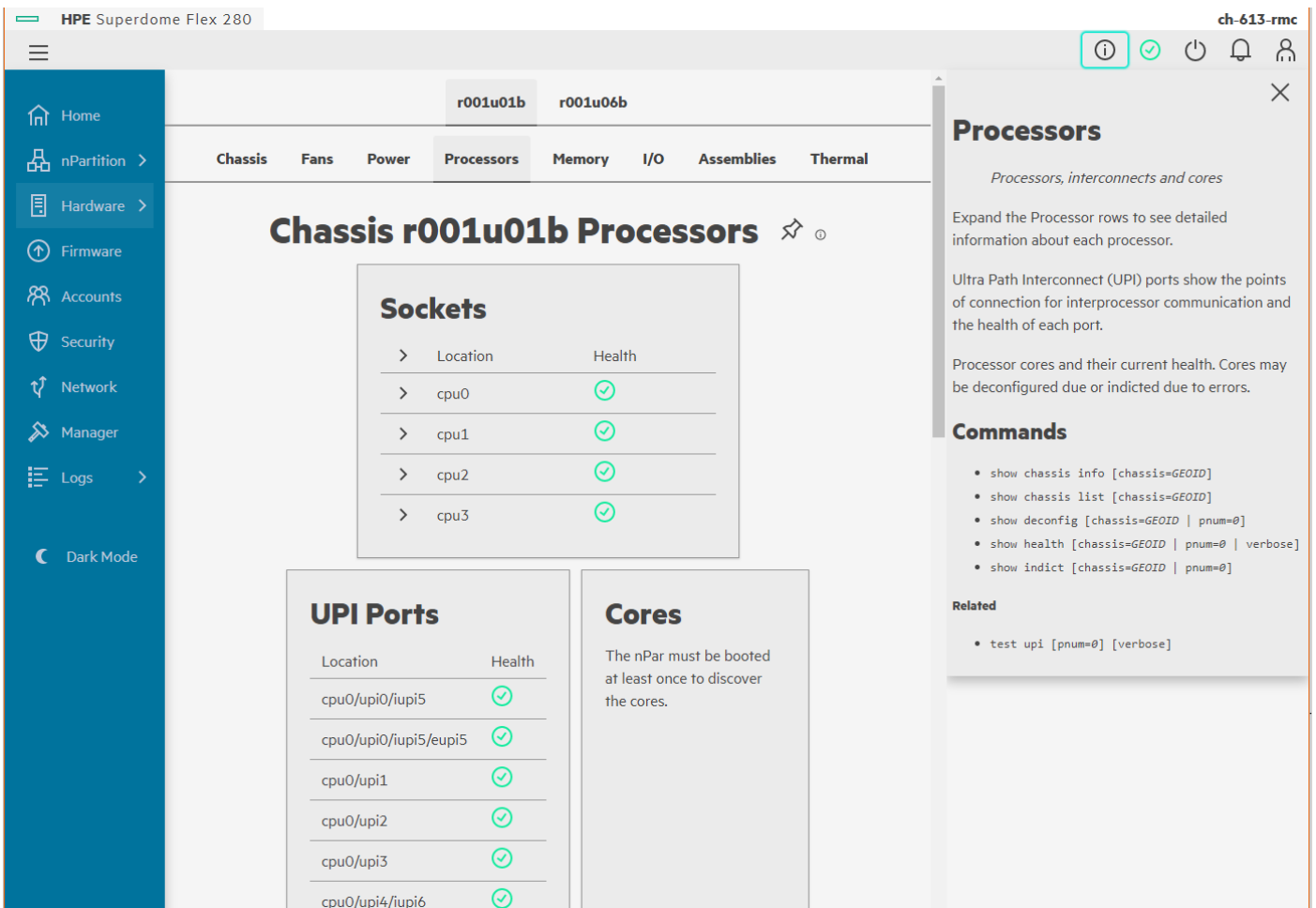


FIGURE 4. HPE Superdome Flex 280 GUI

RMC CLI

HPE Superdome Flex 280 has an extremely powerful CLI, available over SSH to the RMC management LAN. Administrators will find the HPE Superdome Flex 280 CLI is similar to the Linux® CLI—supporting command history and in-line editing. Because the RMC is a secure appliance, HPE Superdome Flex 280 does not expose a full shell (such as bash) to the user, which would open the door to installing the software that could compromise the system. Instead, all RMC capabilities are exposed via the RMC CLI.

An HPE Superdome Flex 280 beginner’s most useful commands are:

- **“help”**
 - Without arguments, this command will display CLI command keywords.
 - Type **“help <command>”** for more information on a specific command.
- **“apropos”**
 - This command searches all the “help” page files for a specified <string>; it displays the commands where that <string> appears.



```

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          2/2    8/8    0/0    48/48    6143/0    1/1

* OK/In = OK/Installed

ch-613-rmc eRMC:r001u01c cli> help

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

ch-613-rmc eRMC:r001u01c cli> apropos reset

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

ch-613-rmc eRMC:r001u01c cli>

ch-613-rmc eRMC:r001u01c cli>

```

FIGURE 5. HPE Superdome Flex 280 CLI

In HPE Superdome Flex and HPE Superdome Flex 280, the term **nPar** is synonymous with **server**. Even though HPE Superdome Flex 280 doesn't support multiple nPartitions (nPars), the term is still used throughout the CLI because the management subsystem builds one nPar from all resources (one or both chassis).

A few key commands to remember:

- `show npar`
 - Shows a high-level overview of the system
- `power on npar`
 - To power up the system; many other options to this command are available
- `show chassis`
 - Shows more detailed health status for each chassis
- `show firmware [verbose]`
 - To request the firmware manager run a consistency check and output the current firmware running on the system
- `show logs`
 - To browse various logs collected on the system for troubleshooting; the `live` option lets a session show logs as they occur on the system while the session runs

An extremely rich set of capabilities is included in the HPE Superdome Flex 280 CLI. Rather than remembering complicated commands, you can use `apropos` and `help` to find what you need. Finally, a CLI is entirely repeatable; once you determine the steps to take to complete a task, you can repeat the steps in the same way later. You can even write scripts that use SSH `exec` to run CLI commands. For an even better scripting experience, Hewlett Packard Enterprise recommends using the Redfish API because the JSON output is easier to parse.

For more information, refer to the following section on the Redfish API.

Redfish

Redfish is a simple human-readable API that enables easy script writing and automation. The Redfish interface is used by all the tools and management software that work with HPE Superdome Flex 280, including (but not limited to):

- HPE OneView
- HPE Smart Update Manager (SUM)
- OpenStack, especially the Ironic bare-metal provisioning service



Redfish is an industry-standard RESTful API for IT infrastructure. Redfish uses the https interface on the RMC and delivers JSON-formatted input and output. The information is organized around a standard information model that organizes all the physical and logical elements of the HPE Superdome Flex 280 system. The interface can be used entirely by software as an API to the system, but the input and output are quite human-readable, so administrators can also write simple scripts to get information or manage the system. All major system vendors have adopted Redfish and it ships in most server products. For more information, go to redfish.dmtf.org/, where you will find documents such as redfish.dmtf.org/education/presentations for education on the standard.

HPE Superdome Flex 280 web GUI is driven entirely from the Redfish API, so anything seen in the web GUI can be done with a Redfish script. Redfish shows the system inventory, the health state of all the components monitored by the RMC and all commonly used system management actions. The HealthRollup property is also supported, so a quick GET of the top branch of any part of the Redfish model will immediately show the health status of any module deeper in the model. Redfish also supports a simple https eventing and alerting mechanism, making it unnecessary to poll the system for status.

A GET of `https://<myRMC-IP>/redfish/v1/` will show the top level of the model. For this command, use a browser with support for JSON or a plug-in that supports JSON; you can also use Linux curl or a developer tool such as Postman (getpostman.com). Going any deeper than the top level requires authentication. Redfish, the web GUI, and the SSH CLI all employ the same user authentication credentials, which can be configured with local users and/or using the directory services integration support.

If you want a command-line tool to issue commands directly, several are available from dmtof.org/, including Redfishtool, which runs on Python 3.

