

HP OneView 1.0 User Guide

Abstract

This guide describes HP OneView features, interfaces, resource model design, and secure working environment. It describes up-front planning considerations and how to use the HP OneView appliance UI or REST APIs to configure, manage, monitor, and troubleshoot your data center infrastructure. It also includes information about the SCMB (State-Change Message Bus) and a step-by-step example that configures a sample data center from start to finish.



© Copyright 2013 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP 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. The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

Google™ is a trademark of Google Inc. Java is a trademark of Oracle or its affiliates. Microsoft® is a US registered trademark of Microsoft Corporation.

Warranty

HP will replace defective delivery media for a period of 90 days from the date of purchase.

Contents

I Learning about HP OneView.....	13
1 Learning about HP OneView.....	15
1.1 HP OneView for converged infrastructure management.....	15
1.2 Hardware and software provisioning features.....	16
1.2.1 Server profiles.....	17
1.2.2 Groups, templates, and sets.....	17
1.2.3 Streamlined process for bringing hardware under management.....	19
1.2.4 Operating system deployment.....	19
1.3 Firmware and configuration change management features.....	20
1.3.1 Simplified firmware management.....	20
1.3.2 Simplified configuration change management.....	20
1.4 Monitoring and response features.....	20
1.4.1 Data center environmental management.....	22
1.4.2 Resource utilization monitoring.....	22
1.4.3 Alert and health management	22
1.4.4 Hardware and firmware inventory information.....	23
1.5 Backup and restore features.....	23
1.6 Security features.....	24
1.7 Availability features.....	24
1.8 Graphical and programmatic interfaces.....	25
1.9 Integration with other HP management software.....	26
1.10 Open integration.....	26
1.11 Convenient licensing model.....	26
1.12 Networking features.....	27
2 Understanding the resource model.....	29
2.1 Resource model summary diagram.....	29
2.2 Server profiles.....	30
2.3 Connection templates.....	30
2.4 Connections.....	31
2.5 Server hardware types.....	31
2.6 Server hardware.....	32
2.7 Enclosure groups.....	33
2.8 Enclosure types.....	33
2.9 Enclosures.....	34
2.10 Interconnect types.....	34
2.11 Interconnects.....	35
2.12 Logical interconnect groups.....	36
2.13 Logical interconnects.....	37
2.14 Uplink sets.....	38
2.15 Networks.....	39
2.16 Network sets.....	39
2.17 Domains.....	40
2.18 Appliance.....	40
2.19 Resources related data center facilities.....	41
2.19.1 Data centers.....	41
2.19.2 Racks.....	41
2.19.3 Power delivery devices.....	42

2.19.4 Unmanaged devices.....	42
3 Understanding the security features of the appliance.....	45
3.1 Securing the appliance.....	45
3.2 Best practices for maintaining a secure appliance.....	46
3.3 Creating a login session.....	47
3.4 Authentication for appliance access.....	47
3.5 Controlling access for authorized users.....	48
3.5.1 Specifying user accounts and roles.....	48
3.6 Protecting credentials.....	48
3.7 Understanding the audit log.....	48
3.8 Appliance access over SSL.....	50
3.9 Managing certificates from a browser.....	50
3.9.1 Overview.....	50
3.9.2 Self-signed certificate.....	50
3.9.2.1 Verifying a certificate.....	51
3.9.2.2 Downloading and importing a self-signed certificate.....	51
3.9.3 Using a certificate authority.....	51
3.10 Browser best practices for a secure environment.....	52
3.11 Nonbrowser clients.....	52
3.11.1 Passwords.....	52
3.11.2 SSL connection.....	52
3.12 Ports needed for HP OneView.....	53
3.13 Access to the appliance console.....	53
3.13.1 Enabling or disabling authorized services access.....	54
3.13.2 Restricting console access.....	54
3.14 Algorithms for securing the appliance.....	54
3.15 Downloads from the appliance.....	55
4 Navigating the graphical user interface.....	57
4.1 Browsers.....	57
4.1.1 Supported browsers.....	57
4.1.2 Required plug-ins and settings.....	57
4.1.3 Commonly used browser features and settings.....	57
4.1.4 Set the browser for US or metric units of measurement.....	58
4.2 About the graphical user interface.....	58
4.3 About the Activity sidebar.....	60
4.4 Banner and main menu.....	60
4.5 Button functions.....	60
4.6 Filters sidebar.....	61
4.7 Help sidebar.....	61
4.8 Icon descriptions.....	62
4.8.1 Status and severity icons.....	63
4.8.2 User control icons.....	63
4.8.3 Informational icons.....	64
4.9 Map view screen details.....	64
4.10 Notifications area.....	65
4.11 Log out of the appliance.....	66
4.12 Search help topics.....	66
4.12.1 About help system search results.....	67
4.13 Search resources.....	67
4.14 View resources according to their health status.....	68
4.14.1 Reset the health status view.....	69

5	Using the REST APIs and other programmatic interfaces.....	71
5.1	Resource operations.....	71
5.2	Return codes.....	72
5.3	URI format.....	72
5.4	Resource model format.....	72
5.5	Log in to the appliance using REST APIs.....	72
5.6	REST API version.....	72
5.7	Asynchronous versus synchronous operations.....	73
5.8	Task resource.....	73
5.9	Error handling.....	73
5.10	Concurrency control using etags.....	73
5.11	Querying resources using common REST API parameters.....	74
5.12	State Change Message Bus.....	74
5.13	Developer tools in a web browser.....	74
5.14	Using Python and Windows PowerShell commands (technical preview).....	74
6	Accessing documentation and help.....	75
6.1	Online help—conceptual and task information as you need it.....	75
6.2	This user guide supplements the online help.....	75
6.3	Where to find HP OneView documentation.....	76
6.4	Enabling off-appliance browsing of UI and REST API HTML help files.....	76
II	Planning tasks.....	77
7	Planning your data center resources.....	79
7.1	How many data centers?.....	79
7.2	Security planning.....	79
7.2.1	Choosing an Administrator password.....	79
7.2.2	Choosing the LAN for the appliance.....	79
7.2.3	Choosing whether or not to enable support access.....	79
7.2.4	Choosing an SNMP read community string.....	79
7.2.5	Choosing a security certificate policy.....	80
7.2.6	Determining roles and restrictions for authorized users.....	80
7.2.7	Determining your backup policy.....	80
7.2.8	Choosing a policy for the audit log.....	80
7.2.9	Determining your vSphere client policy.....	80
7.2.10	Reviewing your firewall access.....	81
7.3	Preparing your data center network switches.....	81
7.4	Planning your resource names.....	81
7.5	Planning the appliance configuration.....	82
7.5.1	Appliance VM and host requirements.....	82
7.5.2	Planning for high availability.....	83
7.5.3	Location of the appliance.....	83
7.5.4	Separate networks for data and management.....	83
7.5.5	Time clocks and NTP.....	83
7.5.6	IP addresses.....	83
8	Planning for configuration changes.....	85
8.1	Configuration changes that require or result in resource outages.....	85
8.2	Configuration changes that might require changes to multiple resources.....	86
8.2.1	Adding a network.....	86
8.2.2	Adding an enclosure.....	87

III Configuration quick starts.....	89
9 Quick Start: Initial Configuration.....	91
9.1 Process overview.....	91
9.2 Configure the environment for the first time.....	91
10 Quick Start: Adding a network to an existing appliance environment.....	95
11 Quick Start: Adding an enclosure and connecting its server blades to networks.....	99
11.1 Checklist: connecting a server blade to a data center network.....	99
11.2 Scenario 1: Adding the enclosure to an existing enclosure group.....	100
11.3 Scenario 2: Defining network connectivity before the enclosure is added.....	101
11.4 Scenario 3: Defining network connectivity as you add the enclosure.....	102
12 Quick Start: Configuring an enclosure and server blade for Direct attach to an HP 3PAR Storage System.....	105
13 Quick Start: Adding an HP ProLiant DL rack mount server.....	107
IV Configuration and management.....	109
14 Managing servers and server profiles.....	111
14.1 Server hardware features supported by the appliance.....	111
14.2 Prerequisites for bringing server hardware under management.....	112
14.3 Roles.....	112
14.4 Tasks for server profiles.....	112
14.5 Tasks for server hardware.....	113
14.6 Tasks for server hardware types.....	113
14.7 Effects of managing server hardware iLOs.....	113
14.8 Learning more.....	114
15 Managing networks and network resources.....	115
15.1 Data center switch port requirements.....	115
15.2 Managing Fibre Channel networks (SANs).....	115
15.2.1 Roles.....	116
15.2.2 Tasks.....	116
15.3 Managing Ethernet networks.....	116
15.3.1 Roles.....	116
15.3.2 Tasks.....	116
15.4 About network connectivity.....	116
15.4.1 About Fibre Channel networks.....	117
15.4.1.1 Fibre Channel network types.....	117
15.4.1.2 Fabric attach Fibre Channel networks.....	118
15.4.1.3 Direct attach Fibre Channel networks.....	118
15.4.1.4 Fibre Channel networks and FCoE.....	119
15.4.2 About Ethernet networks.....	119
15.4.2.1 Ethernet networks and VLAN IDs.....	119

15.4.3 About network sets.....	119
15.5 Learning more.....	120
16 Managing interconnects, logical interconnects, and logical interconnect groups.....	121
16.1 Managing enclosure interconnect hardware.....	121
16.1.1 Roles.....	121
16.1.2 Tasks.....	121
16.1.3 About interconnects.....	121
16.1.4 Learning more.....	122
16.2 Managing logical interconnects and logical interconnect groups.....	122
16.2.1 Roles.....	123
16.2.2 Tasks.....	123
16.2.3 About logical interconnects.....	123
16.2.4 About logical interconnect groups.....	126
16.2.5 About SNMP settings.....	127
16.2.6 Update the logical interconnect configuration from the logical interconnect group.....	128
16.2.7 Configure a port to monitor network traffic.....	129
16.2.8 Learning more.....	129
17 Managing enclosures and enclosure groups.....	131
17.1 Prerequisites for bringing an enclosure under management.....	131
17.2 Roles.....	132
17.3 Tasks.....	132
17.4 About enclosures.....	132
17.5 About enclosure groups.....	133
17.6 Effects of managing an enclosure.....	133
17.7 Learning more.....	133
18 Managing firmware for managed devices.....	135
18.1 About the appliance firmware repository.....	135
18.2 About unsupported firmware.....	135
18.3 Roles and Tasks.....	136
18.4 The firmware update process.....	136
18.5 Best practices for firmware.....	137
18.6 Learning more.....	138
19 Managing power and temperature.....	139
19.1 Managing power.....	139
19.1.1 Roles.....	139
19.1.2 Tasks.....	139
19.1.3 About power delivery devices.....	139
19.1.4 About racks.....	140
19.2 Managing temperature.....	141
19.2.1 Roles.....	141
19.2.2 Tasks.....	141
19.2.3 About data centers.....	141
19.2.4 Learning more.....	142
20 Managing users and authentication.....	143
20.1 Roles.....	143

20.2 Tasks.....	143
20.3 About user accounts.....	143
20.4 About user roles.....	144
20.5 Action privileges for user roles.....	144
20.6 About authentication settings.....	146
20.7 About directory service authentication	146
20.8 Managing user passwords.....	147
20.9 Reset the administrator password.....	148
20.10 Learning more.....	148
21 Backing up an appliance.....	149
21.1 Overview of the backup process.....	149
21.2 Roles.....	149
21.3 Backup file name.....	149
21.4 Guidelines for creating a backup file.....	150
21.5 Create and download a backup file.....	150
21.6 Using REST APIs to create and download an appliance backup file.....	151
21.7 Creating a custom script to create and download an appliance backup file.....	151
22 Managing the appliance.....	153
22.1 Managing appliance availability.....	153
22.1.1 Best practices for managing a VM appliance.....	153
22.1.2 How the appliance handles an unexpected shutdown.....	153
22.1.2.1 What to do when an appliance restarts.....	154
22.1.3 Shut down the appliance.....	154
22.1.4 Restart the appliance.....	154
22.2 Managing the appliance settings.....	155
22.2.1 Roles.....	155
22.2.2 Tasks.....	155
22.2.3 About appliance SNMP settings.....	155
22.2.4 Learning more.....	156
22.3 Managing addresses and ID pools.....	156
22.3.1 Roles.....	156
22.3.2 Tasks.....	156
22.4 Managing the security features of the appliance.....	156
22.4.1 Enabling or disabling HP support access to the appliance.....	156
22.4.1.1 Roles.....	157
22.4.1.2 Tasks.....	157
22.4.2 Managing SSL certificates.....	157
22.4.2.1 Roles.....	157
22.4.2.2 Tasks.....	157
22.4.2.3 Learning more.....	157
22.4.3 Managing the HP public key.....	157
22.4.3.1 Roles.....	158
22.4.3.2 Tasks.....	158
22.4.4 Downloading audit logs.....	158
22.4.4.1 Roles.....	158
22.4.4.2 Tasks.....	158
22.4.4.3 Learning more.....	158
22.5 Managing licenses.....	158
22.5.1 Roles.....	158
22.5.2 Tasks.....	158
22.5.3 About licensing.....	159

22.5.3.1 License types.....	159
22.5.3.2 License delivery.....	159
22.5.3.3 License reporting.....	159
22.5.3.4 View license status.....	160
22.5.4 Server hardware licensing.....	160
22.5.4.1 Server blade licensing at the enclosure level.....	161
22.5.4.2 Rack mount server licensing.....	162
22.5.4.3 Licensing and utilization statistics.....	162
22.5.4.4 Licensing scenarios.....	162
22.6 Updating the appliance.....	163
22.6.1 Roles.....	164
22.6.2 Tasks.....	164
22.6.3 Learning more.....	164

23 About unsupported and unmanaged hardware.....165

23.1 How the appliance handles unsupported hardware.....	165
23.2 About unmanaged devices.....	165

V Monitoring.....167

24 Monitoring data center status, health, and performance.....169

24.1 Daily monitoring.....	169
24.1.1 Initial check: the Dashboard.....	169
24.1.2 Activities.....	169
24.1.3 Utilization graphs.....	169
24.1.4 Monitor data center temperature.....	170
24.2 Best practices for monitoring data centers.....	170
24.2.1 Best practices for monitoring health with the appliance UI.....	170
24.2.2 Best practices for monitoring health using REST APIs.....	171
24.3 Managing activities.....	173
24.3.1 About activities.....	173
24.3.1.1 Activity types: alerts and tasks.....	174
24.3.1.2 Activity states.....	175
24.3.1.3 Activity statuses.....	175
24.4 Using the Dashboard screen.....	176
24.4.1 About the Dashboard.....	176
24.4.2 Dashboard screen details.....	176
24.4.3 How to interpret the Dashboard graphs.....	176

25 Monitoring power and temperature.....179

25.1 UI power and temperature monitoring.....	179
25.1.1 Monitoring data center temperature.....	179
25.1.1.1 Manipulating the view of the data center visualization.....	180
25.1.2 Monitoring power and temperature utilization.....	181
25.1.2.1 About the Utilization panel.....	181
25.1.2.2 About utilization graphs.....	181
25.2 REST API power and temperature monitoring.....	184
25.2.1 Update enclosure power capacity settings.....	184
25.2.2 Update server hardware power capacity settings.....	184

26 Using the State-Change Message Bus (SCMB).....	185
26.1 Connect to the SCMB.....	185
26.2 Set up a queue to connect to the HP OneView SCMB exchange.....	186
26.3 JSON structure of message received from the SCMB.....	187
26.4 .NET C# code example.....	188
26.5 Java code example.....	191
26.6 Python code example.....	192
26.7 Re-create the AMQP client certificate.....	195

VI Troubleshooting.....197

27 Troubleshooting.....	199
27.1 Basic troubleshooting techniques.....	200
27.2 Create a support dump file.....	201
27.3 Create a support dump for authorized technical support using REST API scripting.....	202
27.4 Troubleshooting the appliance.....	203
27.4.1 First time setup.....	203
27.4.2 Appliance cannot access the network.....	203
27.4.3 Unexpected appliance shutdown.....	203
27.4.4 Appliance update is unsuccessful.....	204
27.4.5 Support dump file creation action fails.....	204
27.4.6 Certificate action fails.....	204
27.4.7 Backup file creation, download, or restore action fails.....	205
27.4.8 Restart or shutdown failure.....	206
27.4.9 VM does not restart when VM host time is manually set.....	207
27.4.10 Reinstall the remote console.....	207
27.5 Troubleshooting enclosures and enclosures groups.....	208
27.5.1 Add or remove enclosure is unsuccessful.....	208
27.5.2 Add server blade is unsuccessful.....	210
27.5.3 Certificate Error.....	210
27.6 Troubleshooting firmware bundles.....	210
27.6.1 Incorrect credentials.....	210
27.6.2 Lost iLO connectivity.....	211
27.6.3 HP SUM errors.....	211
27.7 Troubleshooting interconnects.....	211
27.7.1 Interconnect edit is unsuccessful.....	211
27.7.2 Interconnect modules are in Maintenance state.....	211
27.8 Troubleshooting licensing.....	211
27.8.1 Restore a license key that has been erased from an enclosure OA.....	211
27.8.2 The license assigned does not match the type specified.....	212
27.9 Troubleshooting logical interconnects.....	212
27.9.1 I/O bay occupancy errors.....	212
27.9.2 Uplink set warnings or errors.....	212
27.9.3 Physical interconnect warnings and errors.....	213
27.10 Troubleshooting networks.....	213
27.10.1 Network create operation is unsuccessful.....	213
27.11 Troubleshooting server hardware.....	213
27.11.1 Server add or remove is unsuccessful.....	213
27.11.2 Cannot control power on server blade.....	214
27.11.3 Lost connectivity to server hardware after appliance restarts.....	214
27.12 Troubleshooting server profiles.....	215
27.12.1 Server profile is not created or updated correctly.....	215
27.12.2 What to do when you cannot apply the server profile.....	217

27.12.3 Profile operations fail.....	218
27.13 Troubleshooting user accounts.....	218
27.13.1 Incorrect privileges.....	218
27.13.2 Unauthenticated user or group.....	218
27.13.3 User public key is not accepted.....	219
27.13.4 Directory service not available.....	219
27.13.5 Cannot add directory service.....	219
27.13.6 Cannot add server for a directory service.....	220
27.13.7 Cannot add directory user or group.....	220
28 Restoring an appliance from a backup file.....	221
28.1 Roles.....	221
28.2 Restore operation overview.....	221
28.3 Preparing to restore an appliance.....	222
28.4 Restore an appliance from a backup file.....	223
28.5 Using REST APIs to restore an appliance from a backup file.....	224
28.6 Creating a custom script to restore an appliance.....	224
28.7 Post-restoration tasks.....	224
29 Support and other resources.....	227
29.1 Gather information before contacting an authorized support representative.....	227
29.2 How to contact HP.....	227
29.3 Get connected to the HP OneView online user forum.....	227
29.4 Software technical support and software updates.....	227
29.4.1 Registering for software technical support.....	227
29.4.2 Using your software technical support and update service.....	228
29.4.3 Obtaining HP OneView software and firmware updates.....	228
29.4.4 Obtaining software and drivers for HP ProLiant products.....	228
29.4.5 Warranty.....	228
29.5 Related information.....	228
29.6 Submit documentation feedback.....	229
A Step by step: Configuring an example data center using HP OneView.....	231
A.1 Tasks you can perform without data center hardware.....	231
A.2 Information about the sample data center.....	231
A.2.1 Sample data center hardware.....	231
A.2.2 Data center networks.....	233
A.2.2.1 Fibre Channel networks.....	233
A.2.2.2 Ethernet Networks.....	235
A.3 Planning the configuration.....	236
A.3.1 Planning for installation of the appliance.....	236
A.3.2 Planning for network sets.....	237
A.3.3 Planning for users and roles.....	237
A.3.4 Planning resource names.....	238
A.4 Installing the appliance.....	238
A.5 Provisioning eight host servers for VMware vSphere Auto Deploy.....	238
A.5.1 Workflow.....	238
A.5.2 Downloading the latest firmware bundle and adding it to the appliance.....	239
A.5.3 Configuring the networks and network sets.....	239
A.5.3.1 Configuring the Fibre Channel SAN networks.....	239
A.5.3.2 Configuring the Ethernet networks.....	240
A.5.3.3 Configuring the network sets.....	242
A.5.4 Creating a logical interconnect group and its uplink sets.....	244

A.5.5 Creating an enclosure group for vSphere (ESXi) hosts.....	248
A.5.6 Adding the enclosure.....	249
A.5.7 Viewing the server hardware types.....	249
A.5.8 Creating a server profile to use as a template.....	250
A.5.9 Copying the template server profile to eight servers.....	255
A.6 Configuring a server blade to boot from the attached HP 3PAR Storage System.....	256
A.6.1 Workflow.....	256
A.6.2 Creating the Flat SAN networks.....	256
A.6.3 Adding the enclosure that is connected to the HP 3PAR Storage System.....	257
A.6.4 Creating the server profile.....	260
A.6.5 Collecting the WWPNs to use when configuring the HP 3PAR Storage System.....	263
A.7 Bringing an HP ProLiant DL360p Gen8 rack mount server under management.....	264
A.7.1 Workflow.....	264
A.7.2 Adding the server hardware.....	265
A.7.3 Powering on the server.....	265
A.7.4 Viewing information about the server.....	265
A.7.5 Adding a license for the server.....	267
B Using the virtual appliance console.....	269
B.1 Using the virtual appliance console.....	269
C Backup and restore script examples.....	271
C.1 Sample backup script.....	271
C.2 Sample restore script.....	282
Index.....	293

Part I Learning about HP OneView

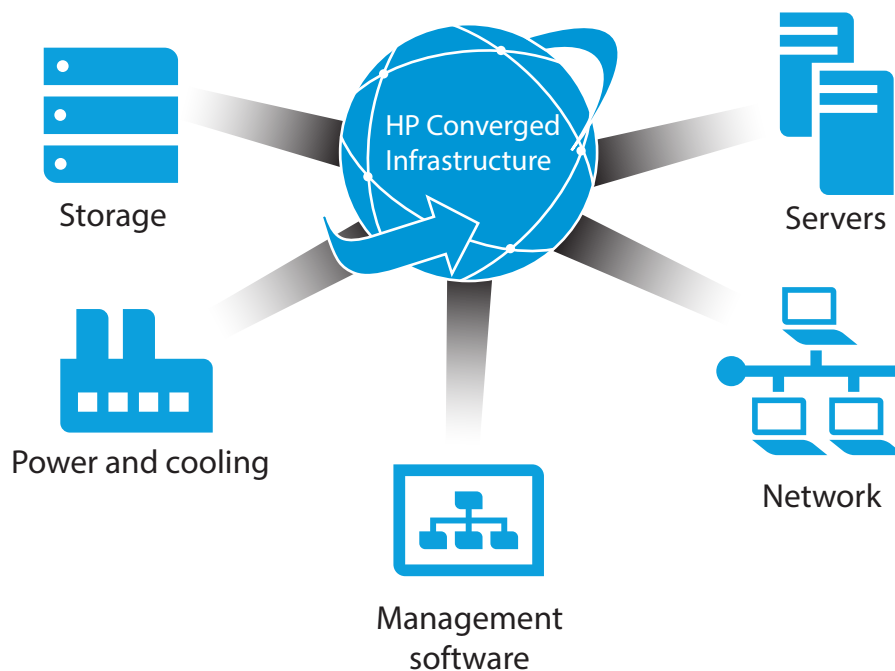
This part describes HP OneView and its model for data center resources and introduces you to the terms and concepts used in this document and the appliance online help.

1 Learning about HP OneView

1.1 HP OneView for converged infrastructure management

Optimized for collaboration, productivity, and reliability, the HP OneView appliance is designed to provide simple, single-pane-of-glass lifecycle management for the complex aspects of enterprise IT—servers, networking, software, power and cooling, and storage.

HP OneView is purpose-built to manage your converged infrastructure and support key scenarios such as deploying bare-metal servers, deploying hypervisor clusters from bare metal, performing ongoing hardware maintenance, and responding to alerts and outages. It is designed for the physical infrastructure needed to support virtualization, cloud computing, big data, and mixed computing environments.



Architecture

HP OneView is delivered as a virtual appliance running in a VMware vSphere virtual machine.

In contrast to management environments that require predefined serialized workflows and different tools for different tasks, HP OneView is a scalable resource-oriented solution focused on the entire life cycle—from initial configuration to on-going monitoring and maintenance—of both logical and physical resources:

- Logical resources are items such as networks, server profiles, and connections.
- Physical resources are items you can touch, such as server hardware, interconnects, and enclosures.

Software-defined flexibility—your experts design configurations for efficient and consistent deployment

The appliance provides several software-defined resources, such as groups and server profiles, to enable you to capture the best practices of your experts across a variety of disciplines, including networking, storage, hardware configuration, and operating system build and configuration. By having your experts define the server profiles and the networking groups and resources, you can eliminate cross-silo disconnects. By using RBAC (role-based access control) and the groups, sets,

and server profiles established by your experts, you can enable system administrators to provision and manage thousands of servers without requiring that your experts be involved with every server deployment.

One tool and one data set—one view

HP OneView combines complex and interdependent data center provisioning and management into one simplified and unified interface. You use one tool and one model to:

- [Provision the data center \(page 16\)](#)
- [Manage and maintain firmware and configuration changes \(page 20\)](#)
- [Monitor the data center and respond to issues \(page 20\)](#)

The solution also provides core enterprise management capabilities, including:

- [Availability features \(page 24\)](#)
- [Security features \(page 24\)](#)
- [Graphical and programmatic interfaces \(page 25\)](#)
- [Integration with other HP management software \(page 26\)](#)

The appliance manages servers and enclosure networking resources, supports connections from enclosures to storage, and provides information to help you manage data center power and cooling:

- Servers are represented and managed through their server profiles. For a brief overview of server profiles, see [“Server profiles” \(page 17\)](#). For detailed information about server profiles, see the online help for the **Server Profiles** screen.
- Storage devices connect to the enclosures using either Fibre Channel Fabric attach (SAN switch) connections or Fibre Channel Direct attach (flat SAN) connections. For more information about Fibre Channel network connections for storage, see [“About network connectivity” \(page 116\)](#).
- Networking is an essential component to provisioning and managing data center servers. For an overview of the networking features of the appliance, see [“Networking features” \(page 27\)](#). For detailed information about networking and the resource model, see [“Understanding the resource model” \(page 29\)](#).
- Environmental management—such as power, cooling, and space planning—requires that you consider all the equipment in the entire data center, including equipment not managed by HP OneView. HP OneView consolidates data center power and cooling information into one interface view. For an overview of the power and cooling management features, see [“Data center environmental management” \(page 22\)](#).

For an example of using the appliance to manage a data center, see [“Step by step: Configuring an example data center using HP OneView” \(page 231\)](#).

1.2 Hardware and software provisioning features

After you install the HP OneView appliance and perform the initial configuration tasks, you can quickly bring existing hardware under management and, using server profiles and other resource templates, groups, and sets, prepare for and deploy hardware to be added to your data center.

Features for provisioning hardware and bringing resources under management include:

- [Server profiles \(page 17\)](#)
- [Groups, templates, and sets \(page 17\)](#)
- [Streamlined process for bringing hardware under management \(page 19\)](#)
- [Operating system deployment \(page 19\)](#)

1.2.1 Server profiles

A server profile captures key aspects of a server configuration in one place, including firmware levels, BIOS settings, network connectivity, boot order configuration, iLO settings, and unique IDs. Server profiles are one of the features that enable you to provision converged infrastructure hardware quickly and consistently according to your best practices. Server profiles enable your experts to specify a server configuration before the server arrives, enabling your administrators to quickly bring a new server under management when the server hardware is installed.

For example, you can create a server profile that is not assigned to a particular server, but specifies all the configuration aspects—such as BIOS settings, network connections, and boot order—to use for a type of server hardware. After the server is installed in an enclosure bay, you can do one of the following:

- Directly assign the server profile to the enclosure bay
- Copy the server profile and assign the copy to the enclosure bay.

You can also copy or move a server profile that has been assigned to hardware in an enclosure bay. If you copy a server profile, you can save it for future use by not assigning the copy to an enclosure bay.

1.2.2 Groups, templates, and sets

Software-defined infrastructure—such as server profiles, groups, templates, and sets—enable you to:

- Use your experts to define server and networking configurations for specific environments before you install data center hardware.
- Provision hundreds of servers quickly and consistently without requiring that your experts take action for every server you deploy.
- Simplify the distribution of configuration changes across your data center.

Expert design with consistent deployment

Your experts in different technical areas can create templates, groups, and sets with their configuration best practices built in. Using these resources and server profiles, you can ensure that the infrastructure for thousands of workloads are provisioned consistently, regardless of who does the provisioning.

Server profiles capture the server configuration in once place. You can use unassigned server profiles to rapidly deploy multiple servers with the same configuration. For more information about server profiles, see [“Server profiles” \(page 17\)](#).