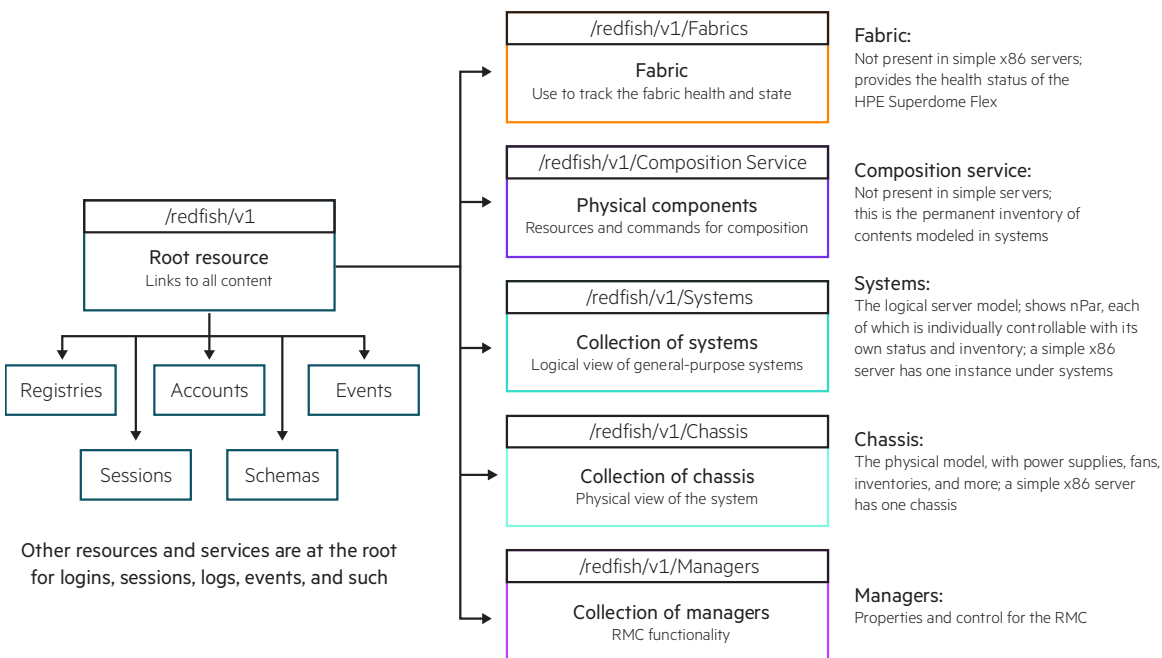


FIGURE 6. Redfish resource map for HPE Superdome Flex and HPE Superdome Flex 280

Various resources (such as schemas, accounts, and more) extend off the root resource (/redfish/v1), but the main parts that model the server are the ones shown earlier. For instance:

- /redfish/v1/Chassis, has the physical components modeled and /redfish/v1/Systems has the logical server model.
- The server information is under /redfish/v1/Systems and each chassis is found under /redfish/v1/Chassis
- The Composition service has ResourceBlocks that give the permanent inventory of objects instantiated in Systems as nPar. Because HPE Superdome Flex 280 nPar cannot be changed, this service will show a state of State: UnavailableOffline. Even though the service cannot be used to change the nPar of the system, the information in that part of the model is still correct and always kept up to date by the RMC.
- The HPE Superdome Flex grid fabric is modeled under Fabric. This is not present on HPE Superdome Flex 280 because it is a directly connected 2–8 socket system, without the HPE Superdome Flex grid chipset and interconnect.
- The RMC settings are modeled under Managers.
- To control the server, see the Actions contained in the /redfish/v1/Systems instance, such as reset actions, BIOS settings, and such.

For more information and examples of how to use Redfish, refer to [Appendix 1](#) at the end of this white paper.



HPE Superdome Flex 280 and HPE ProLiant management

Table 1 shows a summary of major features available in HPE Superdome Flex 280 and HPE ProLiant Gen10 with HPE iLO 5. The vast majority of the most commonly used features are available in both the HPE Superdome Flex 280 with RMC and the HPE ProLiant Gen10 with HPE iLO 5, with a few differences. For instance, legacy HPE ProLiant features, such as RIBCL scripting are not supported in RMC. Instead, for HPE Superdome Flex 280 environments you can use the Redfish API for scripting where interoperability can be achieved not just between HPE products but also between HPE products and other vendors systems that also support Redfish.

HPE Superdome Flex 280 with RMC delivers mission-critical features such as enhanced error coverage and fault-resilient boot, as well as a very comprehensive CLI in the RMC for Linux admins that prefer it. HPE ProLiant with HPE iLO also has similar features and tends to have better feature coverage in areas such as automation and scale-out.

New features in HPE Superdome Flex 280 help make the management experience more similar to HPE ProLiant management, such as workload matching profiles in Redfish. These are similar to HPE ProLiant, allowing one setting in the RMC web GUI, Redfish, or HPE OneView to put many UEFI variables into the right state for particular workloads. HPE Superdome Flex 280 supports high-end, large memory workload profiles tailored toward the areas where this server model is most used.

TABLE 1. HPE Superdome Flex 280 and HPE ProLiant system manageability features

Platform	HPE Superdome Flex 280		HPE ProLiant Gen10 with HPE iLO 5	
	RMC	Standard	Advanced	
Feature				
Virtual power buttons	Y	Y	Y	
Web-based GUI	Y	Y	Y	
Virtual graphics console	Y—HTML5	Pre-OS only—with IRC/HTML5	Y—IRC/HTML5	
SSH CLI	Y—more user friendly	Y	Y	
Workload matching profiles	Y	Y	Y	
Virtual media	Y—via web GUI	Y—via web GUI	Y—via web GUI and IRC	
Scripted virtual media	Y	N	Y	
Redfish API	Y	Y	Y	
IPv6	Y	Y	Y	
RIBCL	N	Y	Y	
Embedded Remote Support	Y—greater error coverage	Y	Y	
Fault-resilient boot and RAS features under it	Y—superior	Y—partial	Y—partial	
Embedded health system	Y—superior embedded Analysis Engine	Y	Y	
Recorded health logging	Y—with lighthouse logs		Y—with AHS	
Server system restore	N	N	Y	
Agentless management	Y	Y	Y	
Silicon root of trust from HPE	Y	Y	Y	
Cyber catalyst designation	In progress	N	Y	
Directory service authentication	Y	N	Y	
2-factor authentication	Planned	N	Y	
Remote syslog	Y	N	Y	
Multiple system management	Y—use HPE OneView	Y—use HPE iLO Federation or HPE OneView		
Licenses required	N	N	Y	

As a high-end product, HPE Superdome Flex 280 enables all advanced features and compares best to HPE iLO Advanced, which can be enabled on HPE ProLiant with an extra license. Some features not yet available on HPE Superdome Flex 280, such as server system restore and 2-factor authentication, are in the road map and planned to be supported with the HPE Superdome Flex product line.



HPE Superdome Flex and HPE Superdome Flex 280 management

HPE Superdome Flex 280 is a new addition to the HPE Superdome Flex product line. It is a glueless 2–8 socket system, where all the CPU sockets are directly connected to each other via Intel® Ultra Path Interconnect (UPI). HPE Superdome Flex 280 shares much of the architecture and capabilities of the HPE Superdome Flex system, except for those that rely on the HPE Superdome Flex Grid, used in HPE Superdome Flex to scale from 4–32 sockets. HPE Superdome Flex Grid enables multiple, electrically isolated hard partitions, or nPars, each running separate bare-metal OS instances in HPE Superdome Flex. In contrast, HPE Superdome Flex 280 supports only **one OS instance**, in the same way HPE ProLiant servers do. Because HPE Superdome Flex 280 is based on the HPE Superdome Flex architecture, the term nPartition is utilized in user interfaces, firmware, and Redfish to indicate a single HPE Superdome Flex 280 system, or a single nPar, which cannot be modified.

The management subsystem of HPE Superdome Flex 280 shares the same architecture and design as HPE Superdome Flex, allowing it to leverage capabilities such as the ability to manage a multi-chassis server as a single system and delivering all the mission-critical RAS functionality, including the built-in Analysis Engine, via the embedded Rack Management Controller.

In addition, HPE Superdome Flex 280 delivers many new features enabled in hardware such as TPM 2.0, silicon root of trust from HPE, and optional intrusion detection.

There are also many new features in the firmware that are primarily focused on increasing ease-of-use and enhancing security. A new web GUI for the RMC is provided and many enhancements have been made to the firmware feature set for Redfish, such as Scriptable vMedia support. The UEFI workload profiles and BIOS attribute configuration via Redfish have been added, so the system can be configured prior to startup in the same manner as the HPE ProLiant, through Redfish, the web GUI, and via HPE OneView profiles. Improvements to on-site setup have been made, bringing the setup more in-line with the HPE ProLiant user experience. For instance, auto-config of local LAN to a laptop so that can be used instead of the micro-serial USB port (which is still there). Support for automatic setting of the RMC hostname into DNS similar to HPE iLO has been added as well.

Foundation software

HPE Foundation Software (HFS) provides a set of commands and scripts to configure, monitor, and tune Linux on HPE Superdome Flex 280 to improve overall system performance.

The [Installing Operating Systems on HPE Superdome Flex 280 Server guide](#) explains how to install the Foundation Software and the [Configuring and Operating HPE Superdome Flex 280 Server guide](#) explains the functionalities and commands.

HPE Data Collection Daemon

HPE Superdome Flex 280 is a fully Redfish-compliant mission-critical platform, where the RMC exposes Redfish APIs for client applications such as HPE Insight Remote Support and HPE OneView.

The RMC, with the aid of the BMC in each chassis, gathers hardware inventory, monitors the hardware for events, and services management requests received through the management LAN port of HPE Superdome Flex 280. However, of all the required manageability data, only a part of it is directly available to the RMC/BMC. The remaining data—such as the information about physical drives attached to storage controllers, link-level events occurring on Fibre Channel adapters, and health of Ethernet adapters—is visible only to the OS running on the HPE Superdome Flex 280 server.

HPE Data Collection Daemon (DCD) is an OS-level service that bridges this gap. It gathers inventory of OS-visible hardware components, proactively monitors the health of those components, and reports this information to the RMC via the in-band IPMI system interface. Figure 7 shows an example of a two-chassis HPE Superdome Flex 280 running Linux with HPE DCD installed.



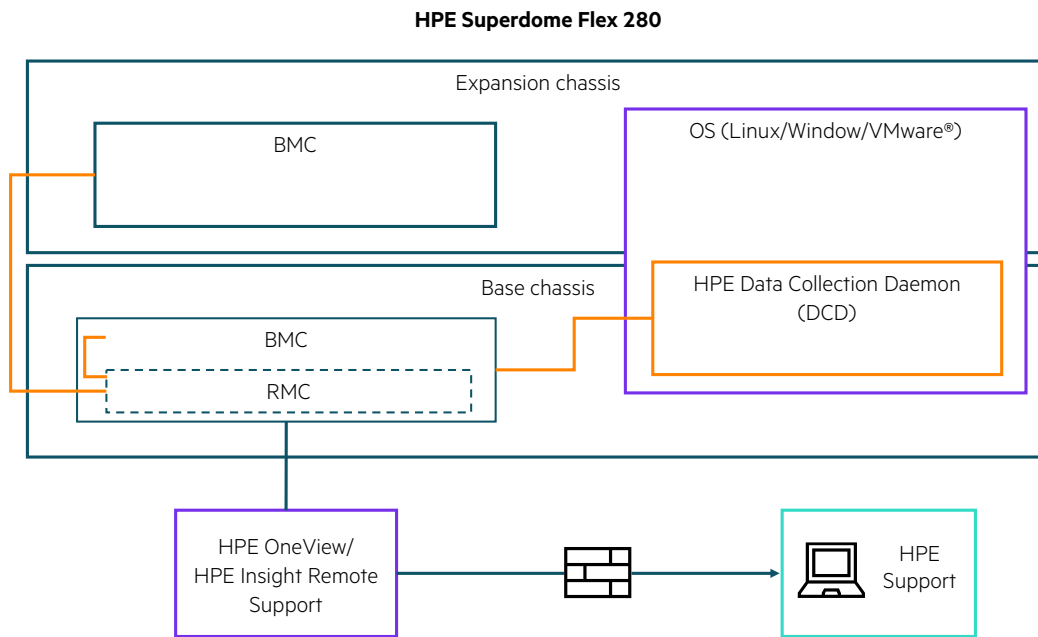


FIGURE 7. Two-chassis HPE Superdome Flex 280 showing HPE DCD

For example, HPE DCD monitors physical drives and volumes in the HPE Superdome Flex 280 internal drive cage by providing richer system information, which helps streamline troubleshooting for Remote Support.

- HPE DCD uses the storage management library APIs and OS interfaces to inventory SAS/SATA drives connected to the storage RAID controllers. Drive details such as model, capacity, media type, serial number, and bay number are also gathered.
- HPE DCD pushes this inventory information periodically to RMC, which is updated in the Redfish tree.
- To monitor drive health, HPE DCD registers with storage management library APIs to receive asynchronous event notifications. When a logical volume fails, HPE DCD is notified of this condition.
- HPE DCD then reports this condition to RMC by generating a `DCD_VOLUME_ERROR` event.
- In the RMC, the HPE Superdome Flex 280 Analysis Engine incorporates the HPE DCD information alongside all information gathered from UEFI, BMCs, and RMC to determine what is wrong and what actions to take.



- RMC informs Remote Support of this failure by generating a service event. The DCD_VOLUME_ERROR event can be seen in the RMC CLI, as shown in the following example.

```
[ATTN] [MFG] ch-114-rmc eRMC:r001u01c cli> show cae dump=8

Alert Number : 8

Event Identification :
  Event ID      : 682
  Provider Name : Hawks2Provider
  Event Time    : 2020-11-03 17:06:14Z (Tue Nov 3 17:06:14 2020)
Managed Entity :
  Name          : ch-114-rmc
  System Type   : 80
  Impacted Domain : Partition
  Partition ID  : 0

Summary :
  Logical volume status error

Full Description :
  A Logical volume has changed its state from OK to Critical due to some fatal error.

Probable Cause 1 :
  Logical volume status changed to Error

Recommended Action 1 :
  Check the Physical Drives which are part of this volume for any errors. Make sure RAID HBA is functioning.
  Check for any cables connecting the drives to HBA. View the Event Logs for any additional information.

Replaceable Unit(s) :
  Part Location      : Not Applicable
  Additional Info    : Not Applicable

Additional Data :
  Severity           : Major
  Alert Type         : Device Alert
```

FIGURE 8. DCD_VOLUME_ERROR event

The following table lists the system resources monitored by HPE DCD on each OS.

TABLE 2. System resources monitored by DCD on each OS

Hardware components monitored	Rack management controller	HPE DCD on Red Hat® Enterprise Linux (RHEL)/SUSE® Linux Enterprise Server (SLES)/Oracle® Linux	HPE DCD on Windows	HPE DCD on VMware ESXi™
Chassis power supply	✓			
Chassis thermal	✓			
DIMMs	✓			
CPUs	✓			
PCIe cards	✓			
Base I/O	✓			
SDF fabric	✓			
Fans	✓			
MCA, system crashes	✓			
OS-critical shutdown events		✓	✓	✓
Storage controllers/HBA		✓	✓	✓
Physical drives		✓	✓	✓
Logical volumes		✓	✓	✓
Ethernet cards		✓	✓	✓
Fibre Channel cards		✓		✓
NVMe cards		✓		
GPU cards		✓		



HPE DCD currently inventories GPU cards. Support for GPU card-related events will be added in a future release.

NOTE

For details on I/O card models supported by HPE DCD, refer to the [release notes of the respective OS](#).

HPE DCD can be downloaded as follows:

- **RHEL/SLES/Oracle Linux:** DCD is part of Foundation Software media. The latest Foundation Software media can be found at [HPE Support Center](#).
- **Windows:** DCD is part of the HPE Superdome Flex I/O Service Pack media, which can be downloaded from [HPE Support Center](#).
- **VMware ESXi:** DCD is published as a VMware ESXi offline bundle, which can be downloaded from [HPE vibsdepot](#).

HPE OneView

HPE OneView is a converged infrastructure management platform that provides a unified interface for the administration of systems in a data center. Through a single GUI—sometimes referred to as a single pane of glass—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 physical systems, storage arrays, and network connectivity.

HPE OneView can manage or monitor up to 80 HPE Superdome Flex 280 servers and HPE Superdome Flex systems. It is licensed to enable functionality in two modes:

HPE OneView Standard or Monitored mode is available at no additional cost. However, to get support, you need to purchase the SKU: R4P95AAE = HPE OV SD Flex 3yr 24x7 E-LTU. After purchasing this, you will receive an email notification from HPE to register in the HPE Support Center. The support contract is initiated only after successful registration in the HPE Support Center.

HPE OneView Standard or Monitored mode enables:

- Server discovery
- A detailed inventory of physical and logical resources
- Comprehensive health monitoring, activities/alerts, and reporting
- Changing the BIOS settings, defining a server profile for efficiently standing up, and deploying servers in the future

To use the advanced version of HPE OneView, you need to purchase the SKU: R4P95AAE = HPE OV SD Flex 3yr 24x7 E-LTU. After purchasing this SKU, you will receive an email notification from HPE to register in the HPE Support Center. Just like with standard mode, the support contract is initiated only after successful registration in the HPE Support Center.