Types of groups and sets

Group or set	Description
Enclosure group	<p>A group of enclosures that use the same configuration, such network connectivity and firmware versions for the Onboard Administrator and interconnect modules. All members of an enclosure group use the same logical interconnect group. When you add an enclosure to the appliance and assign an enclosure group, the interconnects in the enclosure are configured automatically according to the logical interconnect group associated with the enclosure group. Enclosure groups enable administrators to provision multiple enclosures in a consistent, predictable manner in seconds.</p>
Logical interconnect group	<p>A group of logical interconnects that share the same configuration for network connectivity. A logical interconnect is the set of physical interconnects and their links, including the following:</p> <ul style="list-style-type: none">• Uplinks to data center networks as mapped by their uplink sets• Downlinks to the servers• Stacking links (connections to each other) <p>When you or your experts define configurations using logical interconnect groups and enclosure groups:</p> <ul style="list-style-type: none">• Administrators can provision multiple enclosures with consistent network configurations in seconds• Network administrators are not required to take action every time an enclosure is installed because the network configuration is defined by the enclosure group.
Uplink set	<p>A set of physical uplink ports in a logical interconnect that connect to a common set of networks. All member interconnects of a logical interconnect can contribute physical uplinks to an uplink set.</p> <p>Uplink sets can be defined as part of a logical interconnect or a logical interconnect group. When uplink sets are defined as part of a logical interconnect group, they act as the template for the uplink sets that are configured automatically when a logical interconnect is added to the logical interconnect group.</p>
Network set	<p>A set of Ethernet networks, designated by a single name. You can specify a network set instead of an individual network when you define a connection to data center Ethernet networks in a server profile. When you specify a network set in a connection, the server can access any of the networks in that set, including any networks that are subsequently added to that network set.</p>

Define configurations for specific environments

Groups and templates enable you to define configurations that are specific to the environment you want to build, such as VMware vSphere virtual hosts, Microsoft Exchange environments, external or internal web servers, or financial database servers.

For example, to build multiple external web servers:

1. Your networking expert can create logical interconnect groups, uplink sets, networks, and network sets to establish all of the connection policies between data center networks and the interconnects managed by the appliance.
2. Your server expert can create enclosure groups, add enclosures, and create server profiles to establish all of the settings required by an external web server.
3. Your server operators can copy server profiles whenever they need to deploy this type of server.

Flexibility in design and deployment

HP OneView provides flexibility in the creation of groups, templates, and sets. For example, you can create a logical interconnect group in these ways:

- Before you add an enclosure to the appliance, you can create a logical interconnect group that specifies how you want the interconnects to be configured, and an enclosure group that specifies how you want the enclosure to be configured.
- You can add an enclosure to the appliance and, after the appliance discovers and adds the interconnect hardware in the enclosure, you can use or modify the default logical interconnect group that the appliance creates.

Groups, templates, and sets also simplify the distribution of configuration changes across your data center. For more information about configuration changes, see [“Simplified configuration change management” \(page 20\)](#).

For more information about resources, including groups, templates, and sets, see [“Understanding the resource model” \(page 29\)](#).

1.2.3 Streamlined process for bringing hardware under management

HP OneView simplifies the process of bringing the enclosures, interconnects, and server hardware under management.

For example:

- When you add an enclosure, the appliance automatically detects all of the hardware seated in the enclosure and prepares it for you to bring under management. For example, the appliance:
 - Updates the enclosure Onboard Administrator, Virtual Connect interconnect module, and server iLO firmware to the minimum version required
 - Configures each Virtual Connect interconnect module
 - Configures the Onboard Administrator, which includes configuring NTP (Network Time Protocol) and configuring an SSO (single sign-on) certificate for UI access
 - Configures each server iLO, which includes configuring an SSO certificate for UI access
 - Configures the hardware for monitoring, which includes configuring the automatic registration of SNMP (Simple Network Management Protocol) traps
- When you add an HP Intelligent Power Distribution Unit (iPDU) power device, the appliance automatically detects and presents the connected devices so that you can bring the devices under management.

1.2.4 Operating system deployment

Server profiles and enclosure groups make it easier to prepare a bare-metal server for operating system deployment.

For example, you can use server profiles in conjunction with deployment tools such as:

- HP Insight Control server provisioning to install an operating system on the server
- VMware vSphere Autodeploy to deploy hypervisors from bare metal and add them to existing clusters automatically

1.3 Firmware and configuration change management features

1.3.1 Simplified firmware management

The appliance provides fast, reliable, and simple firmware management across the data center. When you add a resource to the appliance, to ensure compatibility and seamless operation, the appliance automatically updates the resource firmware to the minimum version required to be managed by the appliance.

An HP firmware bundle, also known as an SPP (Service Pack for ProLiant), is a tested update package of firmware, drivers, and utilities. Firmware bundles enable you to update firmware on server blades, and infrastructure (enclosures and interconnects).

An on-appliance firmware repository enables you to upload SPP firmware bundles and deploy them across your environment according to your best practices. For example you can:

- View the versions and contents of firmware bundles stored in the firmware repository.
- View the settings of the enclosures and interconnects, if any, that have a specific firmware bundle installed.
- Set a firmware baseline—a desired state for firmware versions—on a resource, such as a server profile, or on a group of resources, such as all of the interconnects in a logical interconnect group.
- Detect when a resource does not comply with the firmware baseline.
- Identify firmware compatibility issues.
- Update firmware for an entire enclosure in minutes.
- Update firmware for individual resources or for groups of resources, such as logical interconnect groups.¹

1.3.2 Simplified configuration change management

Templates and groups simplify the distribution of configuration changes across your data center. For example:

- If you add a network to a network set, the network is available for immediate use by all of the server profiles that have a connection to the network set. You do not need to change or reapply a server profile.
- You can reduce errors by making multiple and complex changes to a group. Then, for each member of the group, you can use a single action to update the configuration to match the configuration of the group.
- The appliance notifies you when it detects that a device does not comply with the current template or group. You control when and if a device configuration is updated.
- The firmware for physical interconnects is managed using the logical interconnects, ensuring that the member interconnects have compatible firmware.

1.4 Monitoring and response features

One user interface

You use the same interface you use to provision resources. There are no additional tools or interfaces to learn.

1. Enclosure groups do not include a firmware baseline; therefore, updates to enclosure firmware are managed on a per-enclosure basis.

Isolated management network

The appliance architecture is designed to separate the management traffic from the production network, which increases reliability of the overall solution. For example, your data center resources remain operational even in the unlikely event of an appliance outage.

Automatic configuration for monitoring

When you add resources to the appliance, they are automatically configured for monitoring, and the appliance is automatically registered to receive SNMP traps. You can monitor resources immediately without performing additional configuration or discovery steps.

Agentless and out-of-band management

All monitoring and management of HP ProLiant Gen8 (or later) servers is agentless and out-of-band for increased security and reliability. For these servers:

- There are no agents to monitor or update.
- The appliance does not require open SNMP ports on the host operating system.
- The appliance does not require an operating system on the host, which frees memory and processor resources on the host for use by server applications, and enables you to manage servers that have no host operating system installed.

Management from other platforms using the REST APIs and the SCMB

The REST APIs and the SCMB (State-Change Message Bus) also enable you to monitor the HP OneView environment from other management platforms. For more information about the SCMB, see [“Using the State-Change Message Bus \(SCMB\)” \(page 185\)](#).

Monitoring the environment and responding to issues

Features for monitoring the environment and responding to issues include the following:

- The [“Dashboard screen” \(page 176\)](#), which displays a summary view of data center capacity and health information
- The [“Activity screen” \(page 173\)](#), which displays and allows you to filter all system tasks and alerts
- [Data center environmental management \(page 22\)](#)
- [Resource utilization monitoring \(page 22\)](#)
- [Alert and health management \(page 22\)](#)
- [Hardware and firmware inventory information \(page 23\)](#)

1.4.1 Data center environmental management

HP OneView integrates these critical areas for environmental management of the data center:

- Thermal data visualization in 3D
- Power delivery infrastructure representation
- Physical asset location in 3D

Feature	Description
Thermal data visualization	3D data center thermal mapping provides a view of the thermal status of your entire data center. The appliance collects thermal data from the managed resources in each data center rack and presents the data graphically, enabling easy identification of hot spots in a rack.
Power delivery infrastructure representation	<p>HP OneView collects and reports processor utilization and power and temperature history for your data center hardware. The appliance monitors power, automatically detects and reports power delivery errors, and provides precise power requirement information for HP ProLiant Gen8 servers and HP BladeSystem enclosures that you can use for planning rack and power usage.</p> <p>Power Discovery Services enable automatic discovery and visualization of the power delivery topology for your data center. HP iPDUs enable the appliance to map the rack power topology automatically. The appliance detects wiring errors—such as lack of redundancy—and updates electrical inventory automatically when new servers are installed. The appliance also supports per-outlet power control for remote power cycling of each iPDU outlet.</p> <p>You can manually define the power requirements and power topology for devices that do not support Power Discovery Services.</p>
Physical asset location	<p>Location Discovery Services enable the appliance to automatically display the exact 3D location of HP ProLiant Gen8 servers in HP Intelligent Series Racks, reducing labor time, lowering operational costs, and eliminating human errors associated with inventory and asset management.</p> <p>You can manually define the positions of racks and devices that do not support Location Discovery Services.</p>

1.4.2 Resource utilization monitoring

HP OneView periodically collects and maintains CPU utilization information for all of the servers it manages. HP OneView also collects port-level statistics for networking, including transmit, receive, and error counters. HP OneView displays all of this data using rich UIs and makes the data available through the REST APIs.

1.4.3 Alert and health management

HP OneView provides streamlined activity monitoring and management. The appliance automatically registers to receive SNMP traps from all managed resources, and resources added to the appliance are immediately available for monitoring and management. When the appliance notifies you of a problem, when possible, it suggests a way to correct the problem.

Using the UI and REST APIs, you can:

- View all activities (alerts and tasks) by description or source, and filter activities using multiple filter criteria.
- Assign alerts to specific users.
- Annotate activities with notes from administrators, enabling the administrators of the data center to collaborate through the appliance instead of through outside tools such as email.

- View alerts for a specific resource from the UI screen for that resource or using the REST API for that resource.
- Automatically forward SNMP traps from managed resources to enterprise monitoring consoles or centralized SNMP trap collectors.

1.4.4 Hardware and firmware inventory information

HP OneView provides detailed hardware and firmware inventory information about the resources it manages. You can access the following data through the UI and the REST APIs:

- Summary and detailed views of managed hardware, such as servers, enclosures, and interconnects.
- Summary and detailed views of firmware bundle contents.

You can use the Smart Search feature of the UI to find specific items in the inventory.

1.5 Backup and restore features

HP OneView provides services to back up an appliance to a backup file, and to restore an appliance from a backup file.

One encrypted backup file for both the appliance and its database

Backup files are encrypted and contain configuration settings and management data—there is no need to create separate backup files for the appliance and its database.

Flexible scheduling and an open interface for backup operations

You can create backup files while the appliance is online. Also, you can use REST APIs to:

- Schedule a backup process from outside the appliance.
- Collect backup files according to your site policies.
- Integrate with enterprise backup and restore products.

A backup file is a snapshot of the appliance configuration and management data at the time the backup file was created. HP recommends that you create regular backups, preferably once a day and after you make hardware or software configuration changes in the managed environment.

Specialized user role for creating backup files

HP OneView provides a user role specifically for backing up the appliance by permitting access to other resource views without permitting actions on those resources, or other tasks.

Recovery from catastrophic failures

You can recover from a catastrophic failure by restoring your appliance from the backup file.

When you restore an appliance from a backup file, all management data and most configuration settings on the appliance are replaced with the data and settings in the backup file, including things like user names and passwords, audit logs, and available networks.

The state of the managed environment is likely to be different from the state of that environment at the time the backup file was created. During a restore operation, the appliance reconciles the data in the backup file with the current state of the managed environment. After the restore operation, the appliance uses alerts to report any discrepancies that it cannot resolve automatically.

For more information about backing up and restoring an appliance, see [“Backing up an appliance” \(page 149\)](#).

1.6 Security features

CATA (Comprehensive Applications Threat Analysis) is a powerful HP security quality assessment tool designed to substantially reduce the number of latent security defects. The design of the HP OneView appliance employed CATA fundamentals and underwent CATA review. To ensure a secure platform for data center management, the appliance includes features such as the following:

- Separation of the data and management environments, which is critical to avoid takeover in DoS (Denial of Service) attacks. For example, the appliance is designed to operate entirely on an isolated management LAN; access to the production LAN is not required. The managed devices remain online in the event of an appliance outage.
- RBAC (role-based access control), which enables an administrator to quickly establish authentication and authorization for users based on their responsibilities for specific resources. RBAC also simplifies what is shown in the UI:
 - Users can view only the resources for which they are authorized. For example, the appliance does not display screens that do not apply to users with the role of Network administrator, such as the **Server Profiles** and **Server Hardware** screens.
 - Users can initiate actions only for the resources for which they are authorized. For example, users with the role of Network administrator can initiate actions for the network resources only, and users with the role of Server administrator can initiate actions for the server resources only.
 - Users with the role of Infrastructure administrator have full access to all screens and actions.
- Single sign-on to iLO and Onboard Administrator without storing user-created iLO or Onboard Administrator credentials.
- Audit logging for all user actions.
- Support for authentication and authorization using an optional directory service such as Microsoft Active Directory.
- Use of certificates for authentication over SSL (Secure Sockets Layer).
- A firewall that allows traffic on specific ports and blocks all unused ports.
- A UI that restricts access from host operating system users.
- Data downloads that are restricted to support dump files (encrypted by default), encrypted backup files, audit logs, and certificates.

For detailed security information, see [“Understanding the security features of the appliance” \(page 45\)](#).

1.7 Availability features

HP OneView separates the management appliance from the managed resources. In the unlikely event that the appliance experiences an outage, the managed resources continue to run.

HP OneView is delivered as a virtual appliance running in a VMware vSphere virtual machine. The VMware vSphere Hypervisor provides the virtual machine with high-availability and recovery capabilities that allow the virtual machine to be restarted on another host in the cluster and to resume management without disruption to the managed resources.

Configuring the appliance for availability is described in [“Managing appliance availability” \(page 153\)](#).

1.8 Graphical and programmatic interfaces

The HP OneView appliance was developed to use a single, consistent resource model embodied in a fast, modern, and scalable HTML5 user interface and industry-standard REST APIs for mobile, secure access and open integration with other management software.

User interface—efficiency and simplicity by design

The UI is designed for the way you work, providing powerful, easy-to use tools, including the following:

Feature	Description
Dashboard screen	Provides a graphical representation of the general health and capacity of the resources in your data center. From the Dashboard you can immediately see the areas that need your attention
Map view	Available from each resource, the Map view enables you to examine the configuration and understand the relationships between logical and physical resources in your data center.
Smart Search box	The banner of every screen includes the Smart Search feature, which enables you to find resource-specific information such as specific instances of resource names, serial numbers, WWNs, and IP and MAC addresses.
Activity feed	The Activity feed gives you a unique perspective into the health of your environment by interleaving the tasks, alerts, and administrator's notes into a single view. The Activity feed simplifies the correlation of user activity with system health, allowing for timely resolution of issues.
Resource-specific management screens	These screens enable you to focus on the resources you are authorized to view and manage. Resource group screens enhance scalability by enabling you to manage multiple resources as one

The UI provides on-screen hints and tips to help you avoid and correct errors, and provides links to learn more about the tasks. At the top of each screen, the help icon gives you access to the entire help system.

For more information about the UI, see [“Navigating the graphical user interface” \(page 57\)](#).

REST APIs—automation and integration

HP OneView has a resource-oriented architecture that provides a uniform REST interface.

The REST APIs:

- Provide an industry-standard interface for open integration with other management platforms.
- Are designed to be ubiquitous—every resource has one URI (Uniform Resource Identifier) and represents a physical device or logical construct.
- Enable you to automate anything you can do from the UI using your favorite scripting or programming language.
- Are designed to be highly scalable.

For more information about the REST APIs, see the REST API scripting chapters in the online help.

For more information about finding online help and other documentation for the appliance, see [“Accessing documentation and help” \(page 75\)](#).

1.9 Integration with other HP management software

Onboard Administrator

HP OneView interacts seamlessly with the Onboard Administrator to provide complete management of HP BladeSystem c7000 enclosures. A user's Onboard Administrator privileges are determined by the role assigned to the user's HP OneView appliance account.

HP Integrated Lights-Out

HP OneView interacts seamlessly with the iLO management processor to provide complete management of HP servers. HP OneView automatically configures the iLO according to the settings specified by the server profile. HP OneView configures seamless access to the iLO graphical remote console, enabling you to launch the iLO remote console from the HP OneView UI in a single click. Your iLO privileges are determined by the role assigned to your HP OneView appliance account.

HP Insight Control server provisioning

HP OneView server profiles enable you to configure servers for PXE boot. Insight Control server provisioning, an optional product, can then install an operating system on the server using either scripted installation or captured image deployment.

1.10 Open integration

The single, consistent resource model, REST APIs, and SCMB enable you to use scripting to integrate HP OneView with other enterprise applications to address user needs and perform tasks such as:

- Automating standard workflows and troubleshooting steps
- Automating integrations with other software, such as a CMDB (content management database)
- Connecting to service desks
- Monitoring resources, collecting data, and mapping and modeling systems
- Exporting data to formats that suit your needs
- Attaching custom databases, data warehouses, or third-party business intelligence tools
- Integrating in-house user customizations

The SCMB is an interface that uses asynchronous messaging to notify subscribers of changes to managed resources—both logical and physical. For example, you can program applications to receive notifications when new server hardware is added to the managed environment or when the health status of physical resources changes—without having to continuously poll the appliance for status using the REST APIs.

For more information about the SCMB, see [“Using the State-Change Message Bus \(SCMB\)” \(page 185\)](#).

1.11 Convenient licensing model

HP OneView provides a convenient and flexible licensing model:

- Purchasing HP OneView integrated with your hardware provides the best experience—a fully automatic approach to license redemption and registration. Your software license for HP OneView and iLO Advanced is delivered embedded in the hardware you purchase, including these options:
 - A license bundle for 16 servers embedded in the enclosure Onboard Administrator
 - A license for a single server embedded in the server iLO

When you add hardware with an embedded license to the appliance, the appliance automatically applies the license. Your software license is also automatically registered for support when the hardware is registered.

- You can also purchase and activate licenses separately, enabling you to add licenses for existing hardware.
- If you already have an iLO Advanced license for a server, you can purchase an HP OneView license that does not include the iLO Advanced license.

The appliance stores licenses in a pool and applies licenses to server hardware as needed. You can view information about the number of licenses available, the number of licensed servers, and the number of servers that require a license.

1.12 Networking features

The HP OneView appliance provides several networking features to streamline the provisioning of networking resources for server blades and to manage configuration changes, including firmware updates, to Virtual Connect interconnect modules.

Supported networks

The Virtual Connect interconnect modules in enclosures support the following types of data center networks:

- Ethernet for data networks
- Fibre Channel for storage networks, including Fibre Channel Fabric attach (SAN switch) connections, and Fibre Channel Direct attach (Flat SAN) connections to supported HP 3PAR storage systems.

Logical interconnects

The appliance enables you to define multiple enclosure interconnect modules as a single administrative entity called a [logical interconnect](#), which provides universal access to data center Ethernet networks from all servers connected to any member interconnect. A logical interconnect is the set of physical interconnects and their links, including the following:

- Uplinks to data center networks as mapped by their uplink sets
- Downlinks to the servers
- Stacking links (connections to each other)

Logical interconnect groups

A [logical interconnect group](#) is a collection of logical interconnects that have the same configuration for features such as the following:

- Stacking domain
- Firmware
- Uplink sets
- Uplink port redundancy and fault tolerance

When you add an enclosure and associate it with an enclosure group, the enclosure is automatically configured according to the logical interconnect group associated with the enclosure group. This feature enables you to provision hundreds of enclosures consistently and efficiently.

After you create a logical interconnect, it continues to be associated with the logical interconnect group and reports if its configuration differs from the group.

Network sets

You can define a collection of Ethernet data center networks to be identified by a single name, called a [network set](#). You can specify a network set instead of an individual network when you define a [connection](#) from a server to the data center networks. By using network sets, you can make changes to networks that are members of a network set without having to make changes to each server profile that uses that network set.

Network sets are useful in virtual machine environments where each server profile connection must access multiple networks. For example, you can configure a hypervisor with a vSwitch to access multiple network VLAN IDs by creating a network set as a trunk that includes the networks that have these VLAN IDs.

For more information about networking resources, see [“Understanding the resource model” \(page 29\)](#).

For detailed information about the networking model for the HP OneView appliance, see [“About network connectivity” \(page 116\)](#).

2 Understanding the resource model

The HP OneView appliance uses a resource model that reduces complexity and simplifies the management of your data center. This model provides logical resources, including templates, groups, and sets, that when applied to physical resources, provides a common structure across your data center.

High level overview

- Resource model summary diagram (page 29)

Server resources

- Server profiles (page 30)
- Connections (page 31)
- Connection templates (page 30)
- Server hardware (page 32)
- Server hardware types (page 31)

Network provisioning resources

- Enclosure groups (page 33)
- Enclosure types (page 33)
- Enclosures (page 34)
- Interconnect types (page 34)
- Interconnects (page 35)
- Logical interconnect groups (page 36)
- Logical interconnects (page 37)
- Uplink sets (page 38)

Network resources

- Networks (page 39)
- Network sets (page 39)

Appliance resources

- Appliance (page 40)
- Domains (page 40)

Data center power and cooling management resources

- Data centers (page 41)
- Racks (page 41)
- Power delivery devices (page 42)
- Unmanaged devices (page 42)

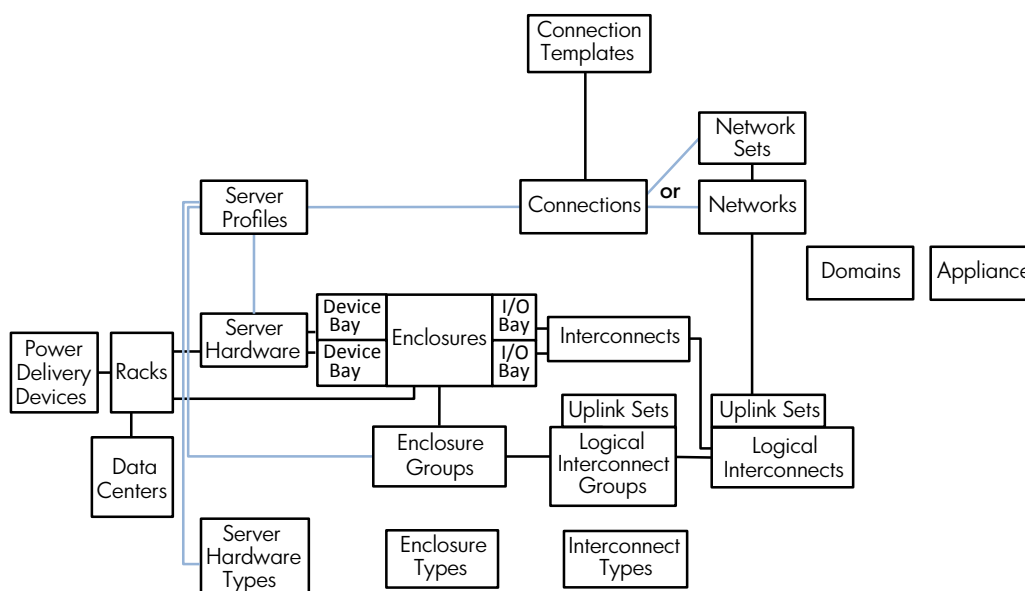
Learn more

- For a complete list of resources, see the *HP OneView REST API Reference* in the online help.
- For information about using this appliance, see the other chapters in this guide and the online help.

2.1 Resource model summary diagram

The following figure summarizes some of the most frequently used resources and shows the relationships between them.

Figure 1 Resource model summary diagram



The UI and REST APIs are organized by resource. The documentation for the UI and REST APIs are also organized by resource.

To view the complete list of resources, see the *HP OneView REST API Reference* in the online help.

The following sections introduce the resources shown in [Figure 1 \(page 29\)](#).

2.2 Server profiles

Server profiles capture key aspects of the server configuration in one place, enabling you to provision converged infrastructure hardware quickly and consistently according to your best practices.

A server profile can contain the following configuration information about the server hardware:

- Basic server identification information
- Connections to Ethernet networks, Ethernet network sets, and Fibre Channel networks
- Firmware versions
- BIOS settings
- Boot order
- Physical or virtual UUIDs (universally unique identifiers), MAC (media access control) addresses and WWN (World Wide Name) addresses

Relationship to other resources

A server profile is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [connection](#) resources. You use a connection resource to specify connection from the server to a network or network set. If you do not specify at least one connection, the server cannot connect to data center networks. The networks and network sets that are available to a server profile connection depend on the configuration of the logical interconnect of the enclosure that contains the server hardware.
- Exactly one [server hardware](#) resource, which can be either `unassigned` or can be located in a specific enclosure and enclosure bay.
- Exactly one [server hardware type](#) resource.
- Exactly one [enclosure group](#) resource.

To enable portability of server profiles, a server profile is associated with an enclosure group resource instead of an enclosure resource. Because enclosures in the enclosure group are configured identically, you can assign a server profile to any appropriate server hardware, regardless of which enclosure and bay in the enclosure group contains that server hardware.

UI screens and REST API resources

UI screen	REST API resource
Server Profiles	server-profiles

For more information about server profiles, see the online help for the **Server Profiles** screen.

2.3 Connection templates

A connection template defines default configuration characteristics, such as the preferred bandwidth and maximum bandwidth, for a network or network set. When you create a network or network set, the appliance creates a default connection template for the network or network set.

Relationship to other resources

A connection template resource is associated with zero or more [connection](#) resources. A connection resource is associated with the appropriate connection template for a type of network or network set.

UI screens and REST API resources

UI screen	REST API resource	Notes
None	connection-templates	The UI does not display or refer to connection templates, but connection templates determine the default values displayed for the connection when you select a network or network set.

2.4 Connections

A connection is the logical representation of a connection between a server and a network or network set. Connections are part of server profiles. A connection specifies the following:

- The network or network set to which the server is to be connected
- Configuration overrides (such as a change to the preferred bandwidth) to be made to the default configuration for the specified network or network set
- Boot order

Relationship to other resources

A connection resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Exactly one [server profile](#) resource.
- Exactly one [connection template](#) resource.
- Exactly one [network](#) or [network set](#) resource. The resources that are available to the connection depend on the configuration of the logical interconnect of the enclosure that contains the server hardware.

UI screens and REST API resources

UI screen	REST API resources
Server Profiles	connections and server-profiles

For more information about connections, see the online help for the **Server Profiles** screen.

2.5 Server hardware types

A server hardware type captures details about the physical configuration of server hardware, and defines which settings are available to the server profiles assigned to that type of server hardware. For example, the server hardware type for the HP ProLiant BL460c Gen8 Server Blade includes a complete set of default BIOS settings for that server blade hardware configuration.

When you add an enclosure to the appliance, the appliance detects the servers installed in the enclosure and creates a server hardware type for each unique server configuration it discovers. When you add a unique rack mount server model, the appliance creates a new server hardware type for that server configuration.

Relationship to other resources

A server hardware type resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [server profiles](#)
- Zero or more servers of the type defined by that server hardware type

UI screens and REST API resources

UI screen	REST API resource
Server Hardware Types	server-hardware-types

For more information about server hardware types, see the online help for the **Server Hardware Types** screen.

2.6 Server hardware

Server hardware represents an instance of server hardware, such as a physical HP ProLiant BL460c Gen8 Server Blade installed in an enclosure, or a physical HP ProLiant DL380p rack server.

For information about the supported server hardware, see the *HP OneView Support Matrix*.

Relationship to other resources

A server hardware resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or one [server profile](#). If a server does not have a server profile assigned, you cannot perform actions that require the server profile resource, such as managing firmware or connecting to data center networks. However, you can:
 - Add the server hardware to the appliance, including automatically updating the server firmware to the minimum version required for management by the appliance.
 - View inventory data.
 - Power on or power off the server.
 - Launch the iLO remote console.
 - Monitor power, cooling, and utilization.
 - Monitor health and alerts.
- If the server hardware is a server blade, exactly one device bay of an [enclosure](#). This association also applies to full-height server blades, which occupy two device bays but are associated with the top bay only.
- If the server hardware is a rack mount server, zero or one [rack](#) resource and zero or more [power delivery devices](#).
- If the appliance discovers an instance of supported server hardware for which it does not have a matching [server hardware type](#), the appliance creates a server hardware type for that server hardware configuration.

UI screens and REST API resources

UI screen	REST API resource	Notes
Server Hardware	server-hardware	You use the server hardware resource, not the server profile resource, to perform actions such as powering off or powering on the server, resetting the server, and launching the HP iLO remote console. You can launch the HP iLO remote console through the UI only. The REST APIs do not include an API to launch the HP iLO remote console.

For more information about server hardware, see the online help for the **Server Hardware** screen.

2.7 Enclosure groups

An enclosure group is a logical resource that defines a set of enclosures that use the same configuration for network connectivity. The same logical interconnect group is used for every enclosure that is a member of the enclosure group, resulting in identically configured enclosures and uplinks to data center networks.