NOTE

HPE OneView initially will run in monitored mode. To initiate HPE OneView Advanced, a profile needs to be configured for the HPE Superdome Flex 280 system.

The HPE OneView monitoring capabilities now include HPE OneView Remote Support (OVRs), featuring one-click activation, pre-failure alerts, and automated case creation. In HPE OneView, the HPE Superdome Flex 280 RMC is a rack manager component, which hosts one nPar. The HPE Superdome Flex nPar show up as servers in HPE OneView because they are independently bootable and manageable entities.



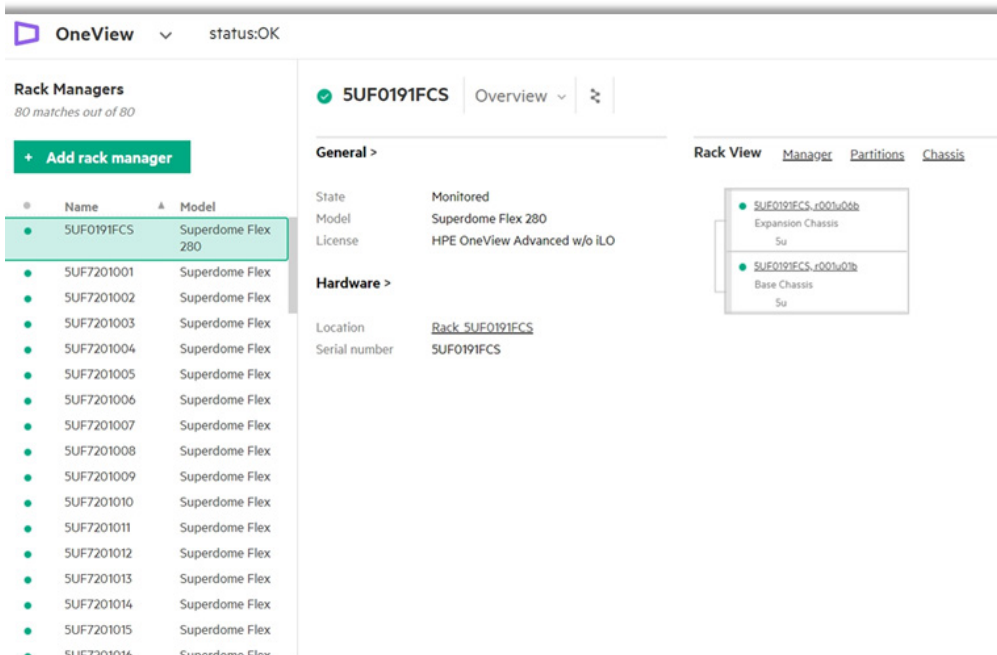


FIGURE 9. HPE OneView user interface

The user interface resembles the HPE OneView Advanced version. It aids in seamless interaction with HPE Superdome Flex 280 server. Some of the HPE OneView features include:

- Monitoring multiple HPE Superdome Flex 280 servers

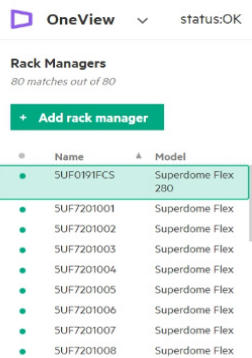


FIGURE 10. HPE OneView Rack Manager user interface



Multiple HPE Superdome Flex 280 servers conveniently stacked together in a single pane and provides a snapshot of the current state of the imported servers.

- HPE Superdome Flex 280 inventory discovery

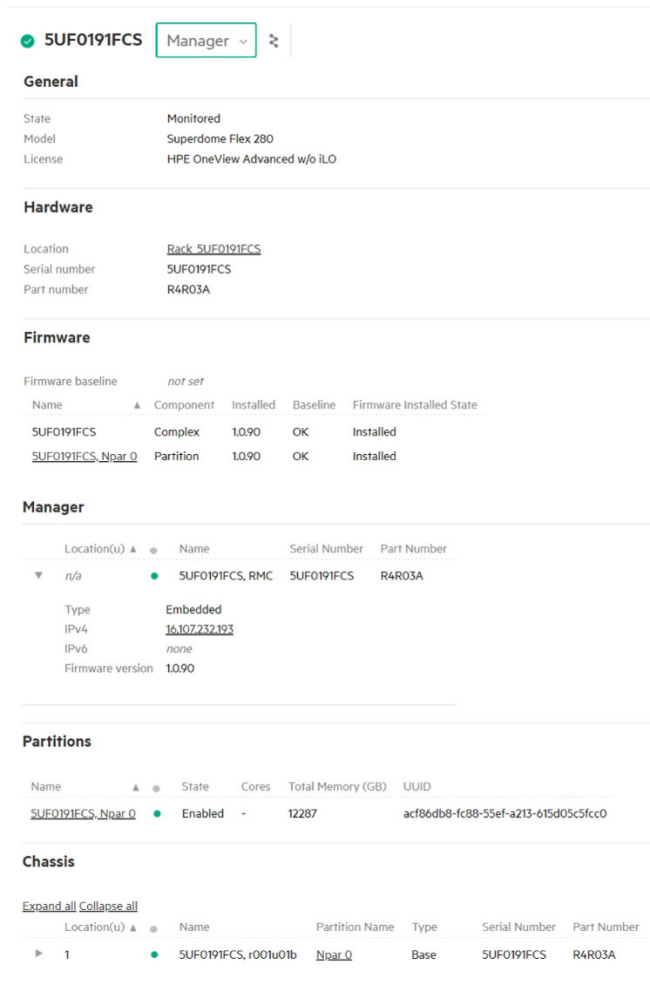


FIGURE 11. HPE OneView discovery capabilities

Comprehensive discovery of the HPE Superdome Flex 280 server, including (but not restricted to) manager, nPar (server) information, chassis, fans, power supplies, PCIe devices, and more.

- Comprehensive health monitoring and active alerting of HPE Superdome Flex 280 chassis and the sub-resources housed inside the chassis, namely fan and power supplies; HPE OneView also supports passive alerting (lifecycle events), which handles the configuration changes of the partitions and sub-resources
- Power on/off for HPE Superdome Flex 280 partitions
- Integration of HPE OneView REST APIs and the state change message bus (SCMB) to communicate between resource managers and foundation services
- Reports that provide details on resource inventory, configuration, and health status; pre-queried reports can be pulled through REST APIs
- Map view



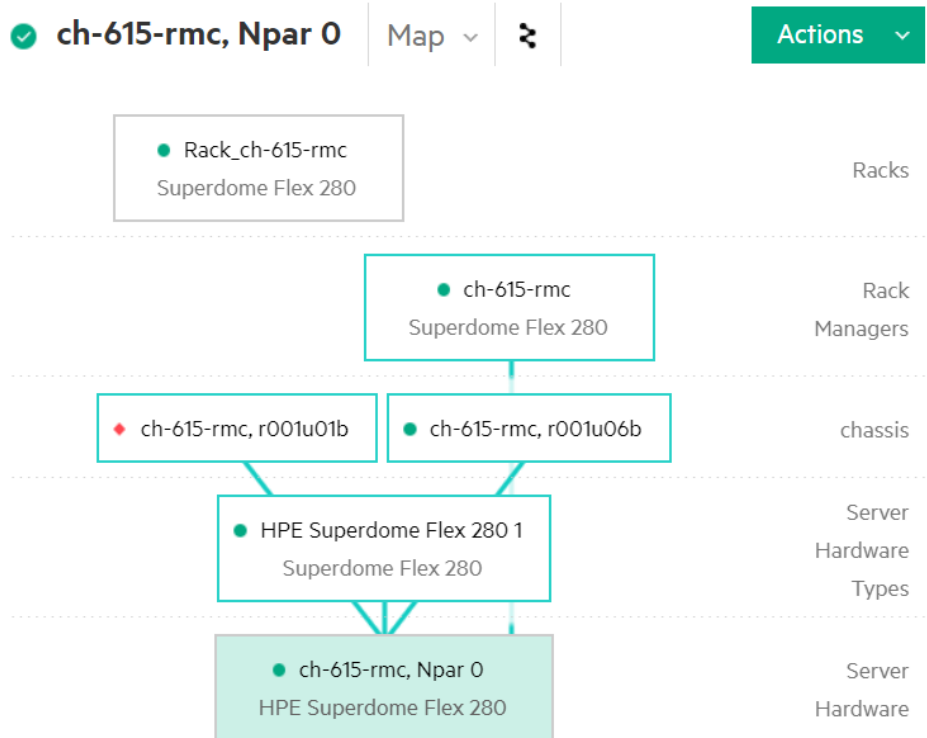


FIGURE 12. HPE OneView Map view

Map view for tracking the relationships between resources using dynamic interactive visualizations; allows users to understand the relationships between logical and physical resources.

- Activity page

The activity view shows a list of events for the resource '5UF0191CQM, Npar 0'. The interface includes a search bar with the resource name, an 'Activity' dropdown, a refresh icon, and an 'Actions' dropdown menu. A red banner at the top highlights a 'Remote Support Ticket: A system fan is not functioning properly (RSAL_1...)' with an 'Active' status and a timestamp of '9/24/20 12:47:58 pm'. Below the banner, there are filters for 'All', 'All types', 'All statuses', 'All states', 'All time', 'All owners', and 'All support states'. The main table lists activities with columns for Name, Date, State, and Owner.

Name	Date	State	Owner
Remote Support Ticket: A system fan is not functioning properly (RSAL_163X)	9/24/20 12:47:58 pm	Active	unassigned
Update sub-resource	9/24/20 12:43:07 pm	Completed	System
A resource's health rollup has changed to critical.	9/24/20 12:42:10 pm 12 minutes ago	Locked	unassigned
A resource's health rollup has changed to critical.	9/24/20 12:42:10 pm 12 minutes ago	Cleared	unassigned
rack1/chassis_u1/psu1 was indicted. The RMC has determined that this resource needs attention to return to normal operation. A service event has been generated.	9/24/20 12:42:10 pm	Locked	unassigned
A resource's health rollup has changed to critical.	9/24/20 12:42:10 pm	Locked	unassigned
A resource has changed status to critical.	9/24/20 12:42:10 pm	Locked	unassigned

FIGURE 13. HPE OneView Activity view



Activity page for listing alerts and other notifications occurring throughout the life of the imported server; the information can be refined using filter and sort options.

- HPE OneView Global Dashboard for providing a unified view of the basic inventory data; the dashboard can be used to define and personalize multiple views in a single pane; the dashboard also provides links to the monitored HPE Superdome Flex 280 servers.
- Remote Support functionality through HPE OneView, which assists in collecting hardware diagnostic and system configuration information that can be sent to HPE to troubleshoot and resolve system issues.

HPE OneView supports features such as managed mode for HPE Superdome Flex 280 Servers including:

- One-time boot settings for partitions
- Rack complex firmware update (all management processors)
- BIOS settings via server profile
- Secure boot via server profile

For the complete support matrix of HPE Superdome Flex 280 for HPE OneView features, refer to the [link](#).

HPE OneView integration with Microsoft System Center

HPE OneView integrates with Microsoft System Center Server to deliver powerful HPE hardware management capabilities directly from System Center consoles—including comprehensive system health and alerting, as well as driver and firmware updates.

For more information, refer to [HPE OneView for Microsoft System Center—Overview](#).

HPE Remote Support

Remote Support is provided as part of an HPE warranty or support contract, with the following benefits:

- Secure 24x7 monitoring of your HPE Superdome Flex 280 system
- Automatic support case trigger in the event of a hardware failure
- Enabling HPE Proactive Care reports with recommendations based on your configuration
- Contacting you to ship a replacement part or dispatch an engineer
- Optionally, integrating with HPE Insight Online to view your connected devices' health, contract and warranty status, and support cases

Remote Support uses highly secure technology. For complete details, read the [HPE Remote Support Security White Paper](#).

HPE Superdome Flex 280 offers two Remote Support options.

- HPE OneView Remote Support
 - Is enabled by checking enable remote support in the settings menu.
 - For more information, refer to the [Remote Support for HPE OneView Customer Presentation](#) and the [HPE Remote Support Enablement in HPE OneView FAQ](#).
- HPE Insight Remote Support
 - Installed as a separate software package on a virtual machine (VM) or Windows machine.
 - For information on installing and configuring your HPE Insight Remote Support hosting device, read the [HPE Insight Remote Support Installation and Configuration Guide](#). For information on configuration and discovery of devices to be monitored, read the [HPE Insight Remote Support Monitored Devices Configuration Guide](#).

OpenStack for resource provisioning and management

[OpenStack software](#) controls large pools of compute, storage, and networking resources located throughout a data center and manages those resources through a dashboard or via the OpenStack API. OpenStack works with popular enterprise and open source technologies, making it the ideal choice for heterogeneous infrastructure. The collection of OpenStack open source tools works together to provide a virtual cloud solution.

To ensure you can use this industry-standard management environment, HPE Superdome Flex and HPE Superdome Flex 280 are validated against the latest versions and updates of the OpenStack software. The HPE Mission Critical Cloud Reference Architecture includes a



multiple-chassis HPE Superdome Flex 280 solution operating in an enterprise-class cloud. This reference architecture validates the HPE Superdome Flex as a fully functioning OpenStack compute node and bare-metal node. Validated abilities of the solution include:

- Certified for Red Hat OpenStack Platform (RHOSP) releases
- Nova virtual machine deployment
- Cinder cloud storage operations
- Neutron software-defined network (SDN) operation
- Nova NUMA scheduling
- Pacemaker high-availability (HA) failover for virtual Instances
- Ironic bare-metal provisioning using Redfish for HPE Superdome Flex partitions

Further development of the OpenStack Ironic service validates the HPE Superdome Flex 280 Redfish functionality for standalone bare-metal deployment. Features beyond Nova use of Ironic include:

- Directed LAN boot
- UEFI HTTP boot
- BIOS/UEFI settings in Redfish
- Secure boot 2.0
- Firmware update
- RAID configuration
- Hardware disk erase
- Boot from Fibre Channel volume
- Virtual media based OS provisioning

OpenStack Ironic enablement for HPE Superdome Flex 280 systems

HPE Superdome Flex systems are supported and can be managed as bare-metal nodes by OpenStack with bare-metal service using Ironic hardware types “redfish” and “sdflex-redfish.” Each HPE Superdome Flex nPar can be enrolled as a separate bare-metal node and managed with the same OpenStack instance, along with any other hardware instances in the cloud. Ironic enables node configuration, management, and faster OS provisioning. Ironic with the new sdflex-redfish hardware type (driver) takes advantage of RMC management Redfish features and enables the Ironic for HPE Superdome Flex specific value-add features, in addition to the features of a standard Redfish driver.

HPE Superdome Flex 280 and HPE Superdome Flex nPar have been certified for the following OpenStack Ironic features with reference Redfish hardware type.

- Bare-metal node enroll/delete
- Power operations on/off/reset/Graceful Restart/Graceful Shutdown
- In-band hardware inspection for automatic hardware inventory collection
- Deploy (provision) OS using the cloud format (.qcow2) images
 - SLES12SPx
 - SLES15SPx
 - RHEL7.x
 - RHEL8.x
 - OL7.x
 - OL8.x
 - OVM
 - Windows Server 2016 (using wholedisk format image)
 - Windows Server 2019 (using wholedisk format image)



NOTE

HPE OneView initially will run in monitored mode. To initiate HPE OneView Advanced, a profile needs to be configured for the HPE Superdome Flex 280 system.

- Configdrive for performing post OS-install tasks
- Cinder volume attach for providing additional storage capacity
- Automated cleaning for cleaning disk metadata, shred based disk erase during node deploy and undeploy operations
- Deploy OS into FC volume and boot from it
- Node rescue operation can be used to boot nodes into a rescue ramdisk so that the rescue user can access the node in case access to OS is not possible
- Undeploy node for performing the cleaning activities
- RHOSP certification
- OpenStack Ironic value add features with sdflex-redfish hardware type (driver)
- Secure boot enables configuring “secureboot” on the node, OS provisioning, and boot OS in the Secure boot mode
- Directed LAN boot is an alternate to regular LAN boot and is more secure as it enables bare metal to connect and boot from only the specified TFTP URL boot file
- UEFI-HTTP boot is an alternate to regular LAN boot and is more secure as it is PXE-less and enables bare metal to connect and boot from only the specified HTTP URL boot file
- BIOS settings provides mechanism to set the specified values for the BIOS parameters
- Firmware update provides a utility to update the complex firmware and nPar (UEFI) firmware
- I/O firmware update using HPE SUM provides mechanism to update the firmware
- RAID configuration provides an in-band RAID configuration functionality for both create and delete logical volumes
- Hardware disk erase provides an in-band disk erase functionality with the specified pattern using the respective HPE Smart Array controller’s utility
- Virtual media-based OS provisioning is an alternate to regular LAN boot, it is a PXE-less OS provisioning
- Boot from Fibre Channel volume and support the following use cases
 - OS provisioning to empty Fibre Channel volume and boot from it
 - Boot from preprovisioned Fibre Channel volume

For more information on Ironic certification, features, and HPE Superdome Flex firmware versions, refer to the [Appendix 2: OpenStack Bare Metal Certification Matrix](#). Also, release notes and a general guide on how to install and an up-to-date certification matrix can be found here: github.com/HewlettPackard/sdflex-ironic-driver/wiki.