By creating enclosure groups and adding enclosures to the group, you can quickly add and manage many identically configured enclosures.

Relationship to other resources

An enclosure group resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [enclosures](#)
- Zero or more [server profiles](#)
- Exactly one [logical interconnect group](#)

UI screens and REST API resources

UI screen	REST API resource
Enclosure Groups	enclosure-groups

For more information about enclosure groups, see the online help for the **Enclosure Groups** screen.

2.8 Enclosure types

An enclosure type defines characteristics of a specific HP enclosure hardware model, such as an HP BladeSystem c7000 Enclosure.

Relationship to other resources

An enclosure type resource is associated with zero or more [enclosures](#).

UI screens and REST API resources

UI screen	REST API resource	Notes
None	None	The UI does not refer to enclosure type, but the enclosure type is used by the appliance when you add an enclosure. The enclosures REST resource includes an enclosureType attribute.

2.9 Enclosures

An enclosure is a physical structure that contains server blades, the Onboard Administrator, and interconnects.

For information about the supported enclosure models, see the *HP OneView Support Matrix*.

The enclosure provides the hardware connections between the interconnect downlinks and the installed server blades.

The enclosure interconnects provide the physical uplinks to the data center networks.

When you add an enclosure, the appliance discovers and adds all of the components within the enclosure, including any installed server blades and any installed interconnects.

Relationship to other resources

An enclosure resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Exactly one [enclosure group](#)
- Zero or more physical [interconnects](#)
- One [logical interconnect](#) and one [logical interconnect group](#) (through the enclosure's association with enclosure groups and interconnects)
- Zero or one [rack](#) resource
- Zero or more [power delivery devices](#)

UI screens and REST API resources

UI screen	REST API resource
Enclosures	enclosures

For more information about enclosures, see the online help for the **Enclosures** screen.

2.10 Interconnect types

The interconnect type resource defines the characteristics of a model of interconnect, such as the following:

- Downlink capabilities and the number of downlink ports
- Uplink port capabilities and the number of uplink ports
- Supported firmware versions

Relationship to other resources

An interconnect type resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [interconnects](#)

UI screens and REST API resources

UI screen	REST API resource	Notes
Interconnects	<code>interconnect-types</code>	The UI does not display or refer to the interconnect type resource specifically, but the information is used by the appliance when you add or manage an interconnect using the Interconnects screen.

2.11 Interconnects

An interconnect is a physical resource that enables communication between hardware in the enclosure and the data center Ethernet LANs and Fibre Channel SANs. The HP Virtual Connect FlexFabric 10Gb/24-port Module is an example of a supported interconnect. For a list of supported interconnects, see the *HP OneView Support Matrix*.

An interconnect has the following types of ports:

Port type	Description
Uplinks	Uplinks are physical ports that connect the interconnect to the data center networks. For example, the X2 port of an HP Virtual Connect FlexFabric 10Gb/24-port Module is an uplink.
Downlinks	Downlinks are physical ports that connect the interconnect to the server hardware through the enclosure midplane.
Stacking links	Stacking links are internal or external physical ports that join interconnects to provide redundant paths for Ethernet traffic from servers to the data center networks.

In the resource model:

- Interconnects are an integral part of enclosures and enclosure groups. The interconnects installed in an enclosure are added automatically when the enclosure is added to the appliance. To remove an interconnect from the appliance, you must remove the enclosure from the appliance.
- Interconnects can also be defined by a logical interconnect group, which in turn defines the logical interconnect configuration to be used for an enclosure. When you associate an enclosure with an enclosure group during an add operation, the appliance uses the interconnect configuration defined by the logical interconnect group that is associated with the enclosure group. The physical interconnect configuration in the enclosure must match the logical interconnect group configuration before an interconnect can be managed.
- An interconnect must be a member of a logical interconnect. For an interconnect to be usable, it must be installed in an enclosure and must be defined as part of a logical interconnect. Each physical interconnect can contribute physical uplink ports to an uplink set.
- Firmware baselines and firmware updates for physical interconnects are managed by the logical interconnect.

Relationship to other resources

An interconnect resource is associated with the following resources in the [resource summary diagram](#) (page 29):

- Exactly one [enclosure](#)
- Exactly one [logical interconnect](#), and, through that logical interconnect, exactly one [logical interconnect group](#)

UI screens and REST API resources

UI screen	REST API resources
Interconnects	interconnects, interconnect-types, and logical-interconnects

For more information about interconnects, see the online help for the **Interconnects** screen.

2.12 Logical interconnect groups

The logical interconnect group represents the physical and logical configuration of connections to data center networks for each logical interconnect in the group. This configuration includes the following:

- The interconnect types, interconnect configurations, and interconnect downlink capabilities
- The stacking mode, which reserves the interconnect ports to be used for stacking links
- The uplink sets, which map uplink ports to Ethernet or Fibre Channel networks
- The available networks

In the resource model:

- A logical interconnect group is associated with an enclosure group instead of an individual enclosure.
- Every enclosure that is a member of an enclosure group has the same network connectivity as all other enclosures in the enclosure group because their logical interconnects are identically configured.
- You can create a logical interconnect group either automatically during an enclosure add operation, or independently of enclosure add operations. If you add an enclosure without specifying an existing enclosure group, the appliance creates both an enclosure group and a logical interconnect group based on the physical interconnects in that enclosure. You can then edit that enclosure group and that logical interconnect group.
- The uplink sets defined by the logical interconnect group establish the initial configuration of the uplink sets of each logical interconnect associated with the logical interconnect group. If you change uplink sets for an existing logical interconnect group:
 - The updated uplink sets are applied to any new logical interconnects that are added to the existing logical interconnect group.
 - Existing logical interconnects are reported as not being consistent with the logical interconnect group. You can then request that those existing logical interconnects be updated with the new configuration.

After a logical interconnect has been created and associated with a logical interconnect group, it continues to be associated with that group and reports if its configuration differs from the group. You can then change the configuration of the logical interconnect to match the group.

Relationship to other resources

A logical interconnect group resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [logical interconnects](#)
- Zero or more [enclosure groups](#)

The uplink sets defined by a logical interconnect group specify the initial configuration of the [uplink sets](#) of each logical interconnect in the group.

UI screens and REST API resources

UI screen	REST API resource
Logical Interconnect Groups	logical-interconnect-groups

For more information about logical interconnect groups, see the online help for the **Logical Interconnect Groups** screen.

2.13 Logical interconnects

A logical interconnect is a single entity for multiple physical interconnects

A logical interconnect is a single administrative entity that consists of the configuration of the interconnects in an enclosure. This configuration includes:

- Interconnects, which are required for the enclosure to connect to data center networks.
- Uplink sets, which map data center networks to physical uplink ports. If no uplink sets are defined, the logical interconnect cannot connect to data center networks, and the servers attached to the downlinks of the logical interconnect cannot connect to data center networks.
- Downlink ports, which connect through the enclosure midplane to the servers in the enclosure. A logical interconnect includes all of the physical downlinks of all of the member interconnects. The downlinks connect the interconnects to physical servers. The set of downlinks that share access to a common set of networks are called logical downlinks.
- Stacking links, which join interconnects either through connections inside the enclosure or external cables between the stacking ports of the interconnects.
- The firmware baseline, which specifies the firmware version to be used by all of the member interconnects. The firmware baseline for physical interconnects is managed by the logical interconnect.

The network administrator configures multiple paths from server bays to networks

The network administrator can ensure that every server bay of an enclosure has two independent paths to an Ethernet data center network by creating a logical interconnect for which the following conditions are true:

- The logical interconnect has at least two interconnects that are joined by stacking links.
- The logical interconnect has at least one uplink set that includes uplinks to the network from at least two physical interconnects.

The appliance detects and reports a configuration or state in which there is only one path (no redundant paths) to a network or in which there are no paths to a network.

The server administrator is not required to know the details about interconnect configurations

Because a logical interconnect is managed as a single entity, the server administrator is isolated from the details of interconnect configurations. For example, if the network administrator configures the logical interconnect to ensure redundant access from each server bay in the enclosure to each Ethernet data center network, the server administrator must only ensure that a server profile includes two connections to a network or to a network set that includes that network.

Relationship to other resources

A logical interconnect resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [interconnects](#). For a logical interconnect to be usable, it must include at least one interconnect. If there are zero interconnects, the enclosure and its contents do not have any uplinks to the data center networks.
- Exactly one [logical interconnect group](#), which defines the initial configuration of the logical interconnect, including its uplink sets. Using logical interconnect groups, you can easily and quickly replicate the same logical interconnect configuration across multiple enclosures. After a logical interconnect is created and associated with a logical interconnect group, it continues to be associated with that group and reports if its configuration differs from the configuration of the group. This feature enables you to manage any number of logical interconnects as though they were one by making all the configuration changes to the logical interconnect group, and then, for each logical interconnect, using a single action to update the configuration from the group.
- Zero or more [uplink sets](#), which associate zero or more uplink ports and zero or more [networks](#).

UI screens and REST API resources

UI screen	REST API resource	Notes
Logical Interconnects	logical-interconnects and logical-downlinks	You use the logical-downlinks REST API to obtain information about the common set of networks and capabilities available to a downlink.

For more information about logical interconnects, see the online help for the **Logical Interconnects** screen.

2.14 Uplink sets

An uplink set assigns data center networks to uplink ports of interconnects. The uplinks must be from physical interconnects that are members of the logical interconnect to which the uplink set belongs. An uplink set is part of a logical interconnect. For each logical interconnect:

- An uplink set cannot include a network set.
- A network can be a member of one uplink set only.
- An uplink set can contain only one Fibre Channel network.
- An uplink set can contain multiple Ethernet networks.
- You cannot assign two instances of the same network to the same physical port.

Relationship to other resources

An uplink set is part of a [logical interconnect](#) or a [logical interconnect group](#).

The uplink sets defined by a [logical interconnect group](#) specify the configuration for uplink sets used by logical interconnects that are members of the group. If the uplink sets of a logical interconnect do not match the uplink sets of the logical interconnect group, the appliance notifies you that the logical interconnect is not consistent with its group.

UI screens and REST API resources

UI screen	REST API resource
Logical Interconnects or Logical Interconnect Groups	uplink-sets

For more information about uplink sets, see the online help for the **Logical Interconnects** and **Logical Interconnect Groups** screens.

2.15 Networks

A network represents a Fibre Channel or Ethernet network in the data center.

Relationship to other resources

A network resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [connections](#)
- Zero or one [uplink set](#) per [logical interconnect](#)
- For Ethernet networks only, zero or more [network sets](#)

UI screens and REST API resources

UI screen	REST API resource
Networks	fc-networks or ethernet-networks

For more information about networks, see the online help for the **Networks** screen.

2.16 Network sets

A network set represents a group of Ethernet networks identified by a single name. Network sets are used to simplify server profile configuration. When a connection in a server profile specifies a network set, it can access any of the member networks. Additionally, if networks is added to or deleted from a network set, server profiles that specify the network set are isolated from the change. One common use for network sets is as a trunk for multiple VLANs to a vSwitch.

In the resource model:

- A network set can contain zero or more Ethernet networks.
- An Ethernet network can be a member of zero or more network sets.
- A connection in a server profile can specify either a network or a network set.
- A network set cannot be a member of an uplink set.

Other configuration rules apply. For more information about network sets, including specifying the network to handle untagged traffic, see [“About network sets” \(page 119\)](#).

Relationship to other resources

A network set resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [connections](#), and, through those connections, zero or more [server profiles](#)
- Zero or more Ethernet [networks](#)

UI screens and REST API resources

UI screen	REST API resource
Network Sets	network-sets

For more information about network sets, see the online help for the **Network Sets** screen.

2.17 Domains

The domain resource describes the management domain for the appliance. All resources managed by the appliance are part of a single management domain.

Relationship to other resources

A domain resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Exactly one [appliance](#)
- Zero or more instances of the other resources in the [summary diagram \(page 29\)](#)

UI screens and REST API resources

UI screen	REST API resource	Notes
None	domains	The UI does not display or refer to domains, but the domain resource provides information about limits such as the total number of networks that you can add to the appliance. You can use the <code>domains</code> REST API to obtain information about the domain.

2.18 Appliance

The appliance resource defines configuration details specific to the appliance (as distinct from the resources the appliance manages).

Relationship to other resources

An appliance resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Exactly one [domain](#)
- Zero or more instances of the other resources in the [summary diagram \(page 29\)](#)

UI screens and REST API resources

UI screen	REST API resource
Settings	Several REST API resources are related to the appliance and appliance settings. See the resources in the following categories in the <i>HP OneView REST API Reference</i> in the online help: <ul style="list-style-type: none">• Settings• Security

For more information about various appliance configuration settings see the online help for the **Settings** screen.

2.19 Resources related data center facilities

2.19.1 Data centers

In the appliance, a data center represents a physically contiguous area in which racks containing IT equipment—such as servers, enclosures, and devices—are located. You create a data center to describe a portion of a computer room that provides a useful grouping to summarize your environment and its power and thermal requirements. A data center resource is often a subset of your entire data center and can include equipment that is not managed by the appliance. By representing the physical layout of your data center equipment, including unmanaged devices, you can use detailed monitoring information provided by the appliance for space planning and determining power and cooling requirements.

In the appliance, you can:

- View a 3D model of the data center layout that includes a color-coding scheme to help you identify areas that are too hot or too cold.
- View temperature history data.
- More easily locate specific devices for hands-on servicing.

Relationship to other resources

A data center resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [racks](#)

UI screens and REST API resources

UI screen	REST API resource
Data Centers	datacenters

For more information about data centers, see the online help for the **Data Centers** screen.

2.19.2 Racks

A rack is a physical structure that contains IT equipment such as enclosures, servers, power delivery devices, and unmanaged devices in a data center. By describing the physical location, size, and thermal limit of equipment in the racks, you enable space and power planning and power analysis features for your data center.

Relationship to other resources

A rack resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or one [data centers](#)
- Zero or more [enclosures](#)
- Zero or more instances of [server hardware](#) (for HP ProLiant DL servers only)
- Zero or more [unmanaged devices](#)
- Zero or more [power delivery devices](#)

UI screens and REST API resources

UI screen	REST API resource
Racks	racks

For more information about racks, see the online help for the **Racks** screen.

2.19.3 Power delivery devices

A power delivery device is a physical resource that delivers power from the data center service entrance to the rack components. You create the power distribution device objects to describe the power source for one or more components in the rack. Power delivery devices can include power feeds, breaker panels, branch circuits, PDUs, outlet bars, outlets, and UPS devices.

For a complete list of power delivery devices, see the screen details online help for the **Power Delivery Devices** screen.

Relationship to other resources

A power delivery device resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [racks](#)
- Zero or more [unmanaged devices](#)

UI screens and REST API resources

UI screen	REST API resource
Power Delivery Devices	power-devices

For more information about power delivery devices, see the online help for the **Power Delivery Devices** screen.

2.19.4 Unmanaged devices

An unmanaged device is a physical resource that is located in a rack or consumes power but is not currently managed by the appliance. Some unmanaged devices are unsupported devices that cannot be managed by the appliance.

By adding unmanaged devices to racks, you can obtain a more complete analysis of space, power, and cooling in the data center, and you can use the appliance to view hardware inventory information about these devices.

All devices connected to an HP Intelligent Power Distribution Unit (iPDU) using an HP Intelligent Power Discovery (IPD) connection are added to the appliance as unmanaged devices:

- If a device is supported for management by the appliance, you can add that device to the appliance.
- If a device is not supported for management by the appliance, you can include that device in power, cooling, and space planning by leaving it in the list of unsupported devices.

Other devices that do not support IPD—such as KVM switches, routers, in-rack monitors and keyboards—are not added to the list of unmanaged devices automatically. To include these devices in the appliance, you can add them manually and describe their names, rack positions, and power requirements.

Relationship to other resources

An unmanaged device resource is associated with the following resources in the [resource summary diagram \(page 29\)](#):

- Zero or more [racks](#)
- Zero or more [power delivery devices](#)

UI screens and REST API resources

UI screen	REST API resource	Notes
Unmanaged Devices	unmanaged-devices	You can view, add, or edit the properties of unmanaged devices using either the UI or the REST APIs. To delete an unmanaged device, you must use the REST APIs.

For more information about unmanaged devices, see the online help for the **Unmanaged Devices** screen.

3 Understanding the security features of the appliance

Most security policies and practices used in a traditional environment are applicable in a virtualized environment. However, in a virtualized environment, these policies might require modifications and additions.

3.1 Securing the appliance

CATA (Comprehensive Applications Threat Analysis) is a powerful HP security quality assessment tool designed to substantially reduce the number of latent security defects. The design of the appliance employed CATA fundamentals and underwent CATA review.

The following factors secured (hardened) the appliance and its operating system:

- Best practice operating system security guidelines were followed.
The appliance operating system minimizes its vulnerability by running only the services required to provide functionality. The appliance operating system enforces mandatory access controls internally.
 - The appliance maintains a firewall that allows traffic on specific ports and blocks all unused ports. See [“Ports needed for HP OneView” \(page 53\)](#) for the list of network ports used.
 - Key appliance services run only with the required privileges; they do *not* run as privileged users.
 - The operating system bootloader is password protected. The appliance cannot be compromised by someone attempting to boot in single-user mode.
- The appliance is designed to operate entirely on an isolated management LAN. Access to the production LAN is not required.
- The appliance enforces a password change at first login. The default password *cannot* be used again.
- The appliance supports self-signed certificates and certificates issued by a certificate authority. The appliance is initially configured with a self-signed certificate. As the Infrastructure administrator, you can generate a CSR (certificate signing request) and, upon receipt, upload the certificate to the appliance. This ensures the integrity and authenticity of your HTTPS connection to the appliance.
- All browser operations and REST API calls use HTTPS. All weak SSL (Secure Sockets Layer) ciphers are disabled.
- The appliance supports secure updating. HP digitally signs all updates to ensure integrity and authenticity.
- Backup files and transaction logs are encrypted.
- Support dumps are encrypted by default, but you have the option to not encrypt them.

- Operating-system-level users are not allowed to access the appliance, with the following exceptions:
 - A special `pwreset` command used only if the Infrastructure administrator password is lost or forgotten. This command requires that you contact your authorized support representative to obtain a one-time password. For more information, see the online help.
 - A setting that enables an authorized support representative to obtain a one-time password so that they can log in to the appliance console (and only the console) to perform advanced diagnostics.
You can either enable or disable access with this setting.
- HP closely monitors security bulletins for threats to appliance software components and, if necessary, issues software updates.

3.2 Best practices for maintaining a secure appliance

The following is a partial list of security best practices that HP recommends in both physical and virtual environments. Differing security policies and implementation practices make it difficult to provide a complete and definitive list.

- HP recommends a strict separation of the management LAN and production LAN, using VLAN or firewall technology (or both) to maintain the separation:
 - Management LAN
All management processor devices (including Onboard Administrators and virtual connections through an Onboard Administrator, iLOs, and iPDUs) are connected to the management LAN.
Grant management LAN access to authorized personnel only: Infrastructure administrators, Network administrators, and Server administrators.
 - Production LAN
All NICs for managed devices are on the production LAN.
- The appliance is preconfigured so that nonessential services are removed or disabled in its management environment. Ensure that you continue to minimize services when you configure host systems, management systems, network devices (including network ports not in use) to significantly reduce the number of ways your environment could be attacked.
- Ensure that a process is in place to determine if software and firmware updates are available, and to install updates for all components in your environment on a regular basis.
- Ensure that the security policies and processes address the virtual environment:
 - Educate administrators about changes to their roles and responsibilities in a virtual environment.
 - Restrict access to the appliance console to authorized users. For more information, see [“Restricting console access” \(page 54\)](#).
 - If you use an Intrusion Detection System (IDS) solution in your environment, ensure that the solution has visibility into network traffic in the virtual switch.
 - Turn off promiscuous mode in the hypervisor and encrypt traffic flowing over the VLAN to lessen the effect on any VLAN traffic sniffing.

NOTE: In most cases, if promiscuous mode is disabled in the hypervisor, it cannot be used on a VM (Virtual Machine) guest. The VM guest can enable promiscuous mode, but it will not be functional.

- Maintain a zone of trust, for example, a DMZ (demilitarized zone) that is separate from production machines.
- Ensure proper access controls on Fibre Channel devices.
- Use LUN masking on both storage and compute hosts.
- Ensure that LUNs are defined in the host configuration, instead of being discovered.
- Use hard zoning (which restricts communication across a fabric) based on port WWNs (Worldwide Names), if possible.
- Ensure that communication with the WWNs is enforced at the switch-port level.
- Clearly define and use administrative roles and responsibilities; for example, the Infrastructure administrator performs most administrative tasks.
- Replace self-signed certificates with your organization's CA-issued certificates. To achieve a higher level of security for components that are delivered with certificates, populate them with trusted certificates at deployment time.
- For local accounts on the appliance, change the passwords periodically according to your password policies. Follow these guidelines:
 - Limit the number of local accounts. Integrate the appliance with an enterprise directory solution such as Microsoft Active Directory or OpenLDAP.
 - Ensure that passwords include at least three of these types of characters:
 - Numeric character
 - Lowercase alphabetic character
 - Uppercase alphabetic character
 - Special character
- Do not connect management systems (for example, the appliance, the iLO card, and Onboard Administrator) directly to the Internet.
If you require access to the Internet, use a corporate VPN (virtual private network) that provides firewall protection.
- For service management, consider using the practices and procedures, such as those defined by the *Information Technology Infrastructure Library* (ITIL). For more information, see the following website:

<http://www.itil-officialsite.com/home/home.aspx>

3.3 Creating a login session

You create a login session when you log in to the appliance through the browser or some other client (for example, using the REST API). Additional requests to the appliance use the session ID, which must be protected because it represents the authenticated user.

A session remains valid until you log out or the session times out (for example, if a session is idle for a longer period of time than the session idle timeout value).

3.4 Authentication for appliance access

Access to the appliance requires authentication using a user name and password. User accounts are configured on the appliance or in an enterprise directory. All access (browser and REST APIs), including authentication, occurs over SSL to protect the credentials during transmission over the network.

3.5 Controlling access for authorized users

Access to the appliance is controlled by roles, which describe what an authenticated user is permitted to do on the appliance. Each user must be associated with at least one role.

3.5.1 Specifying user accounts and roles

User login accounts on the appliance must be assigned a role, which determines what the user has permission to do.

The appliance provides the following roles:

- The **Infrastructure administrator** has full access to view, create, edit, or remove any resources managed by the appliance, including management of the appliance itself.

The Infrastructure administrator can also manage information provided by the appliance in the form of activities, events, notifications, and logs.

All privileges are granted to this role so that the Infrastructure administrator can perform any action on the appliance, including management of deployment content (operating system build plans and scripts).

- The **Server administrator** can manage server profiles and templates, enclosures, firmware drivers, and interconnects; access the Onboard Administrator, physical servers, and vSphere vCenter registration; and view connections, networks, racks, power, activities, logs, and notifications.

The Server administrator cannot manage user accounts.

- The **Network administrator** manages networks, network sets, connections, uplinks, and firmware drivers; and views activities, logs, and notifications.

The Network administrator cannot manage user accounts.

- The **Backup administrator** role is provided for scripts using REST APIs to log in to the appliance. By using this role for backup scripts, you do not expose the Infrastructure administrator credentials for backup operations.

The Backup administrator cannot restore the appliance from a backup file.

- Users with the **Read only** role can only view appliance information, such as network settings.

For information on how to add, delete, and edit user accounts, see the online help.

3.6 Protecting credentials

Local user account passwords are stored using a salted hash; that is, they are combined with a random string, and then the combined value is stored as a hash. A hash is a one-way algorithm that maps a string to a unique value so that the original string cannot be retrieved from the hash.

Passwords are masked in the browser. When transmitted between appliance and the browser over the network, passwords are protected by SSL.

Local user account passwords must be a minimum of eight characters, with at least one uppercase character. The appliance does not enforce additional password complexity rules. Password strength and expiration are dictated by the site security policy (see [“Best practices for maintaining a secure appliance” \(page 46\)](#)). If you integrate an external authentication directory service (also known as an enterprise directory) with the appliance, the directory service enforces password strength and expiration.

3.7 Understanding the audit log

The audit log contains a record of actions performed on the appliance, which you can use for individual accountability.

Monitor the audit logs because they are rolled over periodically to prevent them from getting too large. Download the audit logs periodically to maintain a long-term audit history.

Each user has a unique logging ID per session, enabling you to follow a user's trail in the audit log. Some actions are performed by the appliance and might not have a logging ID.

A breakdown of an audit entry follows:

Token	Description
Date/time	The date and time of the event
Internal component ID	The unique identifier of an internal component
Reserved	The organization ID. Reserved for internal use
User domain	The login domain name of the user
User name/ID	The user name
Session ID	The user session ID associated with the message
Task ID	The URI of the task resource associated with the message
Client host/IP	The client (browser) IP address identifies the client machine that initiated the request
Result	<p>The result of the action, which can be one of the following values:</p> <ul style="list-style-type: none"> • SUCCESS • FAILURE • SOME_FAILURES • CANCELED • KILLED
Action	<p>A description of the action, which can be one of the following values:</p> <ul style="list-style-type: none"> • ADD • LIST • UNSETUP • CANCELED • MODIFY • ENABLE • DEPLOY • LOGIN • DELETE • DISABLE • START • LOGOUT • ACCESS • SAVE • DONE • DOWNLOAD_START • RUN • SETUP • KILLED
Severity	<p>A description of the severity of the event, which can be one of the following values, listed in descending order of importance:</p> <ul style="list-style-type: none"> • INFO • NOTICE • WARNING • ERROR • ALERT • CRITICAL
Resource category	For REST API category information, see the <i>HP OneView REST API Reference</i> in the online help.
Resource URI/name	The resource URI/name associated with the task
Message	The output message that appears in the audit log

Example 1 Sample audit entries: user login and logout

```
2013-09-16 14:55:20.706 CST,Authentication,,,administrator,jrWI9ych,,,
SUCCESS,LOGIN,INFO,CREDENTIAL,,Authentication SUCCESS
```

```
.
.
.
```

```
2013-09-16 14:58:15.201 CST,Authentication,,,MISSING_UID,jrWI9ych,,,
SUCCESS,LOGOUT,INFO,CREDENTIAL,,TERMINATING SESSION
```

3.8 Appliance access over SSL

All access to the appliance is through HTTPS (HTTP over SSL), which encrypts data over the network and helps to ensure data integrity. For a list of supported cipher suites, see [“Algorithms for securing the appliance”](#) (page 54).

3.9 Managing certificates from a browser

3.9.1 Overview

A certificate authenticates the appliance over SSL. The certificate contains a public key, and the appliance maintains the corresponding private key, which is uniquely tied to the public key.

NOTE: This section discusses certificate management from the perspective of the browser. For information on how a non-browser client (such as cURL) uses the certificate, see the documentation for that client.

The certificate also contains the name of the appliance, which the SSL client uses to identify the appliance.

The certificate has the following boxes:

- **Common Name (CN)**

This name is required. By default it contains the fully qualified host name of the appliance.

- **Alternative Name**

The name is optional, but HP recommends supplying it because it supports multiple names (including IP addresses) to minimize name-mismatch warnings from the browser.

By default, this name is populated with the fully qualified host name (if DNS is in use), a short host name, and the appliance IP address.

NOTE: If you enter **Alternative Names**, one of them must be your entry for the **Common Name**.

These names can be changed when you manually create a self-signed certificate or a certificate signing request.

3.9.2 Self-signed certificate

The default certificate generated by the appliance is self-signed; it is not issued by a trusted certificate authority.

By default, browsers do not trust self-signed certificates because they lack prior knowledge of them. The browser displays a warning dialog box; you can use it to examine the content of the self-signed certificate before accepting it.

3.9.2.1 Verifying a certificate

You can verify the authenticity of the certificate by viewing it with your browser.

After logging in to the appliance, choose **Settings**→**Security** to view the certificate. Make note of these attributes for comparison:

- Fingerprints (especially)
- Names
- Serial number
- Validity dates

Compare this information to the certificate displayed by the browser, that is, when browsing from outside the appliance.

3.9.2.2 Downloading and importing a self-signed certificate

The advantage of downloading and importing a self-signed certificate is to circumvent the browser warning.

In a secure environment, it is never appropriate to download and import a self-signed certificate, unless you have validated the certificate and know and trust the specific appliance.

In a lower security environment, it might be acceptable to download and import the appliance certificate if you know and trust the certificate originator. However, HP does not recommend this practice.

Microsoft Internet Explorer and Google Chrome share a common certificate store. A certificate downloaded with Internet Explorer can be imported with Google Chrome as well as Internet Explorer. Likewise, a certificate downloaded with Google Chrome can also be imported by both browsers. Mozilla Firefox has its own certificate store, and must be downloaded and imported with that browser only.

The procedures for downloading and importing a self-signed certificate differ with each browser.

Downloading a self-signed certificate with Microsoft Internet Explorer 9

1. Click in the **Certificate error** area.
2. Click **View certificate**.
3. Click the **Details** tab.
4. Verify the certificate.
5. Select **Copy to File...**
6. Use the Certificate Export Wizard to save the certificate as Base-64 encoded X.509 file.