MANAGING AN HPE SUPERDOME FLEX 280 SERVER

The HPE Superdome Flex 280 management ecosystem includes a wide variety of both open source and HPE tools designed to monitor, manage, and secure each unique HPE Superdome Flex 280 environment.

Monitoring

Analysis Engine

A primary feature of HPE Superdome Flex 280 is the embedded Analysis Engine, which runs in the RMC. The Analysis Engine constantly monitors the system for issues and correlates the information to determine the root cause of any problems. Results of this constant analysis drive the system health status shown in the RMC and any problems detected or change to health status will cause the RMC to send certain Redfish, SNMP, and Service Events. Note that installing HPE DCD (see the [HPE Data Collection Daemon](#) section) will add useful additional troubleshooting coverage from the OS side, such as additional monitoring of I/O. All this information is aggregated in the RMC.

The Analysis Engine also performs indictments and de-configurations to take suspect or broken hardware offline, enabling the system to perform a resilient reboot and come back up without the suspect/broken hardware. This way the system can automatically go back into



service after a failure. The system can be fully repaired during the next planned downtime window, rather than being unable to run or running with faulty hardware that might cause another failure.

Redfish alerting

HPE OneView uses Redfish to monitor and manage HPE Superdome Flex 280. You can also set up your own Redfish event receiver to monitor the HPE Superdome Flex 280 system. You can use a web service on a monitoring system, management network, and simple Python or other script techniques to run the Redfish commands to set up the connection. Doing so sets up an ongoing receipt of events on the monitoring system into a log, similar to a syslog. Refer to redfish.dmtf.org/ for tutorials on how to set up an event receiver that can monitor all your systems that support Redfish.

SNMP traps

Redfish monitoring is recommended but HPE Superdome Flex 280 also supports SNMP traps. Simply log into the RMC CLI and designate the trap receiver. HPE Superdome Flex 280 SNMP traps are primarily encapsulations of Redfish events, with the SNMP information indicating severity.

Service events

In addition to the regular eventing that occurs for status changes and issues, HPE Superdome Flex 280 also connects to HPE OneView Remote Support or HPE Insight Remote Support. These tools receive service events from RMC, which are actionable events automatically forwarded to HPE Support, enabling the fastest possible service response.

HPE OneView monitoring

HPE OneView can be set up to monitor HPE Superdome Flex 280 systems using the Redfish connection. When an issue or status change occurs, HPE OneView will receive a Redfish alert, request the status of the alert, and then gather more health information from the RMC. In the HPE OneView UI, you can see the list of events on all systems HPE OneView is monitoring. You can analyze details and see affected components at any event. If Remote Support is enabled in HPE OneView (or enabled separately using HPE Insight Remote Support), you can also see the service events being sent to HPE.

RMC details

If it is necessary to dig deeper than the information provided by the Analysis Engine and in HPE OneView (which in most cases is sufficient for troubleshooting), the RMC contains a wealth of additional information that expert administrators and HPE Support can tap into to understand and diagnose issues. The following is a subset of information available on the RMC for advanced troubleshooting. For example, the Analysis Engine logs are fully qualified troubleshooting results, complete with recommended actions to take. Be sure to analyze every individual entry to see all the details. Use the `show _logs` command to see the entire list of logs available for viewing.

TABLE 3. Advanced troubleshooting logs and commands available on the RMC

Log or command	Description	Use	Where
CAE	Analysis Engine log	Show the service events, indictments/de-configurations the Analysis Engine has determined	RMC CLI, RESTful https
IEL	Integrated event log	Merged stream of events from the entire system	RMC CLI, RESTful https
searchevents	RMC tool to grab filtered IEL view	searchevents -B 2 days ago; -A 3 Gives all > warning events 2 days ago to now	RMC CLI
support	Automated set of CLI commands	To dump system status and key logs for support to screen capture on SSH	RMC CLI
audit	All security-relevant RMC activity	Security audit information; also useful for change log	RMC CLI, RESTful https
RCU Logs	Generated when a problem occurs	More detailed, diagnostic information for support	RMC CLI—downloadable

For more information on monitoring and troubleshooting, refer to the [Configuring and Operating HPE Superdome Flex 280 Server guide](#).



Firmware update

As HPE Superdome Flex 280 is a mission-critical system, firmware updates are carefully managed and tested. UEFI, BMC, RMC, and FPGAs are not released and managed as separate, independent firmware images, as they are on most x86 systems. Instead, there is one firmware package, with one revision for HPE Superdome Flex 280 called the complex firmware. The embedded firmware management subsystem checks the firmware package against the hardware in all the chassis and then applies the UEFI, BMC, and RMC updates to the entire system. The RMC checks all system components to ensure they comply with the installed firmware package and reports any out-of-sync hardware (due to a board replacement). The firmware service updates the entire set on the system to ensure everything works together and is supported by HPE.

Online-initiated firmware updates are supported. UEFI firmware for the system is updated, but it does not become active until the next time the server is rebooted.

There are several ways to update firmware—using HPE Smart Update Manager (SUM), HPE OneView Firmware Update, or CLI firmware update, and by scripting to the Redfish UpdateService API.

HPE SUM

As HPE’s firmware management and update tool for enterprise environments, HPE SUM can remotely update all the HPE Superdome Flex 280 server’s firmware, as well as firmware from other HPE products. HPE SUM offers recommendations for firmware that needs updating and it has an easy-to-use web user interface that provides reporting capabilities and dependency checking. HPE SUM also installs updates in the correct order through the CLI and/or GUI.

With HPE SUM, updating a system’s complex firmware is made easy—simply run the tool on the data center’s management network (Note: HPE SUM is included in any new HPE Superdome Flex 280 firmware bundle). Provide the RMC IP address, HPE SUM will query the system, and then you can run an update using the user interface.

HPE SUM performs I/O updates, which can be completed offline by booting the SUM ISO on the server or initiated online by running it on a supported OS.

For more information about HPE SUM, visit hpe.com/servers/sum.

HPE OneView firmware update

HPE OneView supports managed mode operations on HPE Superdome Flex 280 systems, which include the ability to update the system complex firmware and maintain a firmware baseline. For complete details, refer to the [HPE OneView documentation](#).

RMC CLI firmware update

The RMC SSH CLI can also initiate a firmware update, and the RMC can download the firmware using the HTTPS, SFTP, or SCP protocol from a server on the management network. For more details, refer to the [Configuring and Operating HPE Superdome Flex 280 Server guide](#).

TABLE 4. HPE firmware update options—which tool for which use case

	HPE SUM	HPE OneView firmware update	RMC CLI firmware update
Recommended use cases	<ul style="list-style-type: none"> Updating complex firmware of one or more HPE Superdome Flex 280 systems simultaneously using the same firmware bundle I/O updates 	<ul style="list-style-type: none"> Updating complex firmware of one or more HPE Superdome Flex 280 systems simultaneously using the same firmware bundle Cannot be used for I/O updates 	<ul style="list-style-type: none"> Updating complex firmware on one HPE Superdome Flex 280 system

Security

As threats move from network security to the hardware and firmware layers, HPE Superdome Flex 280 security features help protect hardware, firmware, and network components from unauthorized access and security threats. The HPE Superdome Flex 280 RMC requires no additional licensing to use any of its security features. The RMC security features are designed to meet the enterprise-level security challenges found in physically protected data centers. The security settings default to recommended security settings. For example, features such as IPMI need to be enabled once a user confirms they are operating in a protected environment.



Some of the key security features in HPE Superdome Flex 280 are:

Silicon Root of Trust from HPE

HPE Superdome Flex 280 comes with built-in Silicon root of trust from HPE implemented directly in HPE controlled specialized hardware that detects potentially compromised firmware every time the system is powered on and prevents it from running. The Silicon Root of Trust from HPE is the first step in the chain of trust using CNSA-level code signing cryptography. All the way from the first code started as AC power is applied to the system, up to and including loading BIOS.

HPE Superdome Flex 280 also has added a resiliency/recovery feature to firmware that utilizes the detections in the chain of trust in Silicon root of trust from HPE. If any issues are detected, the system will automatically switch over to an alternate known-good image in the hardware.

Phlashing protection

Phlashing is a permanent denial of service (PDOS) attack. A PDOS attack could theoretically take advantage of vulnerabilities during updates of network-based firmware. Rogue firmware installed through a PDOS attack could lead to unauthorized server access or permanent hardware damage. HPE Superdome Flex 280 BIOS cannot be written from the host side and there are no direct firmware update paths for UEFI BIOS or manageability from the host. I/O card firmware and option ROMs are a notable exception to this rule.

TPM 2.0

Trusted Platform Module (TPM, also known as ISO/IEC 11889) is an international standard for a secure cryptoprocessor, built based on the Trusted Computing Group (TCG) specification and provides tamper-resistant functionality, protected storage for keys, Platform Configuration Registers (PCRs) to store code measurements and enables many other security features including measured boot and OS features such as drive encryption. HPE Superdome Flex 280 uses the latest version, TPM 2.0, and the component is soldered down onto every HPE Superdome Flex 280 base chassis.

Optional intrusion detection

To protect against unauthorized access of the hardware components in the system, HPE Superdome Flex 280 offers optional intrusion detection switches to detect and log time the hardware was accessed even with power off.

Air-gapped manageability

During the past few years, ransomware has targeted manageability, making it critically important to keep the management network separate from any access to the internet, as well as limited to a smaller number of authorized users. While the manageability system of some industry-standard designs shares the system NIC to cut costs, the HPE Superdome Flex 280 manageability network controller is separate and independent from the system network controllers installed in the system. This means the two networks remain separate, with no worries of a side-channel attack into the manageability network. The RMC is physically unable to bridge traffic between its Ethernet port and the server Ethernet port—so attacks on the server network will not compromise the RMC and vice-versa.

Operating in a demilitarized zone (DMZ)

The RMC is designed to be placed on a separate, secondary network parallel to the primary (production) network. This dual-network architecture separates management traffic from production network traffic. This separation-of-duties strategy allows for restrictive group lists for distinct server management activities and production administration activities inside separate DMZ networks.

Unauthorized access prevention

Access through an RMC portal involves a multilayer security process that includes authentication, authorization, data integrity, and security keys. RMC firmware is digitally signed with a private key that prohibits unauthorized firmware from executing. Remote access to the RMC requires a password. Multiple local accounts can be assigned, preventing the need to share passwords. Three levels of access are available to provide access appropriate to a user's role. Local passwords are synchronized across the complex of connected chassis. LDAP and Active Directory support are available for ease of use. The local serial port can be used for local password recovery; as such, the port should not be connected to any hardware that makes it available remotely.

Authorized secure remote firmware updates

HPE Superdome Flex 280 firmware is updated in a bundle of firmware designed and tested to work together. HPE Superdome Flex 280 can only be updated through the HPE Superdome RMC manageability features. The entire bundle is hashed with SHA512 and signed using the RSA 4096-bit private key from HPE. This signature block is appended to the bundle binary image. When performing a firmware update, the hash is decrypted by the currently executing RMC firmware with HPE's public key. This hash is compared with a hash of the entire image; if the hashes match, the firmware update can proceed. This way, only firmware properly signed by HPE is allowed for an update and the check is automatically performed by the built-in firmware in the RMC before the update proceeds.



Minimized surface area for attack

The HPE Superdome Flex 280 mission-critical servers are not exposed to many of the vulnerabilities common in the server industry because HPE does not include the interfaces and features that are commonly listed with vulnerabilities. Features such as legacy BIOS support, ME, full SPS, AMT, I.E., TXT, and others have been used as attack surfaces against many x86 architecture systems. HPE Superdome Flex 280 includes none of these features, so it is not exposed to security attacks in these areas. Removing these features from HPE Superdome Flex 280 also reduces the number of updates required to fix industry-discovered vulnerabilities in these areas.

Authentication and audit trails

RMC creates a security audit log of authentication failures and successes across every interface, including many security parameter changes such as user accounts, log changes, and certificates. If a company's policy mandates periodic security audits, the RMC maintains an extensive event log containing date- and time-stamped information pertaining to events that occurred in the RMC configuration and operation. Manual access to this log is available via the RMC CLI. SSH-key authentication makes successful brute force attacks even less likely. For additional protection, the RMC uses 3072-bit RSA keys. Weak ciphers are not supported.

Secure out-of-box

Secure out-of-box refers to initial login access to the system, as well as having unencrypted RMC ports disabled by default. Default or well-known user IDs/passwords pose a security threat to the platform infrastructure. Each HPE Superdome Flex 280 server ships with unique random passwords. No common default passwords are used. Unencrypted ports such as IPMI can be enabled from the RMC if necessary. Unused networking ports can also be disabled to reduce the attack surface.

UEFI Secure boot

UEFI Secure boot ensures that only firmware components, UEFI applications, and OS bootloaders that have appropriate digital signatures—and verify as authentic—can run during the boot process. Secure boot ensures that each component launched during the boot process is digitally signed and that the signature is validated against a set of trusted certificates embedded in the UEFI BIOS. Secure boot validates the software identity of the following components in the boot process:

- UEFI drivers loaded from PCIe cards
- UEFI drivers loaded from mass storage devices
- Preboot UEFI shell applications
- OS UEFI bootloaders

Alternatives to PXE boot

PXE is a common OS deployment method; however, PXE is not encrypted. Rogue PXE servers in an IT infrastructure could install malware or ransomware. HPE Superdome Flex 280 does not enable PXE boot by default. To use it, the boot order must be adjusted from the factory defaults. Alternatives that are more secure than PXE include HTTP boot from UEFI and directed LAN boot from UEFI, as well as virtual media, which can be done interactively, or scripted from Redfish.

CONCLUSION

HPE Superdome Flex 280 servers include the comprehensive tools and utilities to manage your environment and address any challenge in your data center. The HPE management capabilities are graphical and easy to use, and industry-standard capabilities allow HPE Superdome Flex 280 servers to easily fit within your enterprise. With these management utilities, it is simple to set up and run your server. In addition, sophisticated tools can monitor, analyze, and alert you to issues you need to address.

If your enterprise uses HPE management solutions such as HPE OneView or HPE SUM, or you have a custom management environment based on industry standards such as OpenStack or Redfish APIs, then you can trust HPE Superdome Flex 280 to easily create and maintain a mission-critical platform for your applications.



APPENDIX 1: REDFISH EXAMPLES

For a wide variety of tools, examples, how-to videos, and more go to the Redfish industry-standard portal: redfish.dmtf.org/.

Simple examples using Linux curl

From the Linux command line on a system able to reach the RMC over HTTPS, you can send simple HTTPS JSON to Redfish and get responses using the built-in shell command, `curl`. See the main pages for specific usage of `curl` on your Linux distribution.

The following examples use an RMC hostname of **myrmc.mycorp.com**, and a username/password of **administrator** and **SDF!123abc**.

```
export HOST="myrmc.mycorp.com" # To save typing
```

Another best practice is to pipe the output of the RMC through something that will format the JSON for easier reading. For instance, Python has a nice JSON tool.

Get RMC information

```
curl -gk -X GET --user administrator:SDF!123abc https://${HOST}/redfish/v1/Managers/RMC | python3 -m json.tool
```

This command will dump the RMC top-level model. You can continue to run individual `curl` commands, each providing the username/password, or you can create a session.

Sessions

Redfish supports a facility to retrieve an authentication token to use for a session, in the same way a browser session does for https. To get a token for a session, POST to `/redfish/v1/SessionService/Sessions/` to create a session. The authentication token is part of the response from that POST. Use the authentication token in subsequent commands, then (as a best practice), remove your session from `SessionService` when you are done. Complete details are included in how-to videos on redfish.dmtf.org/.

The following combines the POST with a variable set, to grab the authentication token for later use.

```
export AUTH_TOKEN=$(curl -gikx "" -X POST -H 'Content-Type: application/json' -d '{"UserName": "administrator", "Password": "SDF!123abc"}' https://${HOST}/redfish/v1/SessionService/Sessions/ | awk '/X-Auth-Token/ {print $2}' | tr -d '\r\n' )
```

This command should grab the authentication token from the output of the POST to create the session, and now you have it in a bash variable.