Importing a self-signed certificate with Microsoft Internet Explorer 9

1. Select **Tools**→**Internet Options**.
2. Click the **Content** tab.
3. Click **Certificates**.
4. Click **Import**.
5. Use the Certificate Import Wizard.
 - a. When it prompts you for the certificate store, select **Place...**
 - b. Select the **Trusted Root Certification Authorities** store.

3.9.3 Using a certificate authority

Use a trusted CA (certificate authority) to simplify certificate trust management; the CA issues certificates that you import. If the browser is configured to trust the CA, certificates signed by the CA are also trusted. A CA can be internal (operated and maintained by your organization) or external (operated and maintained by a third-party).

You can import a certificate signed by a CA, and using it instead of the self-signed certificate. The overall steps are as follows:

1. You generate a CSR (certificate signing request).
2. You copy the CSR and submit it to the CA, as instructed by the CA.
3. The CA authenticates the requestor.
4. The CA sends the certificate to you, as stipulated by the CA.
5. You import the certificate.

For information on generating the CSR and importing the certificate, see the UI help.

3.10 Browser best practices for a secure environment

Best practice	Description
Use supported browsers	See the <i>HP OneView Support Matrix</i> to ensure that your browser and browser version are supported and the appropriate browser plug-ins and settings are configured.
Log out of the appliance before you close the browser	In the browser, a cookie stores the session ID of the authenticated user. Although the cookie is deleted when you close the browser, the session is valid on the appliance until you log out. Logging out ensures that the session on the appliance is invalidated.
Avoid linking to or from sites outside of the appliance UI	When you are logged in to the appliance, avoid clicking links to or from sites outside the appliance UI, such as links sent to you in email or instant messages. Content outside the appliance UI might contain malicious code.
Use a different browser to access sites outside the appliance	When you are logged in to the appliance, avoid browsing to other sites using the same browser instance (for example, via a separate tab in the same browser). For example, to ensure a separate browsing environment, use Firefox for the appliance UI, and use Chrome for non-appliance browsing.

3.11 Nonbrowser clients

The appliance supports an extensive number of REST APIs. Any client, not just a browser, can issue requests for REST APIs. The caller must ensure that they take appropriate security measures regarding the confidentiality of credentials, including:

- The session token, which is used for data requests
- Responses beyond the encryption of the credentials on the wire using HTTPS.

3.11.1 Passwords

Passwords are likely displayed and stored in clear text by a client like cURL. You can download cURL at the following web address:

<http://curl.haxx.se/download.html>

Take care to prevent unauthorized users from:

- Viewing displayed passwords
- Viewing session identifiers
- Having access to saved data

3.11.2 SSL connection

The client should specify HTTPS as the protocol to ensure SSL is used on the network to protect sensitive data. If the client specifies HTTP, it will be redirected to HTTPS to ensure that SSL is used.

The appliance certificate, which the client requires, allows the SSL connection to succeed. A convenient way to obtain a certificate is to use a browser pointed at the appliance; for more

information on obtaining a certificate with a browser, see [“Managing certificates from a browser”](#) (page 50)

3.12 Ports needed for HP OneView

HP OneView requires specific ports to be made available to the appliance to manage servers, enclosures, and interconnects.

Table 1 Required ports

Port number	Protocol	Usage	Description
80	TCP	Inbound	Used for HTTP interface. Typically, this port redirects to port 443; this port provides the access that iLO requires.
123	UDP	Inbound	HP OneView acts as an NTP server, both iLO and Onboard Administrator require access.
123	UDP	Outbound	The appliance uses this port as an NTP client to synchronize the appliance time.
161	UDP	Outbound	Supports SNMP GET calls to obtain status data from a server through iLO. Also used for iPDU.
162	UDP	Inbound	Used for SNMP trap support from the iLO, Onboard Administrator, and iPDU devices.
443	TCP	Inbound	Used for the HTTPS interface to user interface and APIs.
443	TCP	Outbound	Used for secure SSL access to the iLO and Onboard Administrator. Used for RIBCL, SOAP, and iPDU communication.
2162	UDP	Inbound	Used as an alternative SNMP trap port.
5671	TCP	Inbound	Used to allow external scripts or applications to connect to and monitor messages from the SCMB (State Change Message Bus).
17988	TCP	Browser to iLO	Provides browser access to the remote console.
17990	TCP	Browser to iLO	Provides remote console access to iLO virtual media.

3.13 Access to the appliance console

Restrict access to the appliance console (by using the hypervisor management software) to prevent unauthorized users from attempting to access the password reset and service access features. See [“Restricting console access”](#) (page 54).

Typical legitimate uses for access to the console are:

- Troubleshooting network configuration issues
- Resetting an appliance administrator password.
- Enabling service access by an on-site authorized support representative.

The virtual appliance console is displayed in a graphical console; password reset and HP Services access use a non-graphical console.

Switching from one console to another

1. Open the virtual appliance console from vSphere.
2. Press and hold **Ctrl+Alt**.
3. Press and release the space bar.
4. Press and release **F1** to select the non-graphical console or **F2** to select the graphical console.

3.13.1 Enabling or disabling authorized services access

When you first start up the appliance, you can choose to enable or disable access by on-site authorized support representatives. By default, on-site authorized support representatives are allowed to access your system through the appliance console and diagnose issues that you have reported.

Support access is a root-level shell, which enables the on-site authorized support representative to debug any problems on the appliance and obtain a one-time password using a challenge/response mechanism similar to the one for a password reset.

Any time after the initial configuration of the appliance, you can enable or disable services access through the UI by selecting **Actions**→**Edit services access** on the **Settings** window.

You can also use an `appliance/settings` REST API to enable or disable services access.

NOTE: HP recommends that you enable access. Otherwise, the authorized support representative might be unable to access the appliance to correct a problem.

3.13.2 Restricting console access

For the virtual appliance, you can restrict console access through secure management practices of the hypervisor itself.

This information is available from the VMware website:

<http://www.vmware.com/support/pubs>

In particular, search for topics related to vSphere's Console Interaction privilege and best practices for managing VMware's roles and permissions.

3.14 Algorithms for securing the appliance

- SSL (see [Table 2 \(page 54\)](#))
- SHA-256 for hashing local user account passwords
- Other passwords are encrypted using 128-bit Blowfish
- Support dumps:
 - Encryption: 128-bit AES
 - Hash: SHA-256
 - The AES key is encrypted separately using 2,048-bit RSA.
- Updates:
 - Not encrypted; digitally signed using SHA-256 and 2,048-bit RSA

The following SSL cipher suites are enabled on the HP OneView appliance web server. The cipher suites support the connection among the browser, other clients, and the appliance.

Table 2 Supported SSL cipher suites

SSL cipher suite	SSL version	Kx	Au	Enc	Mac
DHE-RSA-AES256-SHA	SSL v3	DH	RSA	AES (256)	SHA1
AES256-SHA	SSL v3	RSA	RSA	AES (256)	SHA1
EDH-RSA-DES-CBC3-SHA	SSL v3	DH	RSA	3DES (168)	SHA1
DES-CBC3-SHA	SSL v3	RSA	RSA	3DES (168)	SHA1

Table 2 Supported SSL cipher suites *(continued)*

SSL cipher suite	SSL version	Kx	Au	Enc	Mac
DHE-RSA-AES128-SHA	SSL v3	DH	RSA	AES (128)	SHA1
AES 128-SHA	SSL v3	RSA	RSA	AES (128)	SHA1

3.15 Downloads from the appliance

You can download the following data files from the appliance:

- **Support dump**
By default, all data in the support dump is encrypted and accessible by an authorized support representative only.
- **Backup file**
All data in the backup file is in a proprietary format. HP recommends that you encrypt the file according to your organization's security policy.
- **Audit logs**
Session IDs are not logged, only the corresponding logging IDs are logged. Passwords and other sensitive data are not logged.

4 Navigating the graphical user interface

4.1 Browsers

For general information about browser use, see the following topics:

- “Supported browsers” (page 57)
- “Required plug-ins and settings” (page 57)
- “Browser best practices for a secure environment” (page 52)
- “Commonly used browser features and settings” (page 57)

4.1.1 Supported browsers

For information about the web browsers that are supported for use with HP OneView, see the *HP OneView Support Matrix*.

4.1.2 Required plug-ins and settings

For information about required plug-ins and settings that are supported for use with HP OneView, see the *HP OneView Support Matrix*.

NOTE: SSL v2 is considered insecure and should not be enabled in the browser unless there is a specific need for it.

4.1.3 Commonly used browser features and settings

Feature	Description
Screen resolution	For optimum performance, the minimum screen size is 1280 × 1024 pixels for desktop monitors and 1280 × 800 for laptop displays. The minimum supported screen size is 1024 × 768 pixels.
Language	US English is the supported language.
Close window	You can close browser windows at any time. Closing the window while you are logged in terminates your session.
Copy and paste	You can select and copy most text, with the exception of text in images. You can paste text into text entry boxes.
Search in a screen	Press Ctrl+F to search for text in the current screen.
Local history	Right-click the browser back button to view the history of the active tab. Use this feature to determine how you arrived at the current screen.
Back and forward buttons	<p>You can use the browser back and forward buttons to navigate the UI.</p> <p>NOTE: Pop-up dialog boxes are not considered screens. If you click the back button while a pop-up dialog box is displayed, you return to the previous screen.</p> <p>If you click the forward button to go to a pop-up dialog box, you go instead to the screen with the link to the pop-up dialog box.</p> <p>The exceptions are screens that you access directly from the Actions menu. If you use the browser navigation buttons with these screens, you lose any unsaved changes you made on the screens.</p>
Bookmarks	You can create bookmarks for commonly-used screens. You can email these links to other users, who must log in and have the appropriate authorization for the screen.

Feature	Description
Open screens in a new tab or window	Right-click a link to a resource or screen to open the link in a new tab or window. NOTE: If you right-click a link while in an edit screen, the actions you take on another screen do not automatically refresh the form in the first screen. For example, if the Add Network dialog box is open, but you do not have any networks to add, you can create networks in a new tab or window. However, the first Add Network dialog box does not recognize the new networks automatically.
Browser refresh	If you click the browser refresh button to refresh a screen on which you have added but not saved information, you lose the information.
Zoom in/zoom out	Use the zoom in or zoom out feature to increase or decrease the text size, respectively.

4.1.4 Set the browser for US or metric units of measurement

To configure how units of measurement are displayed—either in United States (US) or metric units—change the region portion of the language setting in your browser.

Metric units are used for all regions except the United States region. Specify the United States as your region code if you want United States customary units. Specify any other region code if you want metric units.

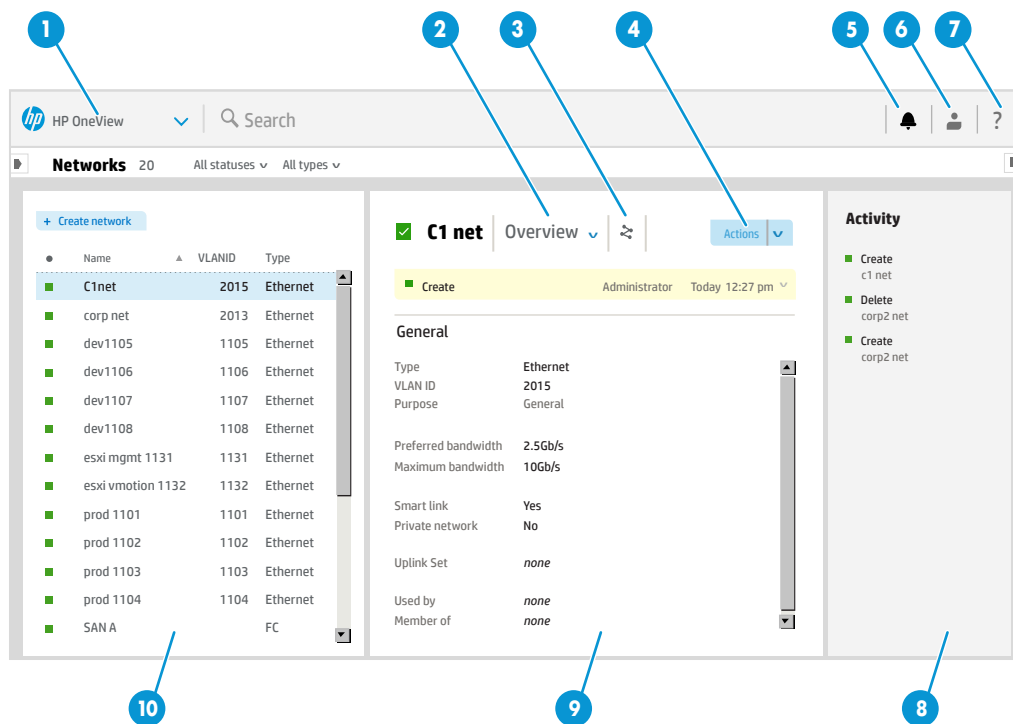
Table 3 Set US or metric units of measurement

Browser	Procedure
Google Chrome	<ol style="list-style-type: none"> 1. Click the Google menu icon. 2. Select Settings→Show advanced settings... 3. Scroll down to Languages and click Language and input settings... 4. Click Add and then select the language you want to use. 5. Restart the browser to apply your changes.
Microsoft Internet Explorer	<p>The browser locale and regions locale are derived from your Windows settings.</p> <ol style="list-style-type: none"> 1. Select Tools+Internet Options+General (tab)+Languages→Language Preference. 2. Specify your own language tags. Click Add button in the Language Preferences dialog box, and then enter your language tag in the User defined box. 3. Click OK. 4. Restart the browser to apply your changes.
Mozilla Firefox	<p>The browser locale and regions locale are derived from the version of Firefox you are running.</p> <ol style="list-style-type: none"> 1. Select Tools→Options→Content→Languages→Choose. 2. Select your preferred language and then click OK. 3. Restart the browser to apply your changes.

4.2 About the graphical user interface

To learn the names of common areas, icons, and controls on a UI screen, see the numbered descriptions that appear after the image.


Figure 2 Screen topography



1 HP OneView main menu: The primary menu for navigating to resources. Click the ▼ icon to expand the menu.

2 View selector: Enables you to control the information displayed about a resource so that you can focus only on what you are interested in.

3 Map view icon: Provides a graphical representation of the relationships between the current resource and other resources. To see these relationships, select the **Map**

view selector or the  icon.

4 Actions menu: Provides the actions that are available to run on the current resource. Actions include, but are not limited to: adding, creating, deleting, removing, and editing a resource instance. If you do not have the appropriate permissions to perform an action, the action does not appear on the **Actions** menu.

5 Activity control: Expands (or hides) a sidebar of recent appliance, resource, or user activity (from the current login session).

6 Session control: Tracks who is currently logged in to the appliance and the duration of each login session. Also enables you to and edit some user account information, depending on your user credentials.

7 Help control: Expands (or hides) a sidebar which provides access to UI and REST API help, the EULA and Written Offer, and the [HP OneView online user forum](#).

8 Activity sidebar: Shows recent alerts and task activity for the current resource. Use the Activity control icon to open (or close) this sidebar.

9 Details pane: Provides all information known about a selected resource instance. To see details about a particular resource instance, click its name in the master pane.

10 Master pane: Lists all resource instances that have been configured on the appliance. In some cases, a [status icon](#) indicates general health of the resource.

In addition to the screen components shown in [Figure 2 \(page 59\)](#), every UI screen has a [notifications area](#) that notifies you when an event or activity requires your attention.

Some screens also have a [filters sidebar](#) that enables you to control the amount and type of information displayed in the details pane.

4.3 About the Activity sidebar

The **Activity** sidebar shows activities (specifically, tasks) initiated during the current session. The most recent task is displayed first.

Task notifications provide information (including in-progress, error, and completion messages) about tasks that were launched.

The **Activity sidebar** differs from the **Activity** screen because it displays only recent activity. The **Activity** screen, in contrast, displays all activities and allows you to list, sort, and filter them. For more information, see [“About activities” \(page 173\)](#).

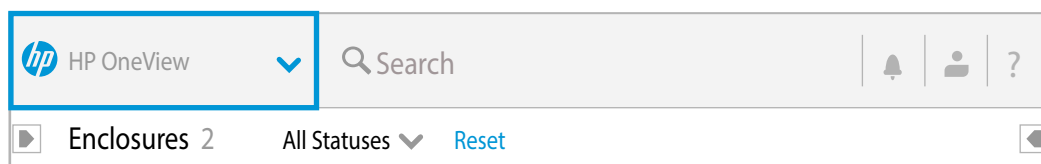
Click an activity to show more details.

4.4 Banner and main menu

The main menu is the primary method for navigating to resources and the actions that can be performed on them.

To expand the main menu, click inside the main menu area of the banner.

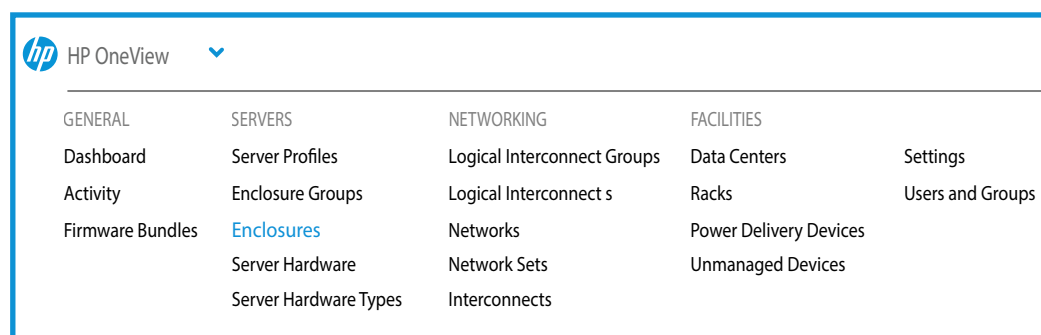
Figure 3 Banner



The main menu provides access to resources; each resource screen contains an **Actions** menu.

- If you are not authorized to view a resource, that resource does not appear in the [main menu](#).
- If you do not have the appropriate permissions to perform an action, the action does not appear on the **Actions** menu.

Figure 4 Expanded main menu



4.5 Button functions

UI buttons function the same, whether they appear on screens or dialog boxes.

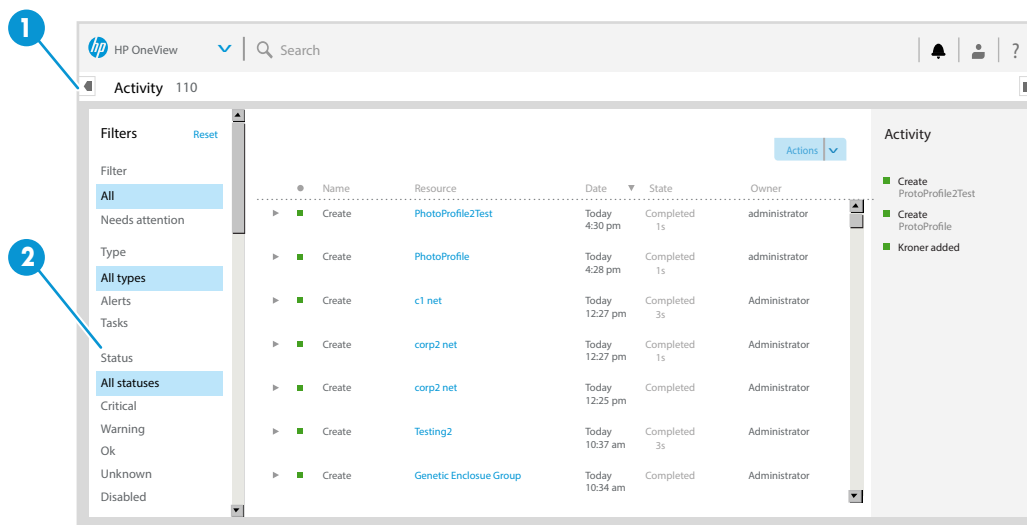
Table 4 UI buttons

Button	Description
Add and Add +	<p>Adds items from your current data center environment (such as enclosures, server hardware, and other physical items) and brings them under appliance management.</p> <ul style="list-style-type: none"> • Add adds a single item and closes the screen or dialog box. • Add + enables you to add another item in the same session.
Create and Create +	<p>Creates logical constructs used by the appliance (such as server profiles, logical interconnect templates, and network sets).</p> <ul style="list-style-type: none"> • Create creates a single item and closes the screen or dialog box. • Create + enables you to create another item in the same session.
Cancel	Closes a screen or dialog box. If you made changes to the screen, unsaved changes are discarded.
OK	Confirms and saves your edits and closes the screen or dialog box.

4.6 Filters sidebar

Some resource screens have a **Filters** sidebar that enables you to control the amount and type of information displayed in the [details pane](#).

Figure 5 Filters sidebar



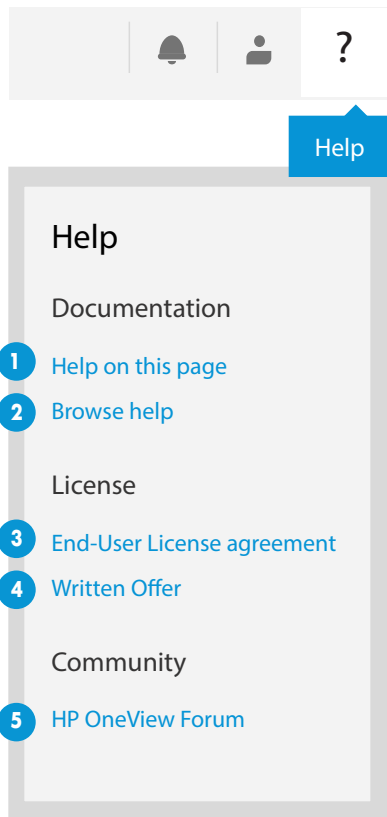
1 Pin control: Expands or hides the **Filters** sidebar.

2 Sorting and filtering criteria enables you to refine the information displayed for a resource in the [details pane](#).

4.7 Help sidebar

Select the help icon in the banner to open the help sidebar, which provides hyperlinks to the help system, license agreement, open source code used in the product, and access to the online user community.

Figure 6 Help sidebar
















- 1 Opens context-sensitive help for the current resource in a new browser window or tab.
- 2 Opens the top of the help system in a new browser window, which enables you to navigate to the entire table of contents for the UI help and REST API documentation.
- 3 Displays the End-User License agreement (EULA).
- 4 Displays the Written offer, which describes the open source products used by HP OneView.
- 5 Opens a new browser window to the <http://www.hp.com/go/oneviewcommunity> online user forum where you can share your experiences using HP OneView and pose or answer questions. This forum also hosts PowerShell and Python libraries, which utilize the comprehensive RESTful API provided by HP OneView to perform any action.

4.8 Icon descriptions










HP OneView uses icons to represent the current status of resources and alerts and to control the display.

- “Status and severity icons” (page 63)
- “User control icons” (page 63)
- “Informational icons” (page 64)





4.8.1 Status and severity icons

Large icon	Small icon	Resource	Activity	Task
		Critical	Critical	Failed/Interrupted
		Warning	Warning	Warning
		OK	Informational	Success
		Disabled		Canceled
		Unknown		
		An In progress rotating icon indicates that a change is being applied or a task is running. This icon can appear in combination with any of the resource states; for example: 		

4.8.2 User control icons

Icon	Name	Action
	Expand menu	Expands a menu to show all options
	View details	Identifies a title that has additional information. Clicking the title changes the view to display details.
	Expand	Expands a collapsed list item
	Collapse	Collapses an expanded list item
	Edit	Enables editing
	Delete or remove	Deletes the current entry
	Search	Searches for the text you enter in the Search box; especially useful for finding types of resources or specific resources by name
	Pin	The left pin expands or collapses the Filters sidebar The right pin expands or collapses the Activity sidebar or Help sidebar
	Sort	Determines whether items are displayed in ascending or descending order

4.8.3 Informational icons

Icon	Name	Description
	Map	Provides a graphical representation of the relationships between the current resource and other resources
	Activity control	Provides a recent history of user and appliance initiated tasks and alerts
	Session control	Displays your login name, how long you are logged on, and provides a link that enables you to log out of the appliance You can use the Edit icon next to your login name to change your full name, password, and contact information.
	Help control	<ul style="list-style-type: none">• At the top of a dialog box, this icon opens context-sensitive help for that topic in another window or tab.• In the banner, this icon expands or collapses the Help sidebar, where you can browse the help documentation or find help on the page currently displayed. The help sidebar provides the following:<ul style="list-style-type: none">◦ A Help on this page hyperlink to access context-sensitive help for the current screen◦ A Browse help hyperlink to access the entire help system◦ Links that you can use to display the EULA (End User License Agreement) and the Written Offer.◦ A link to the HP OneView Forum, an online forum for customers and partners to share their experiences and pose questions related to using HP OneView. Community members as well as HP representatives are welcome to assist with answering questions.

4.9 Map view screen details

The **Map** view enables you to examine the configuration and understand the relationships between logical and physical resources in your data center. This view gives you immediate visibility into your resources from the individual Ethernet and Fibre Channel networks all the way up to the enclosure, rack, and top-level physical data center.

The **Map** view was designed to be highly interactive and useful even at scale.

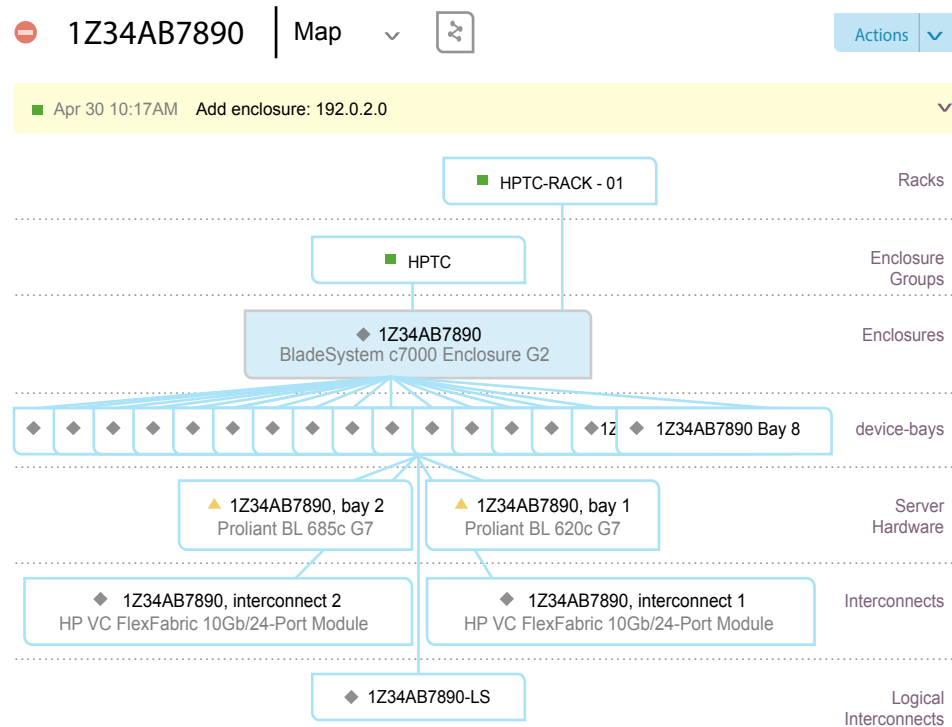
To open the relationship view for a resource, do one of the following:

- Select **Map** from the [view selector](#).
- Select the  icon.

Providing context for a resource can be helpful when troubleshooting problems with the resource. By looking at the **Map** view, you can determine if anything related to the resource is also having a problem.

A [status icon](#) indicates the general health of the resource and provides a quick path to track errors.

Figure 7 Sample Map view



The selected resource is located at the center of the **Map** view. Everything above the resource is an ancestor; everything below the resource is a descendant.

A connecting line between boxes indicates a direct relationship, such as blade servers in an enclosure. Use your pointing device to hover over any resource to see its direct relationships to other resources. Other items can be indirectly related to the resource, such as logical interconnect groups and server profiles.

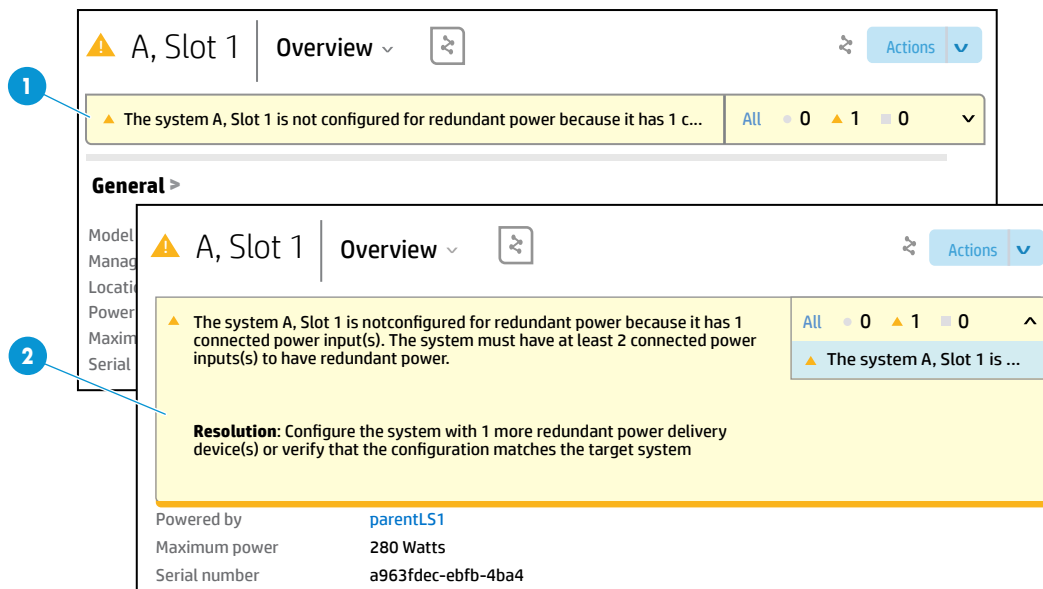
Click any resource that appears in a relationship view to open its specific **Map** view.

4.10 Notifications area

The notifications area on a resource UI screen appears when an activity (an alert or task) has affected the resource, which might require your attention.

By default, only one line of information appears in the notifications area. Click anywhere in the yellow box to expand the notifications area and view more information associated with the activity. Click again to collapse the notifications area.

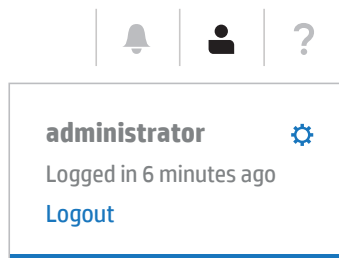
Figure 8 Notifications area



- 1 A collapsed notifications area (the default). Select **All** to view all activity associated with the resource.
- 2 An expanded notifications area, which provides resolutions for critical or warning alerts that require your attention, with links to **Details**, when they are available.

4.11 Log out of the appliance

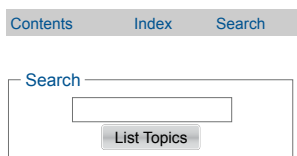
1. Click the [Session control](#) icon in the [banner](#).
2. Select **Logout**.



4.12 Search help topics

1. On any screen, click the [?](#) icon in the [banner](#) to open the help sidebar.
2. In the **Help** sidebar, select **Help on this page**.
Context-specific help appears in a separate browser window.
3. In the new browser window where the help is displayed, click **Search** at the top of the left navigation pane, next to the **Contents** and **Index** links.

Figure 9 UI help search box



4. Enter a search term in the **Search** box. Note the following:
 - Search terms are case insensitive.
 - Cutting and pasting text into the search box is supported.
 - Wildcard characters, such as the asterisk (*), are not supported.
 - Enclosing a search phrase in double quotation marks is not supported.
5. Press **Enter** or click **List Topics** to start the search process.
Search results are presented as links to the sections in which the search term appears.
6. Scan the search results for the section title or titles that best match what you are looking for, and click the link to view the content. Each instance of your search term is highlighted in yellow for easy identification.

4.12.1 About help system search results

Note the following about how the help system search feature operates:

- Unrelated partial terms are not found. For example, a search for `cat`:
 - Finds `cat` and `cats`
 - Does not find `category` because it is an unrelated term with a partial match
- Searches sometime return metadata rather than actual help content.
- Searches sometime return the stem word rather than the search term. For example, searching for `Orchestration` stems to `orchestr` and thus returns no results. This is expected behavior.

4.13 Search resources

The **banner** of every screen includes the **Smart Search** feature, which enables you to find resource-specific information such as specific instances of resource names, serial numbers, WWNs, and IP and MAC addresses. In general, anything that appears in a resource is searchable.

Smart Search makes locating resources by model as simple as typing the model string (for example BL660), enabling you to inventory or take action on a desired set of devices.

Perhaps you are looking for all resources in a given enclosure or need to find one server using a certain MAC address. Smart Search instantly gives you the information you are seeking.

The default search behavior is to focus on the resource you are currently viewing. But, to broaden the scope of your search across all resources, you have the option to search **Everything**, which searches all resources.

Some resources might not include the option to choose between the current resource or everything, in which case the default search is for everything.

When you start typing, search suggestions are provided based on pattern matching and previously-entered search criteria.

- Select a suggestion to change your filter to the suggestion and submit it (as if you had pressed **Enter**).
- Press **Enter** to see the list of search matches.
- If you are doing a resource match, the **master pane** is filtered to match your search input.



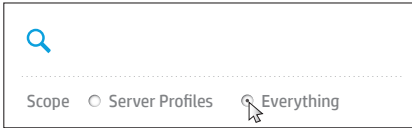


TIP: Enter complete words or names as your search criteria. Partial words or names might not return the expected results.

If you enter a multi-word search term, results show matches for all words you enter.

When you find what you are looking for in the search results, which are organized by resource type, select the item to navigate to it.

NOTE: The **Smart Search** feature does not search the help system. To search the UI and REST API help, see [“Search help topics” \(page 66\)](#).

Search the current resource	Search all resources
<p>1. Click in the Smart Search box.</p>  <p>2. Enter your search text and press Enter. The search results are focused in your current location in the UI.</p>	<p>1. Click in the Smart Search box.</p>  <p>2. Select Everything.</p>  <p>3. Enter your search text and press Enter.</p>

Advanced searching and filtering with properties



TIP: Enclose a search value in double quotes if the value contains spaces. Enter complete values for the properties. Partial values do not return search results.

Example of advanced filtering syntax	Search results
By model name: model:"BladeSystem c7000 Enclosure G2" model:"ProLiant BL460c Gen8" model:"HP VC 8Gb 20-Port FC Module"	All hardware that match the model number and name.
By name: name:enclosure10 name:"192.0.2.0, PDU 1"	An enclosure with the name enclosure10. A power delivery device with the name 192.0.2.0, PDU 1.
By health status: status:Critical	All resources that are in a critical state. Other health status values are: <ul style="list-style-type: none">• Error• Warning• OK• Unknown• Disabled

4.14 View resources according to their health status

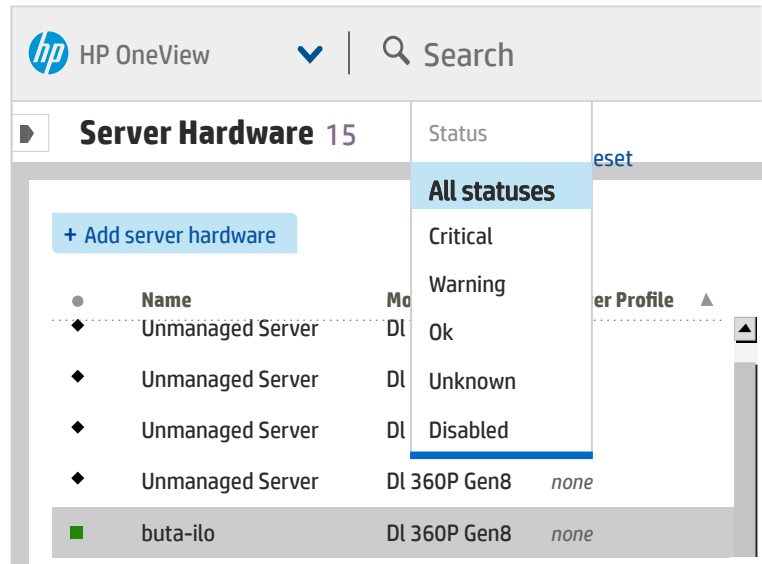
On most screens, you can filter the view of resource instances based on their health status, which might be useful for troubleshooting or maintenance purposes.

The default filtering is **All statuses**, which means that all resource members are shown, regardless of their health status.

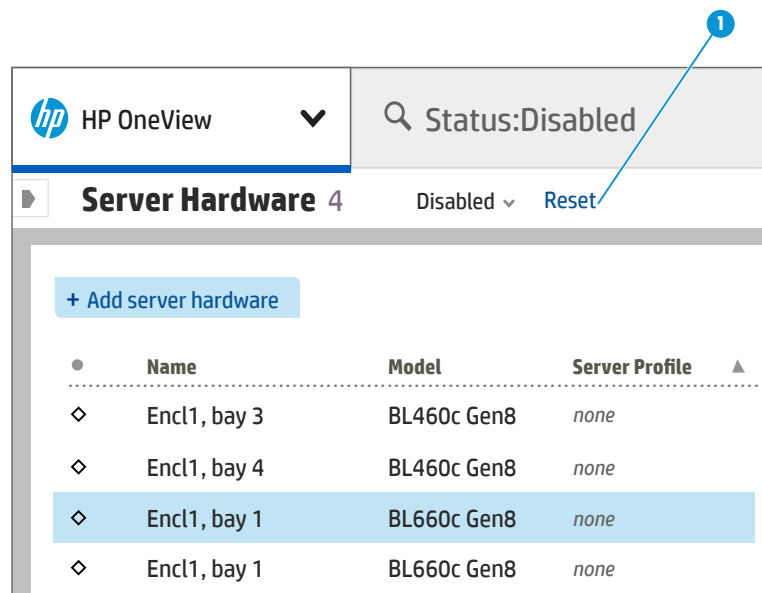
To filter that view based on a specific health status, select the health status you are interested in viewing from the **Status** menu.

For more information about health status icons and what they mean, see “[Icon descriptions](#)” (page 62).

Figure 10 Filter resource instances by their health status



4.14.1 Reset the health status view



1 To return to the default view, **All statuses**, click the **Reset** link.

5 Using the REST APIs and other programmatic interfaces

REST (Representational State Transfer) is a web service that uses basic CRUD (Create, Read, Update and Delete) operations performed on resources using HTTP `POST`, `GET`, `PUT`, and `DELETE`. To learn more about REST concepts, see http://en.wikipedia.org/wiki/Representational_state_transfer.

The appliance has a resource-oriented architecture that provides a uniform REST interface. Every resource has one URI (Uniform Resource Identifier) and represents a physical device or logical construct. You can use REST APIs to manipulate resources.

For general information about REST APIs, see the following topics:

- “Resource operations” (page 71)
- “Return codes” (page 72)
- “URI format” (page 72)
- “Resource model format” (page 72)
- “Log in to the appliance using REST APIs” (page 72)
- “REST API version” (page 72)
- “Asynchronous versus synchronous operations” (page 73)
- “Task resource” (page 73)
- “Error handling” (page 73)
- “Concurrency control using etags” (page 73)
- “Querying resources using common REST API parameters” (page 74)
- “State Change Message Bus” (page 74)
- “Developer tools in a web browser” (page 74)
- “Using Python and Windows PowerShell commands (technical preview)” (page 74)

5.1 Resource operations

RESTful APIs are stateless. The resource manager maintains the resource state that is reported as the resource representation. The client maintains the application state and the client might manipulate the resource locally, but until a `PUT` or `POST` is made, the resource as known by the resource manager is not changed.

Operation	HTTP Verb	Description
Create	<code>POST</code> resource URI (payload = resource data)	Creates new resources. A synchronous <code>POST</code> returns the newly created resource. An asynchronous <code>POST</code> returns a <code>TaskResource</code> URI in the <code>Location</code> header. This URI tracks the progress of the <code>POST</code> operation.
Read	<code>GET</code> resource URI	Returns the requested resource representation(s)
Update	<code>PUT</code> resource URI (payload = update data)	Updates an existing resource
Delete	<code>DELETE</code> resource URI	Deletes the specified resource

5.2 Return codes

Return code	Description
2xx	Successful operation
4xx	Client-side error with error message returned
5xx	Appliance error with error message returned

NOTE: If an error occurs, indicated by a return code 4xx or 5xx, an `ErrorMessage` is returned. The expected resource model is not returned.

5.3 URI format

All URIs point to resources. The client does not need to create or modify URIs. The URI for a resource is static and uses the format `https://{appl}/rest/resource category/resource ID` where:

<code>https://{appl}</code>	Appliance address
<code>/rest</code>	Type of URI
<code>/resource category</code>	Category of the resource (for example <code>server-profiles</code>)
<code>/resource instance ID</code>	Identifier of specific resource instance (optional)

5.4 Resource model format

The resources support JSON (JavaScript Object Notation) for exchanging data using a REST API. If not otherwise specified in the REST API operation, the default is JSON.

5.5 Log in to the appliance using REST APIs

When you log in to the appliance using the `login-sessions` REST API, a session ID is returned. You use the session ID in all subsequent REST API operations in the `auth` header, except as noted in *REST API Request Headers*. The session ID is valid for 24 hours.

Log in	Log out
Operation POST	Operation DELETE
API <code>/rest/login-sessions</code>	API <code>/rest/login-sessions</code>
Request headers <i>REST API Request Headers</i>	Request headers <code>auth: {YourSessionID}</code> <i>REST API Request Headers</i>
Request body <code>{"userName": "YourUserName", "password": "YourPassword"}</code>	Request body None
NOTE: This is an example of a local log in on the appliance. If you are using a directory service, you must add the following attributes: <code>authnHost</code> and <code>authLoginDomain</code> .	Response 204 No Content
Response The <code>LoginSessionIdDTO</code> that includes the session ID	

5.6 REST API version

When you perform a REST API operation, a `X-API-Version` header is required. This version header corresponds to the REST API version of software currently running on the appliance. To

determine the correct REST API version, perform `/rest/version`. This GET operation does not require an `X-API-Version` header. If multiple appliances are running in your environment, you need to determine the REST API version required by each appliance.

The `X-API-Version` header for this release of HP OneView must always be 3 (`X-API-Version:3`).

5.7 Asynchronous versus synchronous operations

A synchronous task returns a response after the REST API operation. For example, `POST /rest/server-profiles` returns a newly created server profile in the response body. An asynchronous task, such as creating an appliance backup returns the URI of a `TaskResource` resource model. You can use the `TaskResource` resource model URI to list the current status of the operation.

5.8 Task resource

When you make an asynchronous REST API operation, HTTP status 202 `Accepted` is returned and the URI of a `TaskResource` resource model is returned in the `Location` header of the response.

You can then perform a GET on the `TaskResource` model URI to poll for the status of the asynchronous operation. The `TaskResource` model also contains the name and URI of the resource that is affected by the task in the `associatedResource` attribute.

Creating an appliance backup example

1. Create an appliance backup.

```
/rest/backups
```

The URI of a `TaskResource` in the `Location` header is returned in the response.

2. Poll for status of the backup using the `TaskResource` URI returned in step 1.

```
/rest/tasks/{id}
```

3. When the task reaches the `Completed` state, use the `associatedResource` URI in the `TaskResource` to download the backup file.

```
GET {associatedResource URI}
```

5.9 Error handling

If an error occurs during a REST API operation, a `4xx` (client-side) or `5xx` (appliance) error is returned along with an error message (`ErrorMessage` resource model). The error message contains a description and might contain recommended actions to correct the error.

A successful REST API `POST` operation returns the newly created resource (synchronous) or a `TaskResource` URI in the `Location` header (asynchronous).

5.10 Concurrency control using etags

A client uses etags to verify the version of the resource model. This prevents the client from modifying (`PUT`) a version of the resource model that is not current. For example, if a client performs a `GET` on a server profile and receives an etag in the response header, modifies the server profile, and then updates (`PUT`) the resource model, the etag in the `PUT` request header must match the resource model etag. If the etags do not match, the client `PUT` request will not complete and a `412 PRECONDITION FAILED` error is returned.

5.11 Querying resources using common REST API parameters

You can use a set of common parameters to customize the results returned from a GET operation, such as sorting or filtering. Each REST API specification lists the set of available common parameters.

5.12 State Change Message Bus

The State-Change Message Bus (SCMB) is an interface that uses asynchronous messaging to notify subscribers of changes to managed resources—both logical and physical. For example, you can program applications to receive notifications when new server hardware is added to the managed environment or when the health status of physical resources changes—without having to continuously poll the appliance for status using the REST APIs. To learn more about receiving asynchronous messages about changes in the appliance environment, see “[Using the State-Change Message Bus \(SCMB\)](#)” (page 185).

5.13 Developer tools in a web browser

You can use developer/debug tools in your web browser to view the REST API operations as they happen in the UI. The UI uses REST APIs for all operations; therefore, anything you can do in the UI can be done using REST API operations.

5.14 Using Python and Windows PowerShell commands (technical preview)

See the HP OneView forum at <http://www.hp.com/go/oneviewcommunity> for code samples and a technical preview of PowerShell and Python libraries that contain command line tools to automate and accelerate using REST APIs on the appliance to perform various administrative tasks.

6 Accessing documentation and help

This chapter describes how to access help from the appliance, how to access the publicly available online information library, and where to find REST API help and reference documentation.

6.1 Online help—conceptual and task information as you need it

The online help documents both the UI and the REST APIs, and includes:

- Overviews of the appliance and its features
- Descriptions of resources and UI screens
- Quick-start instructions for bringing your data center under management
- Step-by-step instructions for using the UI to perform tasks
- Information about using REST API scripting to perform tasks
- The *HP OneView REST API Reference*
- Information about using the SCMB (State-Change Message Bus) to subscribe to state change messages

REST API help design

The REST API help is designed so that:

- Each resource is documented in its own chapter.
- Each REST API scripting chapter identifies the REST API calls you must invoke to complete the tasks.
- Each REST API call links to the *HP OneView REST API Reference* for details about the API, such as attributes and parameters, the resource model schema, and JSON (JavaScript Object Notation) examples.

UI help design

The online help for the UI is designed so that each resource is documented in its own chapter. At the top of each help chapter is a navigation box that directs you to:

- Tasks that you can perform using the UI
- An **About** section that provides conceptual information about the resource
- A screen details section for every screen, which provides definitions of screen components to assist you in data entry and decision making
- Troubleshooting information in case you encounter a problem
- Links to the help for the associated REST APIs if you prefer to use REST API scripting to perform a task

6.2 This user guide supplements the online help

This user guide provides:

- Conceptual information and describes tasks you can perform using the UI or REST APIs. It does not duplicate the step-by-step instructions provided by the online help unless the information might be needed when the online help is not available.
- For procedures that use the REST APIs, the REST APIs are listed, but the complete syntax and usage information is included in the *HP OneView REST API Reference* in the online help.

- Planning information, including configuration decisions to make and tasks that you might need to perform before you install an appliance, add managed devices, or make configuration changes
- Quick starts that provide high-level step-by-step instructions for selected tasks that might require that you configure multiple resources using the UI or REST APIs.
- An illustrated example of using the UI to configure a sample data center

6.3 Where to find HP OneView documentation

The following HP OneView documentation is available to view or download from the HP OneView Information Library:

<http://www.hp.com/go/oneview/docs>

HP OneView documentation

- *HP OneView Release Notes*
- *HP OneView Support Matrix*
- *HP OneView Installation Guide*
- *HP OneView User Guide*
- *HP OneView REST API Reference*
- zip file of the HP OneView UI and REST API HTML help files
- Technical white papers

NOTE: To submit documentation feedback to HP, send email to docsfeedback@hp.com.

6.4 Enabling off-appliance browsing of UI and REST API HTML help files

To enable your users and developers to browse the HP OneView help and *HP OneView REST API Reference* locally on their own computer or from a local web server, download the `hp-oneview-help.zip` file from the HP OneView Information Library.

An off-appliance version of the HP OneView help system is useful for developers who are writing REST API scripts or other users that prefer the convenience of accessing help without logging in to the appliance.

Downloading HTML help and REST API files

1. Go to the HP OneView Information Library:
<http://www.hp.com/go/oneview/docs>
2. Select the `hp-oneview-help.zip` file and save it to your computer or a local directory on a web server.
3. Use the utility of your choice to extract the contents of the `.zip` file.
4. Navigate to the `hp-oneview-help/content` directory.
5. Double click the `index.html` file to open the HP OneView help system.
6. If you are serving the files from a web server, communicate the full URL to the `index.html` file to your user community to enable them to browse to the UI and REST API help and reference information.

Part II Planning tasks

The chapters in this part describe data center configuration planning tasks that you might want to complete before you install the appliance or before you make configuration changes. By completing these planning tasks, you can create a data center configuration that takes full advantage of the appliance features and is easier for your administrators to monitor and manage.

7 Planning your data center resources

In addition to ensuring that your environment meets the prerequisites for installation of the appliance, there are other planning tasks you might want to complete before adding data center resources. By completing these planning tasks, you can create a data center configuration that takes full advantage of the appliance features and is easier for your administrators to monitor and manage.

7.1 How many data centers?

An appliance data center resource represents a physically contiguous area in which racks containing IT equipment are located. You create data centers in the appliance to describe a lab floor or a portion of a computer room, which provides a useful grouping to summarize your environment and its power and thermal requirements.

Using data centers to describe the physical topology and power systems of your environment is optional. If you choose to create multiple data centers, consider including data center information in your other resource names to enable you to use the appliance search capabilities to filter results by data center.

7.2 Security planning

This section recommends security decisions you might want to make before you install the appliance or bring hardware under management.

To learn about the security features of the appliance, and for general information about protecting the appliance, see [“Understanding the security features of the appliance” \(page 45\)](#).

7.2.1 Choosing an Administrator password

During installation you must change the password for the Administrator user, which is a user with Infrastructure administrator privileges. The default password cannot be used again.

For guidelines on choosing passwords, see [“Best practices for maintaining a secure appliance” \(page 46\)](#).

7.2.2 Choosing the LAN for the appliance

The appliance is designed to operate entirely on an isolated management LAN. Access to the production LAN is not required. Isolating the management LAN from the production LAN helps to keep the production LAN secure.

For more information about security for management and production LANs, see [“Best practices for maintaining a secure appliance” \(page 46\)](#).

7.2.3 Choosing whether or not to enable support access

This product contains a technical feature that will allow an on-site authorized support representative to access your system, through the system console, to assess problems that you have reported. This access will be controlled by a password generated by HP that will only be provided to the authorized support representative. You can disable access at any time while the system is running.

As part of the appliance installation, you must choose whether or not to enable access by support personnel. To change this setting, see [“Managing the appliance settings” \(page 155\)](#).

7.2.4 Choosing an SNMP read community string

Network management systems use SNMP (Simple Network Management Protocol) to monitor network-attached devices. The appliance uses SNMP to retrieve information from managed devices. You specify a read community string that serves as a credential to verify access to the SNMP data on managed devices.

The default SNMP read community string, `public`, is easily guessed. You can make your SNMP environment more secure by changing the SNMP read community string to use a strong password. If you use the appliance REST APIs, you can avoid manually refreshing managed devices by changing the SNMP read community string before you add devices to the appliance.

For more information about changing the SNMP read community string, see [“Managing the appliance settings” \(page 155\)](#).

7.2.5 Choosing a security certificate policy

The appliance supports self-signed certificates and certificates issued by a certificate authority.

The appliance is configured initially with a self-signed certificate. To replace self-signed certificates with certificates issued by your organization’s certificate authority, see [“Managing SSL certificates” \(page 157\)](#).

For more information about certificates, see [“Appliance access over SSL” \(page 50\)](#).

7.2.6 Determining roles and restrictions for authorized users

Access to the appliance is controlled by roles, which describe what a user is permitted to see and do on the appliance. Each user must be associated with at least one role. Determine the roles and responsibilities for authorized users of the appliance, and choose appropriate user roles to limit access to the appliance.

Consider limiting the number of local accounts and integrating the appliance with an enterprise directory solution such as Microsoft Active Directory or OpenLDAP.

For more information about users and user roles, see [“Managing users and authentication” \(page 143\)](#).

7.2.7 Determining your backup policy

A backup file is an encrypted snapshot of the appliance configuration and management data at the time the backup file was created. HP recommends that you create regular backups, preferably once a day and after you make hardware or software configuration changes in the managed environment.

As an alternative to using **Settings**→**Actions**→**Create backup** from the appliance UI, you can write and run a script to automatically create and download an appliance backup file. You can schedule the backup script to run automatically in interactive or batch mode on a regular basis. Only a user with Backup administrator or Infrastructure administrator privileges can run the script interactively.

For more information, see [“Sample backup script” \(page 271\)](#).

7.2.8 Choosing a policy for the audit log

Choose a policy for downloading and examining the audit log.

The audit log contains a record of actions performed on the appliance, which you can use for individual accountability. As the audit log gets larger, older information is deleted. To maintain a long-term audit history, you must periodically download and save the audit log.

For more information about the audit log, see [“Understanding the audit log” \(page 48\)](#).

7.2.9 Determining your vSphere client policy

Ensure that only authorized users have access to the appliance console. Use the hypervisor management software to prevent unauthorized users from attempting to log in to the appliance to reset the administrator password or edit services access.

For more information, see [“Access to the appliance console” \(page 53\)](#).

7.2.10 Reviewing your firewall access

The appliance maintains a firewall that allows traffic on specific ports and blocks all unused ports. For a list of the network ports used by the appliance to manage data center resources, see [“Ports needed for HP OneView” \(page 53\)](#).

7.3 Preparing your data center network switches

The switch ports for data center network switches that connect to the Virtual Connect interconnect modules must be configured as described in [“Data center switch port requirements” \(page 115\)](#).

7.4 Planning your resource names

The [banner](#) of every screen includes the **Smart Search** feature, which enables you to find resource-specific information such as instances of resource names, serial numbers, WWNs, and IP and MAC addresses. In general, anything that appears in a resource is searchable.

Defining a standard naming convention for your networks, network sets, enclosures, enclosure groups, logical interconnect groups, and uplink sets makes it easy for you to identify them and enables efficient searching or filtering in the UI.

Consider the following information when choosing resource names:

- To minimize the need for name changes and to make network-related resources easier to identify, consider choosing names that include the following information:
 - The purpose of the resource. For example:
prod for production network resources
dev for development network resources
 - For networks, the VLAN ID
 - An identifier to help you distinguish between resources that use the left side or the right side of an enclosure. For example:
left and right
A and B
1 and 2
 - Examples of network names that follow the recommended naming conventions include the following:
dev_1105_A
prod_1102_1
test_1111_left
 - If you plan to use multi-network connections in server profiles, create network sets that contain all the networks to be used by a single profile connection. Choose names such as the following:
dev_nset_A
prodnset_1
testns_left
 - Changing the names of uplinks sets can result in resources being taken offline temporarily (see [“Configuration changes that require or result in resource outages” \(page 85\)](#)). To minimize the need for name changes, and make the uplink sets easier to identify, choose names such as the following:
devUS_A
prodUS_1

testUS_left

- The appliance does not support the filtering of resources, such as server hardware, based on physical location (data center name). To enable filtering by data center name, choose a naming convention that includes the data center name in the resource name.
- The appliance supports the filtering of resources by model, so you can search for server hardware without having to include the model number in the name.
- The appliance provides default names for many resources. For example:
 - Enclosures are assigned the name `Encln`, where *n* is a number that is incremented by 1 as each enclosure is added.
 - `enclosure_name-LI` is the default name of a logical interconnect, where `enclosure_name` is the name of the enclosure.
 - `Datacenter 1` is the name assigned to the data center when you initialize the appliance.
 - Server hardware types are assigned names based on the server model, such as `BL460c Gen8 1`. If you select a server hardware type as a standard, you can choose to rename that server hardware type to include the word `Standard` or some other identifier to help administrators quickly determine the correct server hardware type to choose.
- You can create shorter names by using abbreviations for resources. For example:

Resource name	Typical abbreviations
Enclosure	Encl
Enclosure group	EG, Group
Logical interconnect	LI
Logical interconnect group	LIG
Uplink set	US

For more information about the search capabilities of the appliance, see [“Search resources” \(page 67\)](#).

7.5 Planning the appliance configuration

7.5.1 Appliance VM and host requirements

HP OneView is delivered as a virtual appliance running on a VMware vSphere Hypervisor VM (virtual machine).

- ❗ **IMPORTANT:** HP OneView cannot import existing VC (HP Virtual Connect) domain configurations, so do not select a host system located in an enclosure that you plan to manage with HP OneView. You can, however, select a host system located on an HP ProLiant DL rack mount server that you plan to manage with HP OneView.

The VM host must be able to support a VM with the following minimum requirements:

- VMware vSphere Hypervisor 5.0 or 5.1.
- Two 2 GHz virtual CPUs.
- 10 GB of memory dedicated to the appliance.
- 160 GB of thick-provisioned disk space.

- A connection to the management LAN. HP recommends that you have separate networks for management and data.
- The clock on the VM host must be set to the correct time. If NTP (Network Time Protocol) is not used to synchronize the time on the VM host, HP recommends configuring the appliance to use NTP directly.

7.5.2 Planning for high availability

To use HP OneView in an HA (high availability) configuration, verify that the VM is configured according to vSphere Hypervisor HA requirements. For more information, see your vSphere Hypervisor documentation or the following website:

<http://www.vmware.com/products/datacenter-virtualization/vsphere/high-availability.html>

7.5.3 Location of the appliance

HP recommends that you do not run the virtual appliance on a host that is to be managed by the same appliance instance.

7.5.4 Separate networks for data and management

HP recommends having separate networks for management and data.

7.5.5 Time clocks and NTP

HP recommends using NTP on the host on which you install the virtual appliance. If you are not using NTP on the host, HP recommends configuring NTP directly on the virtual appliance. Do not configure NTP on both the host and the virtual appliance.