Power on

```
curl -gikx "" --include -H "X-Auth-Token: ${AUTH_TOKEN}" -X POST -H 'Content-Type: application/json' -d '{"ResetType": "On"}' https://${HOST}/redfish/v1/Systems/Partition0/Actions/ComputerSystem.Reset
```

Power off—force

```
curl -gikx "" --include -H "X-Auth-Token: ${AUTH_TOKEN}" -X POST -H 'Content-Type: application/json' -d '{"ResetType": "ForceOff"}' https://${HOST}/redfish/v1/Systems/Partition0/Actions/ComputerSystem.Reset
```

Graceful shutdown

```
curl -gikx "" --include -H "X-Auth-Token: ${AUTH_TOKEN}" -X POST -H 'Content-Type: application/json' -d '{"ResetType": "GracefulShutdown"}' https://${HOST}/redfish/v1/Systems/Partition0/Actions/ComputerSystem.Reset
```

A GET example with Token—Network details

```
curl -gk -H "X-Auth-Token: ${AUTH_TOKEN}" -X GET -H 'Content-Type: application/json' https://${HOST}/redfish/v1/Managers/RMC/EthernetInterfaces/1/ | python3 -m json.tool
```

Check the task after each power operation

```
curl -gikx "" --include -H "X-Auth-Token: ${AUTH_TOKEN}" -H 'Content-Type: application/json' https://${HOST}/redfish/v1/TaskService/Tasks/<TaskID>
```



```
Example: curl -gikx "" -H "X-Auth-Token: ${AUTH_TOKEN}"
https://${HOST}/redfish/v1/TaskService/Tasks/c83a1a0d19564145bde2069c4459be5b
```

Get the top level server information

```
curl -gk -H "X-Auth-Token: ${AUTH_TOKEN}" -X GET -H 'Content-Type: application/json'
https://${HOST}/redfish/v1/Systems/Partition0/ | python3 -m json.tool
```

Finally, in a script using a session, it's always good to delete the session after finishing. Use GET, similar to previous command, to get /redfish/v1/SessionService/Sessions/ and find the session ID you are using. (Or, note it during the step to get the authentication token.) Then just delete that object from the SessionService. This example deletes the session, administrator... d2.

Delete session

```
curl -gik -H "X-Auth-Token: ${AUTH_TOKEN}" -X DELETE -H 'Content-Type: application/json'
https://${HOST}/redfish/v1/SessionService/Sessions/administratord3ab9dcf623149d38749b1037b8bb5d2
```

Postman

Postman is an open source developer's environment for JSON web-based interfaces. While it is not specifically for Redfish, Postman works quite well with Redfish. This environment can be easily configured to send GET, POST, and DELETE operations, using either default username/password authentication, or using session tokens. For more information, visit getpostman.com.

Because it provides ways to save queries, and it formats the output nicely, Postman is a good environment for developing automation against Redfish.

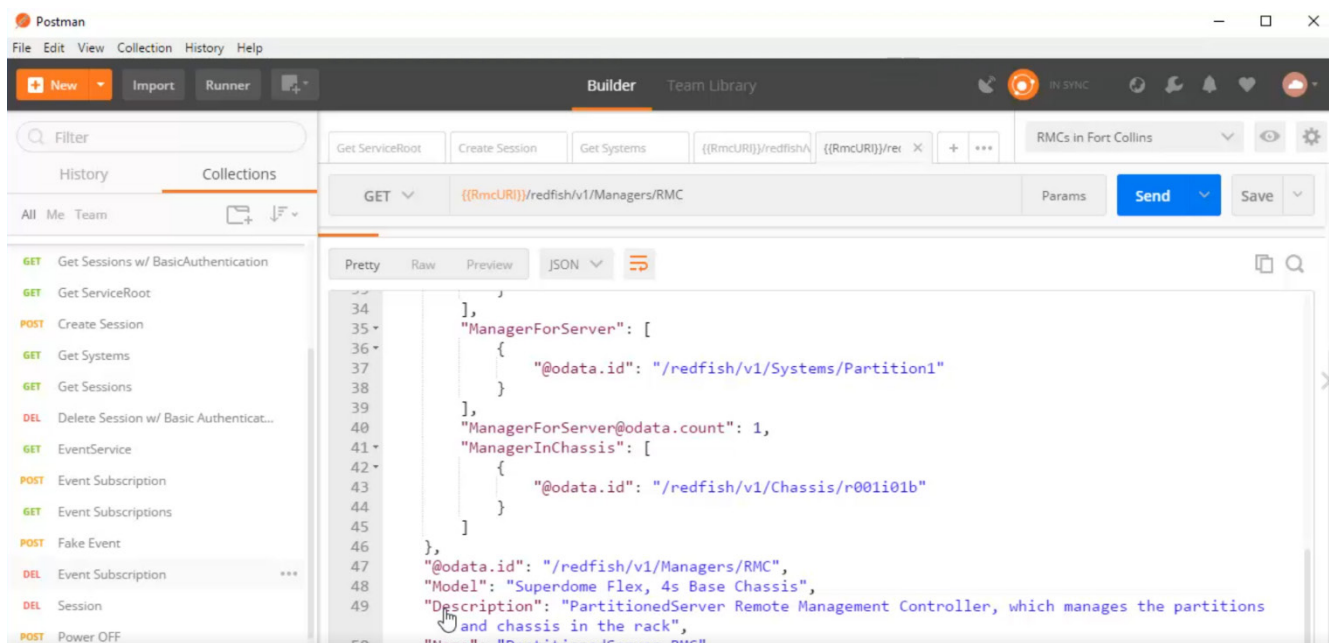


FIGURE 14. Postman user interface

Redfishtool

Redfishtool is a CLI tool provided by the DMTF standards body. Redfishtool is one of the many tools available from the Redfish GitHub tools, contributed by the various companies and organizations using Redfish. The tool can provide access to many of the simple functions you might want to perform (in a command-line fashion), similar to the IPMITool for the legacy IPMI standard. Some Redfishtool examples are provided in the [Configuring and Operating HPE Superdome Flex 280 Server guide](#); extensive information is also provided on github.com/DMTF/Redfishtool.

Python

Python libraries, as well as Python examples, are available on the DMTF GitHub to help you create Python scripts for automation using Redfish.



APPENDIX 2: OPENSTACK BARE METAL CERTIFICATION MATRIX

At the publication of this white paper, the information in this table is correct; however, newer firmware and newer OpenStack bare-metal features continue to be certified on HPE Superdome Flex 280.

OpenStack bare-metal service features have been certified on HPE Superdome Flex 280 systems in the following environments:

- OpenStack Ironic releases: Rocky, Train, and Ussuri
- RHOSP 16
- Standalone Ironic: Bifrost starting from Ussuri release Ironic

Features with OpenStack Ironic Redfish driver

Features	HPE Superdome Flex	HPE Superdome Flex 280
Node enroll/delete	✓	✓
Power operations On/off/reset	✓	✓
Graceful restart/Graceful shutdown		
In band Hardware inspection	✓	✓
Deploy OS with cloud format partition / whole-disk images SLES12SPx SLES15SPx RHEL7.x RHEL8.x OL7.x OL8.x OVM Windows Server 2016 (whole-disk format only) Windows Server 2019 (whole-disk format only)	✓	✓
Deploy OS to a Fibre Channel volume and boot	✓	✓
Configdrive for post install tasks	✓	✓
Undeploy (node tear down)	✓	✓
Cinder volume attach	✓	✓
Automated cleaning	✓	✓
Node rescue	✓	✓

Value-add features with Ironic sdflex-redfish driver

Features	HPE Superdome Flex	HPE Superdome Flex 280
Secure boot	✓	✓
Directed LAN boot	✓	✓
UEFI-HTTP boot	✓	✓
BIOS settings	✓	✓
RAID configuration	✓	✓
Hardware disk erase	✓	✓
Firmware update—Complex and nPar (UEFI) firmware	✓	✓
I/O firmware update using SUM	✓	✓
Boot from preprovisioned Fibre Channel volume	✓	✓
Virtual media based OS provisioning (PXE-less)		✓

NOTE

Refer to the OpenStack section in the [Installing Operating Systems on HPE Superdome Flex 280 Server guide](#) and [sdflex-redfish driver wiki page](#) for more details.



Resources

[HPE Superdome Flex 280 Product Page on hpe.com](#)

[Installing Operating Systems on HPE Superdome Flex 280 Server guide](#) explains how to install HFS

[Configuring and Operating HPE Superdome Flex 280 Server guide](#) provides details on HFS, such as the functionality and commands

[HPE Remote Support](#)

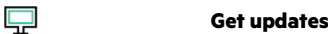
[HPE Smart Update Manager](#)

[HPE OneView](#)

LEARN MORE AT

hpe.com/superdome

**Make the right purchase decision.
Contact our presales specialists.**



© Copyright 2021 Hewlett Packard Enterprise Development LP. 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.

Intel and Intel Xeon are trademarks of Intel Corporation in the U.S. and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Active Directory, Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries. VMware ESXi and VMware are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. Java and Oracle are registered trademarks of Oracle and/or its affiliates. All third-party marks are property of their respective owners.

a50003038ENW, Rev. 1