7.5.6 IP addresses

You must specify what type of IP addresses are in use and how they are assigned to the appliance, either manually by you or assigned by a DHCP (Dynamic Host Configuration Protocol) server:

- You must choose either IPv4 or IPv6 addresses.
- The appliance IP address must be static.
- If you use a DHCP address for the appliance it must have an infinite lifetime or permanent reservation.

8 Planning for configuration changes

This chapter identifies configuration changes that might result in a resource being taken offline temporarily or that might require that you make changes to multiple resources.

8.1 Configuration changes that require or result in resource outages

Appliance

Taking an appliance offline does not affect the managed resources—they continue to operate while the appliance is offline.

When you install an appliance update, the appliance is taken offline.

Enclosures

The Onboard Administrator is taken offline when you update firmware for an enclosure.

Interconnects and logical interconnects

- Server profile connections to networks in an uplink set are taken offline when you delete the uplink set.
- Server profile connections to networks in an uplink set can be interrupted for a few seconds when you change the name of an uplink set using either of these methods:
 - Change the name of the uplink set in the logical interconnect.
 - Change the name of the uplink set in the logical interconnect group, and then update the logical interconnect from the logical interconnect group.
- An interconnect is taken offline when you:
 - Update or activate firmware for a logical interconnect. Staging firmware does not require interconnects be taken offline.
 - Update firmware for an enclosure and select the option to update the enclosure, logical interconnect, and server profiles.
- If an interconnect has firmware that has been staged but not activated, any subsequent reboot of that interconnect activates the firmware, which takes the interconnect offline.
- You can prevent the loss of network connectivity for servers connected to a logical interconnect that has a stacking mode of `Enclosure` and a stacking health of `Redundantly Connected` by updating firmware using the following method:
 1. Staging the firmware on the logical interconnect.
 2. Activating the firmware for the interconnects in even-numbered enclosure bays.
 3. Waiting until the firmware update to complete and the interconnects are in the `Configured` state.
 4. Activating the firmware for the interconnects in the odd-numbered enclosure bays.

Networks

- If you attempt to delete a network that is in use by one or more server profiles, the appliance warns you that the network is in use. If you delete the network while it is in use, server profile connections that specify the network explicitly (instead of as part of a network set) are taken offline.

If you add a network with the same name as the network you deleted, connections that specify the network explicitly (instead of as part of a network set) are not updated—you must edit

each server profile connection to reconfigure it to specify the network you added. Because you must edit the server profile to edit the connection, you must power off the server.

- If you attempt to delete a network that is a member of a network set, the appliance warns you that the network is assigned to at least one network set. If you delete that network and there are other networks in that network set, server profile connectivity to the deleted network is taken offline, but connectivity to other networks in the network set are unaffected.

You can add a network to a network set, including a network that has the same name as a network you deleted, while server profile connections to that network set remain online.

Network sets

- If you attempt to delete a network set that is in use by one or more server profiles, the appliance warns you that the network set is in use. If you delete the network set while it is in use, server profile connections to that network set are taken offline.
- If you add a network set with the same name as the network you deleted, connections that specify the network set are not updated—you must edit each server profile connection to reconfigure it to specify the network set you added. Because you must edit the server profile to edit the connection, you must power off the server.
- Server profiles with connections to a network set can be affected when a network in the network set is deleted. See [“Networks” \(page 85\)](#).

Server profiles and server hardware

- Before you edit a server profile, you must power down the server hardware to which the server profile is assigned.
- Firmware updates require that you edit the server profile to change the firmware baseline. As with any other edits to server profiles, you must power down the server hardware to which the server profile is assigned before you edit a server profile.
- Server profiles and server hardware can be affected by changes to networks and network sets. For more information, see [“networks” \(page 85\)](#) and [“network sets” \(page 86\)](#).
- Server profiles and server hardware can be affected by changes to the names of uplink sets. For more information, see [“Interconnects and logical interconnects” \(page 85\)](#).

8.2 Configuration changes that might require changes to multiple resources

8.2.1 Adding a network

When you add a network to the appliance, you might need to make configuration changes to the following resources:

- **Networks.** Add the network.
- **Network Sets.** (Optional) If the network you are adding is an Ethernet network you might want to add it to a network set or create a network set that includes the network.

- **Logical Interconnects and Logical Interconnect Groups.** For a server connected to a logical interconnect to access a network, the logical interconnect must have an uplink set that includes a connection to that network:
 - You might need to update multiple logical interconnects.
 - You can make configuration changes to the logical interconnect group, and then update each logical interconnect from the group.
 - If your configuration changes include deleting an uplink set or changing the name of an uplink set, server profile network connectivity can be affected. See [“Configuration changes that require or result in resource outages” \(page 85\)](#).
- **Server Profiles.** If the server profile does not have a connection to a network set that includes this network, you must add connections to the network.

For a summary of the tasks you complete when adding a network, see [“Quick Start: Adding a network to an existing appliance environment” \(page 95\)](#).

8.2.2 Adding an enclosure

When you add an enclosure to the appliance, you might need to make configuration changes to the following resources:

- **Enclosures.** Add the enclosure.
- **Enclosure Groups.** Every enclosure must be a member of an enclosure group. If you do not choose an existing enclosure group, you must create one when you add the enclosure.
- **Logical Interconnects and Logical Interconnect Groups.** Logical interconnects and logical interconnect groups define the network connectivity for the enclosure. Enclosure groups must specify a logical interconnect group. When you create an enclosure group, if you do not specify an existing logical interconnect group, you must create one. For a server connected to a logical interconnect to access a network, the logical interconnect group you create must have an uplink set that includes a connection to that network.
- **Server Profiles.** Adding and assigning server profiles to the server blades in the enclosure is not required at the time you add the enclosure, but to use the server blades in an enclosure, you must assign server profiles to them. To access a network, the server profile must include a connection to that network or a network set that includes that network.

For a summary of the tasks you complete when adding an enclosure and connect its server blades to data center networks, see [“Quick Start: Adding an enclosure and connecting its server blades to networks” \(page 99\)](#).

Part III Configuration quick starts

The quick starts provided in this part describe the basic resource configuration tasks required to quickly bring the primary components of your hardware infrastructure under appliance management. Additional resource configuration and ongoing management tasks are documented in Part IV.

9 Quick Start: Initial Configuration

This quick start describes the process to bring your data center resources under management of the appliance after you complete the appliance installation. This quick start recommends an order for adding resources to an appliance that has not previously been configured.

9.1 Process overview

1. Before you install the appliance, you might want to plan for your data center configuration. By deciding things like resource names and the number and composition of network sets before you start adding enclosures and servers to the appliance, you can create a configuration that takes full advantage of the appliance features and results in an environment that is easier for your administrators to monitor and manage. In addition, the switch ports for data center network switches that connect to the Virtual Connect interconnect modules must be configured as described in [“Data center switch port requirements” \(page 115\)](#). For planning information, see [“Planning your data center resources” \(page 79\)](#).
2. When you install the appliance, you perform the configuration steps described in the *HP OneView Installation Guide*, including:
 - Changing the Administrator password.
 - Configuring the networking settings for the appliance, including entering an appliance host name and setting IP addresses and DNS server addresses, if used.
3. After you complete the installation, you perform the initial configuration tasks described in [“Configure the environment for the first time” \(page 91\)](#).
For illustrated examples of these tasks, see [“Step by step: Configuring an example data center using HP OneView” \(page 231\)](#).
4. After you perform the initial configuration, back up the appliance and establish policies and procedures for backing up the appliance on a regular basis. For information about creating a backup policy, see [“Determining your backup policy” \(page 80\)](#). For information about backing up the appliance, see [“Backing up an appliance” \(page 149\)](#).
5. If you have not already done so, establish policies for other aspects of appliance and data center security, such as downloading and archiving audit logs. For more information about security planning, see [“Security planning” \(page 79\)](#).

9.2 Configure the environment for the first time

After installation, you must configure the appliance and bring your environment under management. The individual procedures for configuring the appliance and bringing your environment under management for the first time are no different than when they are performed subsequently or when adding individual components or performing maintenance. However, during the initial configuration, you will likely be bringing your entire environment under management and configuring it in the appliance all at once.

While the appliance is designed to allow flexibility in the order that you create, add, and update resources and devices, HP recommends following the workflow below for your initial set up or when making significant additions or changes to your environment.

For configuring the environment for the first time using REST APIs, see the REST API scripting chapter in the online help.

1. [Configure appliance resources and bring your environment under management of the appliance](#)
2. Optional: [Define the physical topology and power systems of your environment in the appliance](#)

Configure appliance resources and bring your environment under management of the appliance

Configuration step	Required action or input	Related information
Add users to the appliance 1. Add users and define access permissions and authentication method. Do one or both of the following: <ul style="list-style-type: none"> Add a user with local authentication and assign a predefined role or create a specialized role. Add a user with directory-based authentication and assign full access or role-based access. 	Local authentication <ul style="list-style-type: none"> Login name Full name (optional) Initial password Choose a role or create a specialized role Contact information (optional) Directory-based authentication <ul style="list-style-type: none"> At least one authentication directory configured in the appliance Default directory (when multiple directories are configured) 	The online help for the Users and Groups screen
Populate the appliance firmware repository 2. Download firmware bundles from HP to the appliance. NOTE: The appliance includes a default firmware bundle that provides the minimum supported firmware for all supported server hardware, iLO, OA, and interconnects. Upload firmware bundles and apply them to your hardware to ensure that you have the latest firmware and can take advantage of all available management features.	<ul style="list-style-type: none"> At least one HP Service Pack for ProLiant (SPP) firmware bundle TIP: HP recommends starting the firmware upload in one browser window and completing the following steps in another window. This prevents the window from being closed during the upload. You can proceed with the initial configuration procedure while the upload completes (the upload can take several minutes).	The online help for the Firmware Bundles screen
Create networks 3. Create Ethernet networks for data and Fibre Channel networks for storage.	Ethernet <ul style="list-style-type: none"> Network name VLAN ID Purpose Bandwidth settings Smart link, Private network, or both (optional) Fibre Channel <ul style="list-style-type: none"> Choose Fabric attach or Direct attach Bandwidth settings Uplink speed TIP: Use network naming conventions to enable quick and intuitive filtering using the search feature.	The online help for the Networks screen
Create network sets 4. Create network sets to group Ethernet networks together for faster configuration.		The online help for the Network Sets screen

Configuration step	Required action or input	Related information
	<ul style="list-style-type: none"> • Network set name • Networks to add to the network set • Indicate the untagged network (optional) 	
Create a logical interconnect group 5. Create a logical interconnect group to define the uplink configuration for all ports.	<ul style="list-style-type: none"> • Define the logical interconnects in enclosures • Create uplink sets to connect networks to uplink ports 	The online help for the Logical Interconnect Groups screen
Create an enclosure group 6. Create an enclosure group to define how added enclosures will be configured.	<ul style="list-style-type: none"> • Assign a logical interconnect group to the enclosure group 	The online help for the Enclosure Groups screen
Add enclosures 7. Add an enclosure to manage its contents and apply firmware updates. NOTE: <ul style="list-style-type: none"> • If your enclosure or server hardware do not have embedded licenses, you will have to add licenses to the appliance. • If you have an SNMP read community string you prefer to use, set the SNMP read community string before you begin adding enclosures. 	<ul style="list-style-type: none"> • There are sufficient licenses embedded on the enclosure OA, server hardware iLO, or in the appliance pool for the server hardware in the enclosure • Enclosure IP address or fully qualified domain name • OA credentials • Assign the enclosure to an enclosure group • Assign a firmware baseline 	The online help for the Enclosures screen The online help for Licensing
Create server profiles 8. Create and apply server profiles for the server hardware in the enclosure.	<ul style="list-style-type: none"> • Server profile name and description • Enclosure name and bay ID • Network or storage connectivity • FlexNIC to assign to the network connection • BIOS settings • Boot order 	The online help for the Server Profiles screen

Optional: Define the physical topology and power systems of your environment in the appliance

HP OneView enables you to define the physical attributes of your data centers and power systems. The **Data Centers** screen provides a 3D model of your environment, which you can use for planning and organization. It also displays power and temperature data so that you can monitor the consumption rates and health of your data center. The appliance monitors and displays peak temperatures for your racks and their components, which can help you identify potential cooling issues in your data center.

Defining your power systems using the Power Delivery Devices resource enables you to monitor metrics such as consumption rates and power caps.

Configuration step	Required action or input	Related information
Add power devices to the appliance <ul style="list-style-type: none"> Define your power devices using the Power Delivery Devices screen 	<ul style="list-style-type: none"> Device type Device name Rated capacity of the device Line voltage and phase Power feed side (A or B) Power connections to the device <p>NOTE: After you enter the device credentials (user name and password), the appliance automatically discovers the HP Intelligent Power Distribution Units (iPDUs).</p>	The online help for the Power Delivery Devices screen
Add and configure racks <ul style="list-style-type: none"> Add racks and configure the layout of enclosures, power delivery devices, and other rack devices using the Racks screen 	<ul style="list-style-type: none"> Rack name Dimensions of the rack and number of slots Add enclosures and power delivery devices to the rack Edit the layout of devices within the rack The thermal limit of the rack (optional) <p>NOTE: The appliance automatically creates racks and when you import enclosures. It places enclosures that are linked by management cables in the same rack.</p>	The online help for the Racks screen
Create data centers and position racks in them <ul style="list-style-type: none"> Define the physical topology of your data center using the Data Centers screen to enable 3D visualization and temperature monitoring. 	<ul style="list-style-type: none"> Data center name Dimensions of the data center Position racks in the data center Power information such as electrical derating, voltage, and power costs Cooling information such as cooling capacity and cooling to power cost multiplier <p>NOTE: The appliance displays new racks in all existing data centers until you position them in a specific data center. If you are viewing a data center with unpositioned racks, a notification is displayed.</p>	The online help for the Data Centers screen

10 Quick Start: Adding a network to an existing appliance environment

This quick start describes the process to add a network to an existing appliance environment and enable existing server blades to access the network you added.

NOTE: If you are performing initial configuration steps after installing an appliance, HP recommends that you add networks and network sets before you add enclosures. See [“Quick Start: Initial Configuration” \(page 91\)](#).

Prerequisites

- Minimum required privileges: Infrastructure administrator or Network administrator for adding the network.
- Minimum required privileges: Infrastructure administrator or Server administrator for changing the configurations of the server profiles.
- The enclosures and server blades are already added to the appliance.
- All data center switch ports that connect to the VC (Virtual Connect) interconnect modules are configured as described in [“Data center switch port requirements” \(page 115\)](#).

Process

When you add a network to the appliance, you might need to make configuration changes to the following resources:

Resource	Task	Description
Networks	1. Add the network.	<ul style="list-style-type: none"> Adding a network does not require that you take resources offline. For more information about networks, see “Managing networks and network resources” (page 115), the online help for the Networks screen, or the REST API scripting help for networks and network sets.
Logical Interconnect Groups	2. Add the network to an uplink set.	<ul style="list-style-type: none"> When you add a network to an appliance, it is immediately available. However, for a server blade to connect to that network, the network must be included in an uplink set on the logical interconnect for that server blade, and the server profile for the server blade must include a connection to either the network or a network set that includes the network. You can either add the network to an existing uplink set or create a new uplink set for the network. Changing the configuration of an uplink set does not require that you take resources offline. Configuration changes made to a logical interconnect group are not automatically propagated to the member logical interconnects. However, by changing the logical interconnect group, for each logical interconnect, you can update it with a single action. For more information, see “Managing interconnects, logical interconnects, and logical interconnect groups” (page 121), the online help for the Logical Interconnect Groups screen, or the REST API scripting help for logical interconnects and the REST API for the <code>uplink-sets</code> resource.
Logical Interconnects (one or more)	3. Do one of the following: <ul style="list-style-type: none"> Add the network to an uplink set. Update the logical interconnect from the group. 	<ul style="list-style-type: none"> Changing the configuration of an uplink set does not require that you take resources offline. Configuration changes made to a logical interconnect group are not automatically propagated to the member logical interconnects. To update a logical interconnect with changes made to its logical interconnect group, you must do one of the following: <ul style="list-style-type: none"> From the Logical Interconnects screen, select Actions→Update from group Use the REST APIs to reapply the logical interconnect group. When adding a network, updating a logical interconnect from its group does not require that you take resources offline. You can also make changes to a logical interconnect without also changing the logical interconnect group. In this case, you add the network to an uplink set on the logical interconnect. However, the appliance labels the logical interconnect as being inconsistent with its group. For more information, see “Managing interconnects, logical interconnects, and logical interconnect groups” (page 121), the online help for the Logical Interconnects screen, or the REST API scripting help for logical interconnects.
Network Sets	4. (Optional) Add the network to a network set.	

Resource	Task	Description
		<ul style="list-style-type: none"> • Applies to Ethernet networks only. • Adding a network to a network set does not require that you take resources offline. Server profiles that have connections to the network set do not have to be updated when a network is added to the network set. • For more information about network sets, see “Managing networks and network resources” (page 115), the online help for the Network Sets screen, or the REST API scripting help for networks and network sets.
Server Profiles and Server Hardware	<ol style="list-style-type: none"> 5. Power off the server before you edit the server profile. 6. Edit the server profile to add a connection to the network. 7. Power on the server after you apply the server profile. 	<ul style="list-style-type: none"> • If you add the network to a network set, server profiles that have connections to the network set automatically have access to the added network. Server profiles that have connections to the network set do not have to be edited when a network is added to the network set. • If the network is not added to a network set, you must add a connection to the network in all the server profiles you want to connect to the added network. Configuration changes to server profiles require that you apply the server profile to server hardware. The server hardware must be powered off before you can edit a server profile. • Server profiles contain much more configuration information than the connections to networks. For more information about server profiles, see “Managing servers and server profiles” (page 111), the online help for the Server Profiles screen, or the REST API scripting help for server profiles.

11 Quick Start: Adding an enclosure and connecting its server blades to networks

This quick start describes the process to add an enclosure to an existing appliance environment and enable the server blades to access the existing data center networks.

The steps you take to add an enclosure and ensure that its server blades are connected to the data center networks depend on whether you use an existing enclosure group, or if you need to define the network connectivity by configuring enclosure groups, and logical interconnects and their uplink sets.

For a server blade in an enclosure to connect to a data center network, you must ensure that several resources are configured. For a complete list of resources and the reasons you need them, see [“Checklist: connecting a server blade to a data center network” \(page 99\)](#).

Logical interconnect groups, their uplink sets, and their associated enclosure groups can be created in different ways:

- You can create them before the enclosure is added to the appliance.
- You can create them as part of the enclosure add operation. During the enclosure add operation, the appliance detects the interconnects installed in the enclosure and creates the groups based on the hardware in the enclosure. You complete the configuration of the groups before you complete the enclosure add operation.

11.1 Checklist: connecting a server blade to a data center network

Connecting a server blade to a data center network requires the following resources:

- Enclosure group
- Enclosure
- Logical interconnect group
- Logical interconnect
- Uplink set
- Network or network set
- Server profile assigned to server hardware

The following table describes the configuration elements required for a server blade to connect to a data center network.

Configuration requirement	Why you need it
Enclosure must specify a logical interconnect group	The logical interconnect group defines the standard configurations to be used for the interconnect modules in the enclosure.
Logical interconnect group must have at least one uplink set	The uplink set determines which data center networks are permitted to send traffic over which physical uplink ports.
Uplink set must include at least one network	The uplink sets defines the networks that are to be accessible from this logical interconnect.
Uplink set must include at least one uplink port	The uplink set defines which hardware ports can accept traffic from which networks.
Server profile must be assigned to server hardware	The server hardware provides the physical connections to at least one interconnect that is part of the logical interconnect.

Configuration requirement	Why you need it
Server profile must have at least one connection, which must specify a network or network set	You do not have to know the hardware configuration, but you do have to choose an available network or network set to specify which networks the server is to use.
If you specify a network set in a server profile connection, the network set must include at least 1 network	You can think of a network set as an alias through which you can refer to many different networks. If a network set contains no networks, a connection to that network set does not result in a connection to any networks.

11.2 Scenario 1: Adding the enclosure to an existing enclosure group

The quickest way to add an enclosure to an appliance is to specify an existing enclosure group. When you add an enclosure to an existing enclosure group, the enclosure is configured like the other enclosures in the group, including the network connections.

Prerequisites

- Minimum required privileges: Infrastructure administrator or Server administrator.
- The hardware configuration of the enclosure interconnects must match the configuration expected by the logical interconnect group that is associated with the enclosure group.
- The uplink sets for the logical interconnect group includes connections to the networks you want to access.
- All data center switch ports that connect to the VC (Virtual Connect) interconnect modules are configured as described in [“Data center switch port requirements” \(page 115\)](#).
- The networks and network sets, if any, have been added to the appliance. To add networks or network sets, see [“Quick Start: Adding a network to an existing appliance environment” \(page 95\)](#) or [“Managing networks and network resources” \(page 115\)](#).
- See [“Prerequisites for bringing an enclosure under management” \(page 131\)](#) for prerequisites and preparation you must complete before you add an enclosure.
- See [“Prerequisites for bringing server hardware under management” \(page 112\)](#) for prerequisites and preparation you must complete before you add a server.

Process

Resource	Task	Description
Enclosures	1. Add the enclosure.	<ul style="list-style-type: none">• When you add the enclosure, specify an existing enclosure group.• When you add an enclosure, you also must select a firmware baseline and a licensing option.• For more information about enclosures, see “Managing enclosures and enclosure groups” (page 131), the online help for the Enclosures screen, or the REST API scripting help for enclosures.
Server Profiles	<p>2. Do one of the following:</p> <ul style="list-style-type: none">• Create a server profile and assign it to the server hardware.• Copy a server profile and assign it to the server hardware, then modify it as necessary. <p>3. Power on the server hardware.</p>	<p>For a server blade to connect to a data center network, it must have a server profile assigned to it, and that server profile must include a connection to either the network or a network set that includes the network:</p> <ul style="list-style-type: none">• If there is an existing server profile that matches how you want the server hardware configured, you can copy that server profile and assign it to the server hardware.• Otherwise, you must create or copy and modify a server profile that includes at least one connection to the network or a network set that contains the network.• Server profiles contain much more configuration information than the connections to networks. For more information about server profiles, see “Managing servers and server profiles” (page 111), the online help for the Server Profiles screen, or the REST API scripting help for server profiles.

11.3 Scenario 2: Defining network connectivity before the enclosure is added

In this scenario, you configure the logical interconnect group, including its uplink sets, and the enclosure group before you add the enclosure. After you define those configurations, the process is the same as adding an enclosure to an existing enclosure group.

For a step-by-step illustrated example of this scenario, see [“Provisioning eight host servers for VMware vSphere Auto Deploy” \(page 238\)](#).

Prerequisites

- Minimum required privileges: Infrastructure administrator or Server administrator.
- The hardware configuration of the enclosure interconnects must match the configuration expected by the logical interconnect group that you create.
- All data center switch ports that connect to the VC (Virtual Connect) interconnect modules are configured as described in [“Data center switch port requirements” \(page 115\)](#).
- The networks and network sets, if any, have been added to the appliance. To add networks or network sets, see [“Quick Start: Adding a network to an existing appliance environment” \(page 95\)](#) or [“Managing networks and network resources” \(page 115\)](#).
- See [“Prerequisites for bringing an enclosure under management” \(page 131\)](#) for prerequisites and preparation you must complete before you add an enclosure.
- See [“Prerequisites for bringing server hardware under management” \(page 112\)](#) for prerequisites and preparation you must complete before you add a server.

Process

Resource	Task	Description
Logical Interconnect Groups	1. Create a logical interconnect group.	<ul style="list-style-type: none"> You must create a logical interconnect group before you can create an enclosure group. You add uplink sets as part of creating a logical interconnect group. Ensure that at least one of the uplink sets you add includes an uplink port to the data center networks you want to access. For more information about logical interconnect groups, see “Managing interconnects, logical interconnects, and logical interconnect groups” (page 121), the online help for the Logical Interconnect Groups screen, or the REST API scripting help for logical interconnect groups.
Enclosure Groups	2. Create an enclosure group.	<ul style="list-style-type: none"> You must create a logical interconnect group before you can create an enclosure group. You cannot create an enclosure group that does not specify a logical interconnect group. For more information about enclosure groups, see “Managing enclosures and enclosure groups” (page 131), the online help for the Enclosure Groups screen, or the REST API scripting help for enclosure groups.
Enclosures	3. Add the enclosure.	<ul style="list-style-type: none"> When you add the enclosure, specify the enclosure group you created. When you add an enclosure, you also must select a firmware baseline and a licensing option. For more information about enclosures, see “Managing enclosures and enclosure groups” (page 131), the online help for the Enclosures screen, or the REST API scripting help for enclosures.
Server Profiles and Server Hardware	4. Do one of the following: <ul style="list-style-type: none"> Create a server profile and assign it to the server hardware. Copy a server profile and assign it to the server hardware, then edit the server profile as necessary. 5. Power on the server hardware.	<p>For a server blade to connect to a data center network, it must have a server profile assigned to it, and that server profile must include a connection to either the network or a network set that includes the network:</p> <ul style="list-style-type: none"> If there is an existing server profile that matches how you want the server hardware configured, you can copy that server profile and assign it to the server hardware. Otherwise, you must create or copy and modify a server profile that includes at least one connection to the network or a network set that contains the network. Server profiles contain much more configuration information than the connections to networks. For more information about server profiles, see “Managing servers and server profiles” (page 111), the online help for the Server Profiles screen, or the REST API scripting help for server profiles.

11.4 Scenario 3: Defining network connectivity as you add the enclosure

In this scenario, you configure the logical interconnect group, including its uplink sets, and the enclosure group during the enclosure add operation. The appliance detects the interconnects installed in the enclosure and prompts you to create a logical interconnect group and enclosure group based on the hardware in the enclosure.

For a step-by-step illustrated example of this scenario, see [“Configuring a server blade to boot from the attached HP 3PAR Storage System” \(page 256\)](#).

Prerequisites

- Minimum required privileges: Infrastructure administrator or Server administrator.
- All data center switch ports that connect to the VC (Virtual Connect) interconnect modules are configured as described in [“Data center switch port requirements” \(page 115\)](#).

- The networks and network sets, if any, have been added to the appliance. To add networks or network sets, see [“Quick Start: Adding a network to an existing appliance environment”](#) (page 95) or [“Managing networks and network resources”](#) (page 115).
- See [“Prerequisites for bringing an enclosure under management”](#) (page 131) for prerequisites and preparation you must complete before you add an enclosure.
- See [“Prerequisites for bringing server hardware under management”](#) (page 112) for prerequisites and preparation you must complete before you add a server.

Process

Resource	Task	Description
Enclosures	1. Add the enclosure.	<ul style="list-style-type: none"> • When you add the enclosure, select Create new enclosure group. • When you add an enclosure, you also must select a firmware baseline and a licensing option. • For more information about enclosures, see “Managing enclosures and enclosure groups” (page 131), the online help for the Enclosures screen, or the REST API scripting help for enclosures.
Enclosure Groups	2. Enter a name for the new enclosure group.	<ul style="list-style-type: none"> • During the enclosure add operation, the appliance prompts you to enter an enclosure group name.
Logical Interconnect Groups	3. Select Create new logical interconnect group . 4. Edit the default logical interconnect group.	<ul style="list-style-type: none"> • During the enclosure add operation, select Create new logical interconnect group. After you click Add, the appliance discovers the interconnects in the enclosure, creates a default logical interconnect group, and opens an edit screen for that logical interconnect group. • The default logical interconnect group name is the enclosure group name you entered followed by <code>interconnect group</code>. For example, if you specified <code>DirectAttachGroup</code> for the enclosure group name, the default logical interconnect group name is <code>DirectAttachGroup interconnect group</code>. • You add uplink sets as part of editing the logical interconnect group. Ensure that at least one of the uplink sets you add includes an uplink port to the data center networks you want to access. • For more information about logical interconnect groups, see “Managing interconnects, logical interconnects, and logical interconnect groups” (page 121), the online help for the Logical Interconnect Groups screen, or the REST API scripting help for logical interconnect groups.
Server Profiles and Server Hardware	5. Do one of the following: <ul style="list-style-type: none"> • Create a server profile and assign it to the server hardware. • Copy a server profile and assign it to the server hardware, then edit the server profile as necessary. 6. Power on the server hardware.	<p>For a server blade to connect to a data center network, it must have a server profile assigned to it, and that server profile must include a connection to either the network or a network set that includes the network:</p> <ul style="list-style-type: none"> • If there is an existing server profile that matches how you want the server hardware configured, you can copy that server profile and assign it to the server hardware. • Otherwise, you must create or copy and modify a server profile that includes at least one connection to the network or a network set that contains the network. • Server profiles contain much more configuration information than the connections to networks. For more information about server profiles, see “Managing servers and server profiles” (page 111), the online help for the Server Profiles screen, or the REST API scripting help for server profiles.

12 Quick Start: Configuring an enclosure and server blade for Direct attach to an HP 3PAR Storage System

This quick start describes the process for adding and configuring an enclosure so that its servers can connect to an HP 3PAR Storage System that is directly attached to the enclosure.

For a step-by-step illustrated example of this scenario (except that configuring the enclosure group and logical interconnect occurs during the enclosure add operation), see [“Configuring a server blade to boot from the attached HP 3PAR Storage System”](#) (page 256).

Prerequisites

- Minimum required privileges: Infrastructure administrator or Network administrator for adding the networks.
- Minimum required privileges: Infrastructure administrator or Server administrator for adding the enclosure and server profiles.
- The HP 3PAR Storage System is installed and configured and the cables are attached to the enclosure you want to use.
- See [“Prerequisites for bringing an enclosure under management”](#) (page 131) for prerequisites and preparation you must complete before you add an enclosure.
- See [“Prerequisites for bringing server hardware under management”](#) (page 112) for prerequisites and preparation you must complete before you add a server.

Process

Resource	Task	Description
Networks	1. Add the Fibre Channel Direct attach networks.	<ul style="list-style-type: none"> If you add the networks from the Networks screen: <ul style="list-style-type: none"> For Type, select <code>Fibre Channel</code> For Fabric type, select <code>Direct attach</code> For more information about networks, see “Managing networks and network resources” (page 115), the online help for the Networks screen, or the REST API scripting help for networks and network sets.
Logical Interconnect Groups	2. Create a logical interconnect group that defines the uplink sets for the Direct attach network connections.	<ul style="list-style-type: none"> Choose a name for the logical interconnect group that helps you distinguish logical interconnect groups that have connections to Direct attach Fibre Channel networks from other logical interconnect groups. You add uplink sets as part of creating the logical interconnect group. Ensure that the uplink sets use the uplink ports on the enclosure that are physically connected to the HP 3PAR Storage Server. For more information about logical interconnect groups, see “Managing interconnects, logical interconnects, and logical interconnect groups” (page 121), the online help for the Logical Interconnect Groups screen, or the REST API scripting help for logical interconnect groups.
Enclosure Groups	3. Create an enclosure group.	<ul style="list-style-type: none"> Choose a name that helps you distinguish enclosures that use Direct attach Fibre Channel connections from enclosures that use Fabric attach Fibre Channel connections.
Enclosures	4. Add the enclosure.	<ul style="list-style-type: none"> When you add the enclosure, select the enclosure group that you added in the preceding step. When you add an enclosure, you also must select a firmware baseline and a licensing option. For more information about enclosures, see “Managing enclosures and enclosure groups” (page 131), the online help for the Enclosures screen, or the REST API scripting help for enclosures.
Server Profiles	5. Do one of the following: <ul style="list-style-type: none"> Create a server profile and assign it to the server hardware. Copy a server profile, edit it as necessary, and then assign it to the server hardware. 	<ul style="list-style-type: none"> For a server blade to connect to the HP 3PAR Storage System, it must have a server profile assigned to it, and that server profile must include at least one connection to the Direct attach Fibre Channel network that connects to the storage system. For example, if the networks you added are <code>FlatSAN A</code> and <code>FlatSAN B</code>, ensure that the server profile has one connection to the <code>FlatSAN A</code> network and one connection to the <code>FlatSAN B</code> network. Server profiles contain much more configuration information than the connections to networks. For more information about server profiles, see “Managing servers and server profiles” (page 111), the online help for the Server Profiles screen, or the REST API scripting help for server profiles.
Server Profiles	6. Collect the WWPN for the Direct attach Fibre Channel connections the server profile you created in the preceding step. 7. After you configure the HP 3PAR Storage System, power on the server hardware.	<ul style="list-style-type: none"> For example, for each server profile, record the WWPN for the <code>FlatSAN A</code> and <code>FlatSAN B</code> Fibre Channel connections. For more information about server profiles, see “Managing servers and server profiles” (page 111), the online help for the Server Profiles screen, or the REST API scripting help for server profiles. You use these WWPNs when you configure the HP 3PAR Storage System. For more information about configuring the HP 3PAR Storage System, see the documentation for that storage system.

13 Quick Start: Adding an HP ProLiant DL rack mount server

This quick start describes the process for adding a rack mount server.

The features supported by the appliance vary by server model. For information about the features supported for HP ProLiant DL servers, see [“Server hardware features supported by the appliance” \(page 111\)](#).

For an illustrated example of this task, see [“Step by step: Configuring an example data center using HP OneView” \(page 231\)](#).

Prerequisites

- Minimum required privileges: Infrastructure administrator or Server administrator.
- The server is connected to a live power source.
- See [“Prerequisites for bringing server hardware under management” \(page 112\)](#) for prerequisites and preparation you must complete before you add a server.

Process

Resource	Task	Description
Server Hardware	<ol style="list-style-type: none">1. Add the server using the Server Hardware screen or the REST APIs for the <code>server-hardware</code> resource.2. Power on the server.	<ul style="list-style-type: none">• When you add a server, you must provide the following information:<ul style="list-style-type: none">◦ The iLO IP address or host name◦ The user name and password for an iLO account with administrator privileges.◦ A license type to use for the server hardware. <p>For more information about server hardware, see “Managing servers and server profiles” (page 111), the online help for the Server Hardware screen, or the REST API scripting help for server hardware.</p> <ul style="list-style-type: none">• If this server configuration differs from the other servers in the appliance, the appliance automatically adds a server hardware type for this model.• Because this is a rack mount server:<ul style="list-style-type: none">◦ You cannot use this appliance to provision any networks for this server.◦ Server profiles are not supported.◦ The features supported by the appliance vary by server model. For information about the features supported for HP ProLiant DL servers, see “Server hardware features supported by the appliance” (page 111).

Part IV Configuration and management

The chapters in this part describe the configuration and management tasks for the appliance and the resources it manages.

14 Managing servers and server profiles

Managing servers with the appliance involves interacting with several different resources on the appliance:

- A server profile captures the entire server configuration in one place, enabling you to consistently replicate new server profiles and to rapidly modify them to reflect changes in your data center environment.
- A server profile enables management of your server hardware.
- An instance of server hardware is a physical server, such as an HP ProLiant BL460c Gen8 Server Blade, installed in an enclosure or an HP ProLiant DL380p rack mount server.
- A server hardware type defines the characteristics of a specific server model and set of hardware options, such as mezzanine cards.
- A connection, which is associated with a server profile, connects a server to the data center networks.

Server profiles provide most of the management features for servers, but server hardware and server profiles are independent of each other:

- A physical server, which is an instance of server hardware, might or might not have a server profile assigned to it.
- A server profile might be assigned to one instance of server hardware, or no server hardware at all.

It is the combination of the server hardware and the server profile assigned to it that is the complete server in the appliance.

You must use the server hardware resource to add physical servers to the appliance when you install a rack mount server. Server blades are added to the appliance automatically when you add an enclosure or install a server blade in an existing enclosure.

UI screens and REST API resources

UI screen	REST API resource
Server Profiles	server-profiles and connections
Server Hardware	server-hardware
Server Hardware Types	server-hardware-types

14.1 Server hardware features supported by the appliance

Feature	HP ProLiant BL G7 ¹	HP ProLiant BL Gen8	HP ProLiant DL Gen8 ²
Power on or power off the server	✓	✓	✓
View inventory data	✓	✓	✓
Monitor power, cooling, and utilization	✓	✓	✓
Monitor health and alerts	Only with manual installation of SNMP Agents	✓	✓
Launch iLO remote console	✓	✓	✓

Feature	HP ProLiant BL G7 ¹	HP ProLiant BL Gen8	HP ProLiant DL Gen8 ²
SSO (single sign-on): The appliance enables SSO to iLO and OA without storing user-created iLO or OA credentials.	✓	✓	✓
Automatic firmware upgrade (iLO) to minimum supported version when added to the appliance	✓	✓	✓
Automatic rack visualization and editing	✓	✓	✓
Manual rack visualization and editing			✓
Automatic discovery of server hardware type	✓	✓	✓
Server profile features			
Edit BIOS Settings		✓	
Firmware management		✓	
Connections to networks	✓	✓	

¹ The appliance might report an unsupported status for some double-wide, double-dense ProLiant G7 blade servers models, which means that the appliance cannot manage them.

² Not every model of HP ProLiant DL rack server supports every feature listed in this table.

14.2 Prerequisites for bringing server hardware under management

Server hardware must meet the following prerequisites in order for the appliance to manage it:

Prerequisites

Item	Requirement
Server hardware model	The server hardware must be a supported model listed in the <i>HP OneView Support Matrix</i> . The server hardware is connected to a live power source.
iLO firmware	The iLO3 and iLO4 (Integrated Lights-Out) firmware version must meet the minimum requirement listed in the <i>HP OneView Support Matrix</i> . NOTE: Rack mount ProLiant DL G7 iLO3 server hardware is not supported.
IP addresses	IPv4 configuration is required. iLOs on rack mount server hardware must have an IP address.
Local user accounts	iLOs must be configured to allow for local user accounts. As part of bringing an iLO under management, a local user account is added to the iLO, so it must be configured to work with local accounts.

14.3 Roles

- Minimum required privileges: Infrastructure administrator or Server administrator

14.4 Tasks for server profiles

The appliance online help provides information about using the UI or the REST APIs to:

- Get information about (read) a server profile.
- Create and apply a server profile.
- Specify identifiers and addresses when creating a server profile and adding connections.
- Connect the server to data center networks by adding a connection to a server profile.
- Edit the BIOS settings of a server profile.

- Manage the boot order of a server profile.
- Manage virtual or physical IDs for the server hardware.
- Copy a server profile.
- Delete a server profile.
- Edit a server profile.
- Move a server profile to another server.
- Power on and off the server hardware to which the server profile is assigned.
- Install a firmware bundle using a server profile.

NOTE: Firmware will not be downgraded to the selected firmware baseline when applying a server profile. Use an external tool, for example HP SUM, to force firmware downgrades or rewrites.

- View activities (tasks and alerts).

14.5 Tasks for server hardware

The appliance online help provides information about using the UI or the REST APIs to:

- Get information about (read) the server hardware.
- Power on a server.
- Power off a server.
- Reset a server.
- Launch the iLO remote console to manage servers remotely.
- Add a rack mount server.
- Add a server blade to an existing enclosure.
- Claim a server currently being managed by another appliance.
- Remove a server from management.
- Remove a server blade from an existing enclosure.
- Refresh the connection between the appliance and the server hardware.
- View activities (tasks and alerts).

14.6 Tasks for server hardware types

The appliance online help provides information about using the UI or the REST APIs to:

- Edit the name or description of the server hardware type.
- Delete a server hardware type from an appliance that no longer includes any servers of that type.

14.7 Effects of managing server hardware iLOs

When server hardware is being managed by the appliance, the effect to the server hardware iLO is:

- A management account is created.
- SNMP is enabled and the appliance is added as an SNMP trap destination.

NOTE: Health monitoring is not enabled on ProLiant G7 iLO3 server hardware until the HP management agents are installed on the OS and the [SNMP service is configured](#) with the same SNMP read community string shown on the **Settings** screen.

- NTP is enabled and the appliance becomes the server hardware's NTP time source.
- An appliance certificate is installed to enable single sign-on operations.
- iLO firmware is updated to the minimum versions listed in the *HP OneView Support Matrix*.
- The iLO time zone is set to Atlantic/Reykjavik as recommended by the iLO documentation.

The time zone setting determines how the iLO adjusts UTC time to obtain the local time and how it adjusts for daylight savings time (summer time). For the entries in the iLO event log and IML to display the correct local time, you must specify the time zone in which the server is located.

If you want iLO to use the time provided by the SNTP server, without adjustment, configure the iLO to use a time zone that does not apply an adjustment to UTC time. In addition, that time zone must not apply a daylight saving time (summer time) adjustment.

There are several time zones that fit this requirement. One example is the Atlantic/Reykjavik time zone. This time zone is neither east nor west of the prime meridian and time does not change in the Spring or Fall.

14.8 Learning more

- [“Understanding the resource model” \(page 29\)](#)
- [“About enclosures” \(page 132\)](#)
- [“Managing licenses” \(page 158\)](#)
- [“Troubleshooting server hardware” \(page 213\)](#)
- [“Troubleshooting server profiles” \(page 215\)](#)

15 Managing networks and network resources

This chapter describes configuring and managing networks and network resources for the enclosures and server blades managed by the appliance. For information about configuring the network settings for the appliance, see [“Managing the appliance settings” \(page 155\)](#).

NOTE: The network features described in this chapter apply to enclosures and server blades only. The appliance does not monitor or manage the network features and hardware for rack mount servers or for networking equipment outside the enclosures.

For more information about the network features and the appliance, see [“About network connectivity” \(page 116\)](#).

UI screens and REST API resources

UI screen	REST API resource
Interconnects	interconnects
Networks	connection-templates, ethernet-networks, and fc-networks
Network Sets	network-sets

15.1 Data center switch port requirements

Although you can configure an uplink set to receive incoming network traffic as untagged by designating a network on in that uplink set as `Native`, traffic egressing the uplink set is always VLAN tagged.

The switch ports for data center network switches that connect to the Virtual Connect interconnect modules must be configured as follows:

- Spanning tree edge (because the Virtual Connect interconnect modules appear to the switch as access devices instead of switches).
- VLAN trunk ports (tagging) to support the VLAN IDs included in the uplink set that connects to switch port.

For example, if you configure an uplink set, `prodUS`, that includes the production networks `prod 1101` through `prod 1104` to use the X2 ports of the interconnects in bay 1 and bay 2 of Enclosure 1, then the data center switch ports that connect to those X2 ports must be configured to support VLAN IDs 1101, 1102, 1103, and 1104.

- If multiple uplinks in an uplink set connect the same interconnect to the same data center switch, to ensure that all the uplinks in the uplink set are active, you must configure the data center switch ports for LACP (Link Aggregation Control Protocol) in the same LAG (Link Aggregation Group).

15.2 Managing Fibre Channel networks (SANs)

You can manage Fibre Channel networks from the UI **Networks** screen or by using the REST APIs.

15.2.1 Roles

- Minimum required privileges: Infrastructure administrator or Network administrator

15.2.2 Tasks

The appliance online help provides information about using the UI or the REST APIs to:

- Add a Fibre Channel SAN.
- Delete a Fibre Channel SAN.
- Edit a Fibre Channel SAN configuration.

15.3 Managing Ethernet networks

When you add an Ethernet network to the appliance, you are adding a VLAN to the configuration. VLANs allow multiple networks to use the same physical connections. Servers can specify networks without knowledge of the underlying hardware configuration.

When you add an Ethernet network, you might also want to add it to an existing network set or add it to a new network set. For example, by adding the Ethernet network to an existing network set, all servers that have connections to the network set can access the added network without requiring you to change the server profiles.

For Ethernet connections, a logical uplink is a way to identify interconnect module uplinks that carry multiple networks over the same cable. When you add a network, you must also add it to an existing uplink set or a new uplink set.

You can manage networks and network sets from the UI **Networks** and **Network Sets** screens or by using the REST APIs.

-
- ❗ **IMPORTANT:** HP recommends that you back up the appliance after you make configuration changes to networks. For information about backing up the appliance, see [“Backing up an appliance” \(page 149\)](#).
-

15.3.1 Roles

- Minimum required privileges: Infrastructure administrator or Network administrator

15.3.2 Tasks

The appliance online help provides information about using the UI or the REST APIs to:

- Add a network.
- Edit a network (change a network configuration).
- Delete a network.
- Add a network set.
- Edit a network set.
- Delete a network set.

15.4 About network connectivity

The network connectivity features of the appliance are designed to separate the logical resources from the physical hardware, allowing you to add or change the physical components without

having to replicate configuration changes across multiple servers. In addition, the logical and physical network resources can be configured for high availability, including:

- Providing redundant physical links to the data center networks
- Configuring stacking links between interconnects in an enclosure to provide redundant paths from servers to data center networks
- Using logical resources, such as logical interconnects, that represent multiple physical resources to allow continued uninterrupted operation if a physical component fails

The Virtual Connect interconnect modules in enclosures support the following types of networks:

- Fibre Channel for storage networks, including both Fabric attach (SAN) Fibre Channel connections and Direct attach (Flat SAN) Fibre Channel connections
- Ethernet for data networks

15.4.1 About Fibre Channel networks

You can use Fibre Channel networks to connect to storage devices.

15.4.1.1 Fibre Channel network types

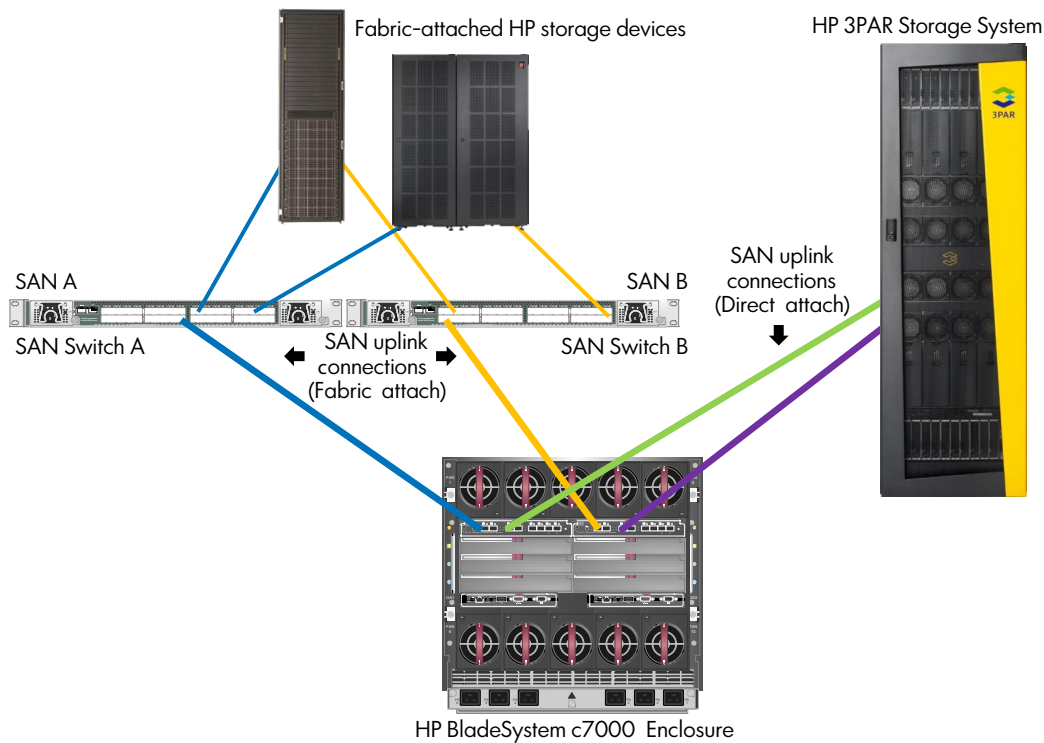
The Virtual Connect interconnect modules in enclosures support two types of Fibre Channel connections to storage devices:

- Fabric attach connections—The enclosure interconnects connect to data center SAN fabric switches.
- Direct attach connections—Also called Flat SAN, in which the enclosure interconnects connect directly to a supported storage device, such as an HP 3PAR StoreServ Storage system.

You cannot change the type of a Fibre Channel network, but you can delete the network from the appliance, and then add the network as a different type.

A logical interconnect can use both Direct attach storage and Fabric attach storage at the same time.

Figure 11 Direct attach and Fabric attach Fibre Channel networks



15.4.1.2 Fabric attach Fibre Channel networks

SAN infrastructures typically use a Fibre Channel switching solution involving several SAN switches that implement NPIV (N-Port ID Virtualization) technology. NPIV uses N-ports and F-ports to build a Fibre Channel SAN fabric. NPIV enables multiple N_Ports to connect to a switch through a single F_Port, so that a virtual server can share a single physical port with other servers, but access only its associated storage on the SAN.

When you configure a Fabric attach Fibre Channel network, the port you choose for the uplink from the enclosure interconnect to the storage SAN must support NPIV (N_Port ID Virtualization).

15.4.1.3 Direct attach Fibre Channel networks

The Direct attach Fibre Channel solution, also called the Flat SAN solution, eliminates the need for a connection from the enclosure interconnects to a Fibre Channel SAN switch. This means you can connect the enclosure interconnects directly to the storage system. The port you choose for the uplink from the enclosure interconnect to the storage system must support NPIV.

Servers connecting to a Direct attach Fibre Channel network have access to all devices connected on the uplink ports defined for that network. If there is more than one connection from a FlexFabric module to the storage system, each server can access as many paths to the storage LUN (logical unit number) as there are connections to the storage system.

For Direct attach Fibre Channel networks, the enclosure interconnect does not distribute server logins evenly across uplink ports. Server login-balancing and login-distribution do not apply to Fibre Channel networks.

- ❗ **IMPORTANT:** When you move a server profile to a different enclosure, and the profile is configured to boot from a Direct attach storage device, you must manually update the boot connection of the profile to specify the WWPN (World Wide Port Name) used for the storage device that is directly attached to the enclosure.

Each enclosure connects to a different port of the Direct attach storage device, so the WWPN for that storage device is different for each enclosure. If you do not specify the correct WWPN and LUN for the storage device, the server will not boot successfully from the boot target.

15.4.1.4 Fibre Channel networks and FCoE

Servers connect to the enclosure interconnect downlinks using FCoE (Fibre Channel over Ethernet), and uplink to SANs and Direct attach storage systems using Fibre Channel. The interconnects automatically handle the routing between the server blades and the Fibre Channel networks, so you do not need to specify a VLAN ID for a Fibre Channel network.

15.4.2 About Ethernet networks

You use Ethernet networks for data networks.

Ethernet networks and network sets

You can assign multiple Ethernet networks to a named group called a network set. Later, when you add a connection in a server profile, you can select this network set to enable multiple networks to be selected for that single connection. For information about network sets, see the online help for the **Network Sets** screen.

15.4.2.1 Ethernet networks and VLAN IDs

When you add an Ethernet network to the appliance, you are adding a VLAN (virtual local area network) to the configuration. VLANs allow multiple networks to use the same physical connections. server profiles can specify networks without knowledge of the hardware configuration of the data center network.

When defined on this appliance, Ethernet networks connected to enclosure interconnects require a VLAN ID.

15.4.3 About network sets

A network set is a collection of Ethernet networks that form a named group to simplify server profile creation. Network sets are useful in ESXi environments where each server profile connection needs to access multiple networks. Network sets define how packets will be delivered to the server when a server Ethernet connection is associated with the network set. Network sets also enable you to define a VLAN trunk and associate it with a server connection.

Instead of assigning a single network to a connection in a server profile, you can assign a network set to that connection.

- Using network sets, you can quickly deploy changes to the network environment to multiple servers. For example, you have 16 servers connected to a network set. To add a new network to all 16 servers, you only need to add it to the network set instead of each server individually.
- You can create a network set for your production networks and one for your development networks.
- You can configure a hypervisor with a vSwitch to access multiple VLANs by creating a network set as a trunk that includes these networks.

Network set details

- Network sets are supported for use in server profiles only.
- All networks in a network set must be Ethernet networks.
- All networks in a network set must be configured in the same appliance.
- A network can be a member of multiple network sets.
- When a network is deleted, it is automatically deleted from all network sets to which it belonged.
- A network set can be empty (contain no networks) or can contain one or more of the networks configured in the appliance. Empty network sets enable you to create network sets in the configuration before you create the member networks, or to remove all of the member networks before you add their replacements. However, if a server profile adds a connection to an empty network set, the server cannot connect to any data center networks using that connection.
- When you create or modify a network set, you can designate a network for untagged packets. If you do not designate a network an untagged network, untagged packets are rejected.
- Server traffic must be tagged with the VLAN ID of one of the Ethernet networks in the network set. Untagged server traffic is either sent to the untagged network (if an untagged network is defined) or is rejected (if no untagged network is defined).
- The untagged network can send tagged and untagged traffic between the server and the interconnect simultaneously.
- When you create or modify a network set, you define the maximum bandwidth and the preferred bandwidth for connections to that network set. A server profile can override the preferred bandwidth but not the maximum bandwidth.
- When you delete a network set, the networks that belong to the network set are not affected. However, any servers with a connection to that network set are affected because their connections are defined as being to the network set and not to the individual networks. Because the network set is no longer available, the network traffic to and from that server through that connection is stopped. When you delete a network set, any server profile connections that specified that network set become undefined.

15.5 Learning more

- [“Managing interconnects, logical interconnects, and logical interconnect groups” \(page 121\)](#)
- [“Managing the appliance settings” \(page 155\)](#)

16 Managing interconnects, logical interconnects, and logical interconnect groups

A logical interconnect group acts as a recipe for creating a logical interconnect representing the available networks, uplink sets, stacking links, and interconnect settings for a set of physical interconnects in a single enclosure.

UI screens and REST API resources

UI screen	REST API resource
Interconnects	interconnects
Logical Interconnects	logical-interconnects
Logical Interconnect Groups	logical-interconnect-groups

16.1 Managing enclosure interconnect hardware

When you add an enclosure, any interconnects in the enclosure are also added to the management domain, and they remain in the domain as long as the enclosure is part of the domain. You can manage enclosure interconnect hardware from the UI **Interconnects** screen or by using the REST APIs.

16.1.1 Roles

- Minimum required privileges: Infrastructure administrator or Network administrator

16.1.2 Tasks

The appliance online help provides information about using the UI or the REST APIs to:

- Enable or disable uplink ports or downlink ports.
- Add a physical interconnect.
- View data transfer statistics for uplink and downlink ports.
- Clear port counters.
- Replace a physical interconnect.
- Reapply an interconnect configuration.

16.1.3 About interconnects

Interconnects enable communication between the server hardware in the enclosure and the data center networks. An interconnect has several types of links:

Uplinks	Uplinks are physical ports that connect the interconnect to the data center networks.
Downlinks	Downlinks connect the interconnect to the server hardware through the enclosure midplane.
Stacking links	Stacking links, which can be internal or external, connect interconnects together to provide redundant paths for Ethernet traffic from server blades to the data center networks.

Interconnects are added automatically when the enclosure that contains them is added to the appliance.

Interconnects are an integral part of an enclosure, and each interconnect is a member of a logical interconnect. Each logical interconnect is associated with a logical interconnect group, which is associated with an enclosure group. For more information about logical interconnects, see [“About logical interconnects” \(page 123\)](#). For information about the relationship that enclosures and enclosure groups have with interconnects, logical interconnects, and logical interconnect groups, see [“Understanding the resource model” \(page 29\)](#).

You can update interconnect firmware using an SPP (Service Pack for ProLiant).

Connectivity and synchronization with the appliance

The appliance monitors the health status of interconnects and issues alerts when there is a change in status of an interconnect or port. The appliance maintains the configuration that you specify on the interconnects that it manages.

The appliance also monitors the connectivity status of interconnects. If the appliance loses connectivity with an interconnect, an alert is displayed until connectivity is restored. The appliance attempts to resolve connectivity issues and clear the alert. If it cannot, you have to resolve the issues and manually refresh the interconnect to synchronize it with the appliance.

You can manually refresh the connection between the appliance and an interconnect from the **Interconnects** screen. See the online help for the **Interconnects** screen to learn more.

About unsupported interconnects

Unsupported hardware is hardware that the appliance cannot manage. If the appliance detects an interconnect that it does not expect or cannot manage, it assigns the interconnect a `critical` health status and displays an alert with a resolution of replacing the interconnect with a model it can manage. The appliance displays the model name of the unsupported interconnect that it obtains from the OA (Onboard Administrator).

If the unsupported interconnect is in an unmanaged bay, the appliance places it into an `inventory` state and creates a resource for it, but does not bring it under management.

NOTE: If you try to create a server profile that has a connection to an unsupported interconnect, the operation will fail.

16.1.4 Learning more

- [“Interconnects” \(page 35\)](#)
- [“Networking features” \(page 27\)](#)

16.2 Managing logical interconnects and logical interconnect groups

A logical interconnect represents the available networks, uplink sets, and stacking links for a set of physical interconnects in a single enclosure. The **Logical Interconnects** screen provides a graphical view of the logical interconnect configuration in an enclosure. Use this screen or the REST APIs to manage the uplink sets for the logical interconnect.

When you add an enclosure, a logical interconnect is created automatically. The logical interconnect group serves as a template to ensure the consistent configuration of all of its logical interconnects.

16.2.1 Roles

- Minimum required privileges: Infrastructure administrator or Network administrator

16.2.2 Tasks

The appliance online help provides information about using the UI or the REST APIs to:

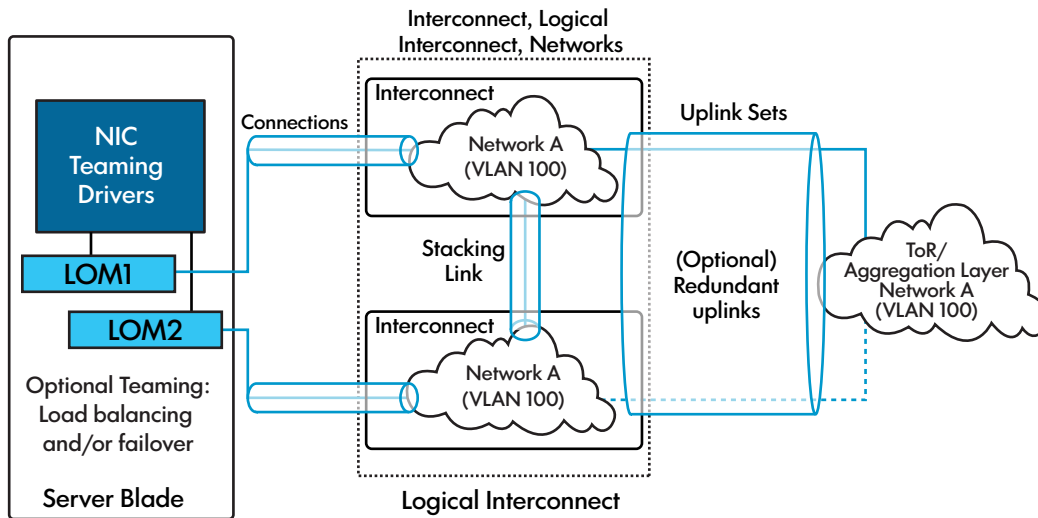
- Update the logical interconnect firmware.
- Add an uplink set.
- Create a logical interconnect support dump file.
- Enable and disable physical ports.
- Manage SNMP (Simple Network Management Protocol) access and trap destinations.
- Reapply the logical interconnect configuration to its physical interconnects.
- Update the logical interconnect configuration from the logical interconnect group.
- Configure a port to monitor network traffic.
- Change Ethernet settings such as:
 - Fast MAC cache failover
 - MAC refresh interval
 - IGMP (Internet Group Management Protocol) snooping
 - IGMP idle timeout interval
 - Loop protection

16.2.3 About logical interconnects

A logical interconnect is a single administrative entity that consists of the configuration for the interconnects in an enclosure, which includes:

- The uplink sets, which connect to data center networks.
- The mapping of networks to physical uplink ports, which is defined by the uplink sets for a logical interconnect.
- The downlink ports, which connect through the enclosure midplane to the servers in the enclosure.
- The connections between interconnects, which are called stacking links. Stacking links can be internal cables (through the enclosure) or external cables between the stacking ports of interconnects.

For a server administrator, a logical interconnect represents the available networks through the interconnect uplinks and the interconnect downlink capabilities through a physical server's interfaces. For a network administrator, a logical interconnect represents an Ethernet stacking domain, aggregation layer connectivity, stacking topology, network reachability, statistics, and troubleshooting tools.



Uplink sets

An uplink set defines a group of networks and physical ports on the interconnect in an enclosure. An uplink set enables you to attach the interconnect to the data center networks. An uplink set enables multiple ports to support port aggregation (multiple ports connected to a single external interconnect) and link failover with a consistent set of VLAN networks.

For Ethernet connections, an uplink set enables you to identify interconnect uplinks that carry multiple networks over the same cable. For Fibre Channel connections, you can only add one network to an uplink set. Fibre Channel does allow virtual networks or VLANs.

An uplink set is part of a logical interconnect. The initial configuration of the uplink sets for a logical interconnect is determined by the configuration of the uplink sets for the logical interconnect group, but you can change (override) the uplink sets for a specific logical interconnect. Changes you make to the uplink sets for a logical interconnect group are not automatically propagated to existing logical interconnects. For example, to propagate a newly added VLAN to a logical interconnect group uplink set to its existing logical interconnects, you must individually update each logical interconnect configuration from the logical interconnect group.

For each logical interconnect:

- You can define zero, one, or multiple uplink sets. If you do not define any uplink sets, the servers in the enclosure cannot connect to data center networks.
- A network can be a member of one uplink set only.
- An uplink set can contain only one Fibre Channel network.
- An uplink set can contain multiple Ethernet networks.
- You must specify Ethernet networks individually. The use of network sets in uplink sets is not supported for the following reasons:
 - The networking configuration is intended to be managed by users with a role of Network administrator. Because users with a role of Server administrator can create and edit network sets, allowing network sets to be members of uplink sets could result in server administrators changing the mapping of networks to uplink ports without the knowledge of the network administrator.
 - Because a network can be a member of more than one network set, allowing network sets to be members of uplink sets would make it more difficult to ensure that no single network is a member of more than one uplink set, especially as the network set configurations change over time.

Stacking modes

Stacking modes and stacking links apply to Ethernet networks only.

Interconnects that are connected to one another through stacking links create a stacking mode. Ethernet traffic from a server connected to an interconnect downlink can reach the data center networks through that interconnect or through a stacking link from that interconnect to another interconnect.

The supported stacking mode is `enclosure`. For this stacking mode:

- All the interconnects in the enclosure form a single logical interconnect.
- Stacking links between interconnects in different enclosures are not supported.
- When two interconnects of the same type are installed in horizontally adjacent enclosure I/O bays, they connect through internal stacking links.
- Installing interconnects of different types in horizontally adjacent enclosure I/O bays is not supported.

Stacking health

The appliance detects the topology within an enclosure of the connections between interconnects and the uplink sets, and determines the redundancy of paths between servers and data center networks. The appliance reports redundancy information as the stacking health of the logical interconnect, which is one of the following:

Redundantly Connected	There are at least two independent paths between any pair of interconnects in the logical interconnect, and there are at least two independent paths from any downlink port on any interconnect in the logical interconnect to any other port (uplink or downlink) in the logical interconnect.
Connected	There is a single path between any pair of interconnects in the logical interconnect, and there is a single path from any downlink port on any interconnect in the logical interconnect to any other port (uplink or downlink) in the logical interconnect.
Disconnected	At least one interconnect is not connected to the other member interconnects in the logical interconnect.

The configuration defined in the logical interconnect group is the expected configuration within the enclosure. If any of the interconnects are defined to be in the `Configured` state but instead are in a different state, such as `Absent`, `Inventory`, or `Unmanaged`, the stacking health is displayed as `Disconnected`. If none of the interconnects are in the `Configured` state, no stacking health information is displayed.

Adding a logical interconnect

Every enclosure belongs to an enclosure group. When you add an enclosure:

- The appliance detects the physical interconnects and their stacking links.
- The appliance automatically creates a single logical interconnect for the enclosure. The configuration of the logical interconnect, including uplink sets, is defined by the logical interconnect group associated with the enclosure group. This ensures that all enclosures in the enclosure group are configured with the same network connectivity.
- The appliance automatically names the logical interconnect when you add the enclosure. The naming convention for logical interconnects follows:

`enclosure_name-LI`

Where `enclosure_name` is the name of the enclosure.

Deleting a logical interconnect

To delete a logical interconnect, you must remove the enclosure from management.

16.2.4 About logical interconnect groups

A logical interconnect group is associated with an enclosure group and is used to define the logical interconnect configuration for every enclosure that is added to that enclosure group. Logical interconnect configurations include the I/O bay occupancy, stacking mode, uplink ports and uplink sets, available networks, and downlinks.

The logical interconnect group reserves the appropriate interconnect ports for stacking links required for the stacking mode. For the enclosure stacking mode:

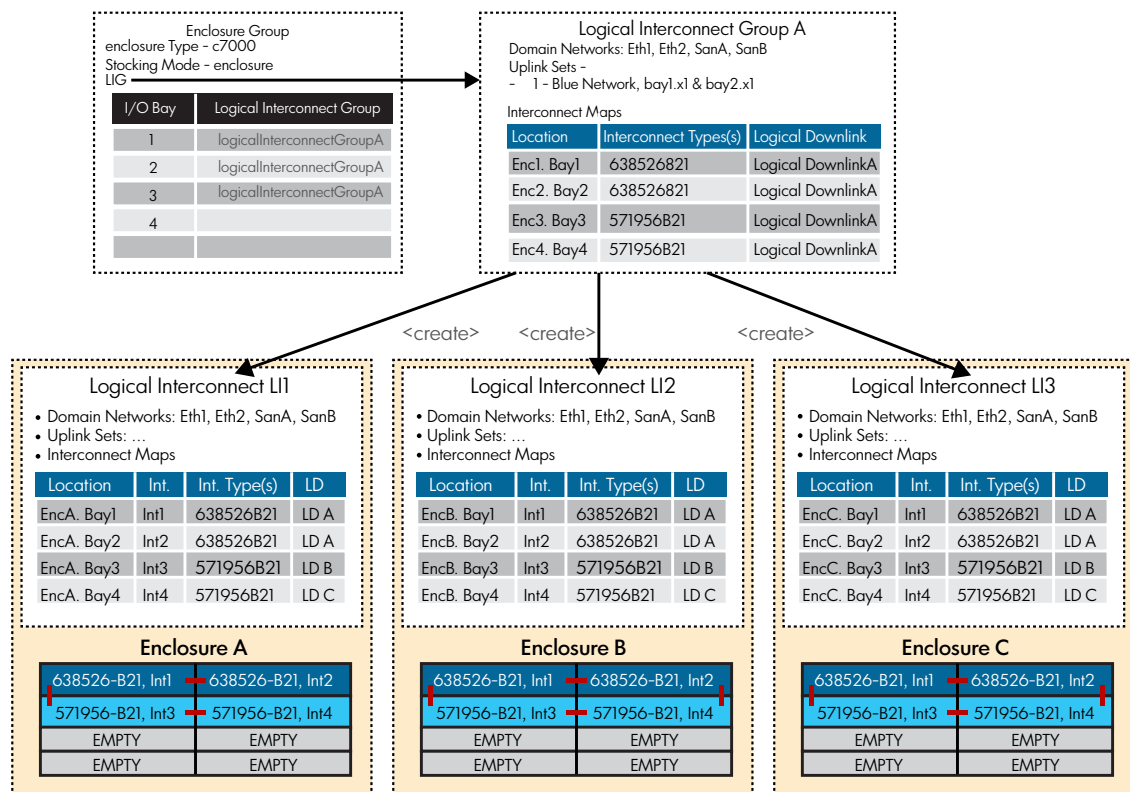
- All interconnects in an enclosure are members of the logical interconnect.
- Horizontally adjacent interconnects must be the same interconnect type.
- Horizontally adjacent interconnects reserve one port per enclosure for internal stacking links, called East-West links.
- Vertically adjacent interconnects reserve an additional port per enclosure for external stacking links, called North-South links.

The uplink sets portion of the logical interconnect group defines the initial configuration for uplink sets for each enclosure added to the enclosure group. You can change the uplink sets for a logical interconnect, and existing enclosures are not affected by changes you make to uplink sets in the logical interconnect group. If you change the uplink sets for an existing logical interconnect group, only enclosures that you add after the configuration change are configured with the new uplink set configuration.

For more information about logical interconnects and the rules for uplink sets, see the online help for the **Logical Interconnects** screen.

When you add an enclosure and assign an enclosure group, the appliance creates a logical interconnect for that enclosure. The logical interconnect it creates matches the configuration specified by the logical interconnect group that is associated with the enclosure group. When the add operation completes, the interconnects are fully configured and the networks are available for use by server profiles.

Figure 12 Relationship of a logical interconnect group to a logical interconnect



You can create a logical interconnect group independently of adding an enclosure, or you can edit the logical interconnect group that the appliance creates when you add the enclosure to the appliance. When you add the first enclosure to the appliance, the preliminary logical interconnect group is based on the physical interconnects in that enclosure and is created with the following properties:

- Existing interconnect types in their existing positions
- All physical uplink ports disabled except for stacking links

You can edit this logical interconnect group, and when the configuration is complete, an enclosure group is created and associated with this logical interconnect group.

If you assign an enclosure group (which includes a logical interconnect group) to an enclosure in which the interconnects installed in the enclosure do not match the logical interconnect group, each interconnect reports its state as *unmanaged*. The physical interconnect configuration in the enclosure must match the logical interconnect group before an interconnect can be managed.

To delete a logical interconnect group, you must delete the associated enclosure group.

16.2.5 About SNMP settings

Network management systems use SNMP (Simple Network Management Protocol) to monitor network-attached devices for conditions that require administrative attention. By configuring settings on the **Logical Interconnect Groups** and **Logical Interconnects** screens, you can enable third-party SNMP managers to monitor (read-only) network status information of the interconnects.

The SNMP manager typically manages a large number of devices, and each device can have a large number of objects. It is impractical for the manager to poll information from every object on every device. Instead, each agent on the managed device notifies the manager without solicitation by sending a message known as an event trap.

The appliance enables you to control the ability of SNMP managers to read values from an interconnect when they query for SNMP information. You can filter the type of SNMP trap to

capture, and then designate the SNMP manager to which traps will be forwarded. By default, SNMP is enabled with no trap destinations set.

When you create a logical interconnect, it inherits the SNMP settings from its logical interconnect group. To customize the SNMP settings at the logical interconnect level, use the **Logical Interconnects** screen or REST APIs.

16.2.6 Update the logical interconnect configuration from the logical interconnect group

Compliance checking is the validation of a logical interconnect to ensure that it matches the configuration of its parent logical interconnect group. The appliance monitors both the logical interconnect and logical interconnect group, comparing the two, and checking the following for consistency:

Items	Compliance checking
Ethernet interconnect settings	Are there differences in the following logical interconnect settings from the expected configuration defined by the logical interconnect group? <ul style="list-style-type: none">• Enabling Fast MAC cache failover• MAC refresh intervals• Enabling IGMP snooping• IGMP idle timeout intervals• Loop and pause flood protection
Uplink sets	Are there differences in port assignments or network associations from the configuration defined by the logical interconnect group? Did you add an uplink set?
Interconnect maps	Is an interconnect type absent from an enclosure interconnect bay or different from the expected configuration defined by the logical interconnect group?

If both configurations match, the logical interconnect **Consistency state** field is set to `Consistent` and is considered to be compliant.

Non-compliance results in an alert for the logical interconnect and the **Consistency state** field is set to `Inconsistent with group`. It is also set to `Inconsistent with group` whenever you edit the logical interconnect or the logical interconnect group, even if your edit does not lead to a difference between the two.

Updating the logical interconnect configuration from the logical interconnect group

To bring a non-compliant (`Inconsistent with group`) logical interconnect configuration back into compliance (`Consistent`) with the logical interconnect group, you must reapply the settings from the logical interconnect group.

1. From the **Logical Interconnects** screen, select **Actions**→**Update from group**.

NOTE: The **Update from group** option is not available if the logical interconnect group and logical interconnect are already compliant (**Consistency state** field is set to `Consistent`).

Compliance alerts are cleared automatically and settings now match the logical interconnect group.

NOTE: You cannot make a logical interconnect compliant by editing or by manually clearing the alert; you must select **Actions**→**Update from group**.

2. Click **Yes, update** to confirm.

16.2.7 Configure a port to monitor network traffic

Port monitoring enables you to send a copy of every Ethernet frame coming in and going out of a port to another port. By monitoring a port's network traffic, you can connect debugging equipment, such as a network analyzer, to monitor those server ports. This capability is important in a server blade environment where there is limited physical access to the network interfaces on the server blades. You can configure one network analyzer port (the monitored-to uplink port) for up to 16 downlink server ports within a single enclosure.

To configure a port for monitoring, use the **Logical Interconnects** screen or REST APIs.

16.2.8 Learning more

- [“Logical interconnect groups” \(page 36\)](#)
- [“Logical interconnects” \(page 37\)](#)
- [“Uplink sets” \(page 38\)](#)

17 Managing enclosures and enclosure groups

An enclosure is a physical structure that can contain server blades, infrastructure hardware, and interconnects.

An enclosure group specifies a standard configuration for all of its member enclosures. Enclosure groups enable administrators to provision multiple enclosures in a consistent, predictable manner in seconds.

UI screens and REST API resources

UI screen	REST API resource
Enclosures	enclosures
Enclosure Groups	enclosure-groups

17.1 Prerequisites for bringing an enclosure under management

An enclosure must meet the following prerequisites in order for the appliance to manage it:

Prerequisites

Item	Requirement
Enclosure model	The enclosure must be a supported model listed in the <i>HP OneView Support Matrix</i> . The enclosure power is turned on. NOTE: To enable the appliance to manage the server hardware seated in an enclosure, the server hardware must meet the prerequisites listed in “Prerequisites for bringing server hardware under management” (page 112).
Firmware	The enclosure firmware must be at the minimum supported firmware version listed in the <i>HP OneView Support Matrix</i> . The appliance firmware repository must be populated with at least one firmware bundle.
Onboard Administrator	If the enclosure has two Onboard Administrators, both OAs must be at the same firmware version. The primary or standby OA must be configured with a host name or IP address and must be reachable by the appliance. As part of bringing an OA under management, a local user account is added, so the OA must be configured to allow for local user accounts.
IP addresses	IPv4 configuration is required.
iLO IP address	Server hardware iLOs must be configured with IP addresses, automatically with DHCP addresses or manually with Enclosure Bay IP Addressing (EBIPA)-specified addresses.
Interconnects	Interconnects must be configured with IP addresses, automatically with DHCP addresses or manually with EBIPA-specified addresses.
Open ports	The following ports must be opened between the appliance and the enclosure: <ul style="list-style-type: none">• TCP 80, 443• UDP 123, 161, 162

17.2 Roles

- Minimum required privileges: Infrastructure administrator or Server administrator

17.3 Tasks

The appliance online help provides information about using the UI or the REST APIs to:

- Add an enclosure to manage its contents.
- Remove an enclosure from management.
- Add a server blade to an existing enclosure.
- Remove a server blade from an existing enclosure.
- Bring an unmanaged enclosure under management.
- Claim an enclosure currently being managed by another appliance.
- Forcibly remove an enclosure if a remove action fails.
- Resolve connectivity issues between an enclosure and the appliance.
- View activities (alerts and tasks).
- Create an enclosure group.
- Edit an enclosure group.
- Delete an enclosure group.

17.4 About enclosures

An enclosure is a physical structure that can contain server blades, infrastructure hardware, and interconnects.

The enclosure provides the hardware connections between the interconnect downlinks and the installed server blades.

You add an enclosure so that its contents can be managed, enabling you to apply configurations, deploy server profiles, monitor operation status, collect statistics, and alert users to specific conditions.

When you add an enclosure, you specify an enclosure group. Enclosure groups enable you to maintain configuration consistency among enclosures. Each enclosure group is associated with a logical interconnect group that enables creation and configuration of a logical interconnect. Each enclosure is associated with a logical interconnect, which represents the configuration of all interconnects in the enclosure.

Connectivity and synchronization with the appliance

The appliance monitors the connectivity status of enclosures. If the appliance loses connectivity with an enclosure, a notification is displayed until connectivity is restored. The appliance attempts to resolve connectivity issues and clears the alert automatically, but if it is unsuccessful, you must resolve the issue and manually refresh the enclosure to synchronize it with the appliance.

The appliance also monitors enclosures to ensure that they are synchronized with changes to hardware and configuration settings. However, some changes to enclosures made outside of the appliance (from iLO or the OA (Onboard Administrator), for example) might cause the enclosure to lose synchronization with the appliance. You might have to manually refresh devices that lose synchronization with the appliance.

NOTE: HP does not recommend using iLO or the OA to make changes to a device. Making changes to a device from its iLO or OA could cause it to become out of synchronization with the appliance.

You can manually refresh the connection between the appliance and an enclosure from the **Enclosures** screen. Refreshing an enclosure will refresh all devices in it. See the online help for the **Enclosures** screen to learn more.

17.5 About enclosure groups

An enclosure group is a logical resource that defines a set of enclosures that use the same configuration for network connectivity. The network connectivity for an enclosure group is defined by the logical interconnect group associated with the enclosure group. This ensures that each enclosure has an identically configured logical interconnect and the same configuration for network connectivity.

17.6 Effects of managing an enclosure

When an enclosure is being managed by the appliance, the following enclosure settings are in effect:

- A management account is created.
- SNMP is enabled and the appliance is added as an SNMP trap destination.
- NTP (Network Time Protocol) is enabled and the appliance becomes the NTP time source.
- The NTP default polling interval is set to 8 hours.
- An appliance certificate is installed to enable single sign-on operations.
- Enclosure firmware management is disabled.
- The OA firmware is updated to minimum firmware levels, listed in the *HP OneView Support Matrix*.
- The server hardware iLO time zone is set to `Atlantic/Reykjavik` as recommended in the iLO documentation.

The time zone setting determines how the server hardware iLO adjusts UTC (Coordinated Universal Time) time to obtain the local time, and how it adjusts for daylight saving time (summer time). For the entries in the iLO event log and IML to display the correct local time, you must specify the time zone in which the server is located.

If you want iLO to use the time provided by the NTP server, without adjustment, configure the iLO to use a time zone that does not apply an adjustment to UTC time. In addition, that time zone must not apply a daylight saving time (summer time) adjustment.

There are several time zones that meet this requirement. One example is the `Atlantic/Reykjavik` time zone. This time zone is neither east nor west of the prime meridian and time does not change in the spring or fall.

17.7 Learning more

- [“Understanding the resource model” \(page 29\)](#)
- [“Managing licenses” \(page 158\)](#)
- [“Troubleshooting enclosures and enclosure groups” \(page 208\)](#)

18 Managing firmware for managed devices

NOTE: This chapter describes how to manage the firmware for devices managed by the appliance. For information about updating the firmware for the appliance, see [“Updating the appliance”](#) (page 163).

A firmware bundle, also known as an HP Service Pack for ProLiant (SPP), comprises a set of deliverables, a full-support ISO file, and six subset ISOs divided by HP ProLiant server family and operating system. An SPP is a comprehensive collection of firmware and system software, all tested together as a single solution stack that includes drivers, agents, utilities, and firmware packages for HP ProLiant servers, controllers, storage, server blades, and enclosures. Each SPP deliverable contains the HP Smart Update Manager (SUM), and software and firmware smart components.

You can apply SPPs as baselines to enclosures, interconnects, and server profiles, establishing a version for firmware and drivers across devices. You download SPPs from the HP website www.hp.com/go/spp to your local system, and then upload them to the firmware bundle repository on the appliance.

NOTE: Firmware will not be downgraded to the selected firmware baseline when applying a server profile. Use an external tool, for example HP SUM, to force firmware downgrades or rewrites.

Every resource (OA, iLO, server, and Virtual Connect) goes offline when you upgrade its firmware. Always perform the upgrade during a maintenance window.

UI screens and REST API resources

UI screen	REST API resource
Firmware Bundles	firmware-bundles

18.1 About the appliance firmware repository

The firmware bundle repository contains the HP SPPs you upload to the appliance.

You can view the versions and contents of the SPPs in the repository from the **Firmware Bundles** screen. Selecting a firmware bundle displays its release date, supported languages and operating systems, and the bundle components. The screen also displays the amount of storage space available for additional firmware bundles on the appliance. You cannot add a firmware bundle that is larger than the amount of space available in the repository.

When you update firmware for enclosures, interconnects, and server profiles, you select from the versions in the repository.

18.2 About unsupported firmware

A default firmware bundle (SPP) is pre-installed in the appliance and provides the minimum supported firmware for all supported server hardware and interconnects. When you add a resource to bring it under management, the resource firmware must be updated to the minimum supported level. The appliance attempts to automatically update the firmware while the resource is being added to the appliance. If the update fails, an alert is generated.

Unsupported firmware for firmware bundles

If you attempt to add a firmware bundle that contains firmware below the minimum versions supported, an alert is generated and the firmware bundle is not added to the appliance firmware repository.

Unsupported firmware for enclosures

When adding an enclosure, the appliance:

- Generates an alert if the logical interconnect firmware for the interconnects is below the required minimum level or if the interconnect firmware levels do not match. You must update the logical interconnect firmware from the **Logical Interconnects** screen or REST APIs.
- Updates the OA firmware automatically, if below the required minimum
- Updates the iLO firmware automatically, if below the required minimum

Unsupported firmware for server profiles

You are prevented from applying server profiles if the associated iLO firmware is below the minimum supported version, and instead, are directed to the **Server Hardware** screen to update iLO firmware.

Unsupported firmware for interconnects

If you attempt to add an interconnect with firmware that is below the minimum supported version, an alert is generated. You must update the logical interconnect firmware from the **Logical Interconnects** screen or REST APIs.

The **Firmware** panel of the **Logical Interconnects** screen displays the installed version of firmware and the firmware baseline for each interconnect.

18.3 Roles and Tasks

The appliance online help provides information about using the UI or the REST APIs to:

- View the firmware repository for firmware bundles to see the following:
 - List of firmware bundles in the repository
 - Contents of a firmware bundle
 - Available storage space for the repository

Minimum required privileges: Network administrator, Server administrator, or Read only

- Upload a firmware bundle to the appliance.
Minimum required privileges: Network administrator or Server administrator
- Install a firmware bundle for managed devices.
Minimum required privileges: Network administrator for interconnects or Server administrator for server profiles and enclosures
- Remove a firmware bundle from the firmware repository.
Minimum required privileges: Network administrator or Server administrator
- Create a custom SPP.
Minimum required privileges: Network administrator or Server administrator

18.4 The firmware update process

Firmware bundles enable you to update firmware on servers, blades, and infrastructure (enclosures and interconnects).

- To update the firmware on all devices in an enclosure, you select a new SPP as the new firmware baseline and to apply it to either the enclosure only (OA firmware), or to all the

resources in the enclosure (OA, all member interconnects, and server hardware firmware including iLO).

In the UI, select **Enclosures**→**Actions**→**Update firmware**, and then select from the following options:

Option	Device updated
Enclosure	OA firmware
Enclosure + logical interconnect + server profiles	OA, all member interconnects, and server hardware firmware including iLO

- You update a firmware bundle for a logical interconnect to apply the same firmware baseline to all member interconnects. This operation by default updates firmware only on those member interconnects that are running a different version of firmware and ignores the interconnects that are running the same firmware version. You select from the following options:

Option	Description
Update firmware (stage + activate)	Stages (uploads) the selected firmware to the secondary flash memory on the interconnect, and then activates the firmware as the baseline. During firmware activation, the interconnect will be offline.
Stage firmware for later activation	Writes the selected firmware to the secondary flash memory on the interconnect, but does not activate the firmware. You can activate the firmware at a later time.
Activate firmware	Activates the selected staged firmware. During firmware activation, the interconnect will be offline.

- To update the firmware bundle for a specific server, edit the existing server profile or create a new server profile to specify the version of the SPP, and then click **Create** in the user interface or use the REST APIs to apply.

NOTE: To apply a server profile, the selected server hardware must be powered off.

18.5 Best practices for firmware

Best practice	Description
First step: Upload the latest current SPP.	You should upload the SPP to your appliance repository.
Set the same firmware baseline for all devices in an enclosure.	HP recommends that you set the firmware baseline using the Update Firmware option on the Enclosures screen. This immediately updates all of the devices in the enclosure to the specified SPP level.
Update the firmware in the proper sequence.	It is not always possible to update all of the devices in an enclosure in a single operation. The appliance supports installing firmware on one device at a time. In this case, upgrade the firmware in the following order: OA, logical interconnect, and then the server hardware.
Install the drivers and other software after updating the firmware.	After you update the firmware, install the drivers and other software through the operating system. HP recommends that you install the drivers from the same SPP that contains the firmware.
Use HP SUM to install the drivers.	The appliance does not install drivers. Use an external tool, such as HP SUM, to install the drivers and other nonfirmware components.

Best practice	Description
Verify the managed device setting before updating the firmware.	Do not update the firmware on a managed device unless the firmware baseline is set to manage manually .
If you choose to create custom SPPs, use HP SUM to create them.	HP recommends using HP SPPs. You can use HP SUM 6.0 or later to create custom SPPs, which can be uploaded to the appliance repository. The appliance only supports installation of SPP ISO files, but using HP SUM, you can insert firmware updates into custom SPPs for the appliance. Download HP SUM 6.0 as a standalone product.
Store custom SPPs in a separate repository.	The appliance does not back up SPPs, so store custom SPPs in a repository that is not on the appliance, such as in the HP SUM repository used to create the custom SPP.

18.6 Learning more

- “Troubleshooting firmware bundles” (page 210)

19 Managing power and temperature

You can manage the power and temperature of your IT hardware using the appliance.

19.1 Managing power

To manage power, you describe your power delivery devices to the appliance using the **Power Delivery Devices** screen or the REST APIs. The appliance discovers HP Intelligent Power Delivery Devices (iPDUs) and their connections automatically.

UI screens and REST API resources

UI screen	REST API resource
Power Delivery Devices	power-devices
REST API only	enclosures (power capacity)
REST API only	server-hardware (power capacity)

19.1.1 Roles

- Minimum required privileges: Infrastructure administrator or Server administrator

19.1.2 Tasks

The appliance online help provides information about using the UI and REST APIs to:

- Add a power delivery device.
- Add a power connection.
- Filter power delivery devices.
- View last 5 minutes of power consumption for an iPDU.
- View last 24 hours of power consumption for an iPDU.
- Edit the properties of a power delivery device.
- Power on or off the locator light for a power delivery device.
- Power down a power delivery device.
- Remove a power delivery device.
- Resolve connectivity issues between an iPDU and the appliance.
- Add an iPDU currently being managed by another management system.
- View power utilization statistics.
- Update enclosure power capacity settings (REST API only).
- Update server hardware power capacity settings (REST API only).

19.1.3 About power delivery devices

Power delivery devices provide power to IT hardware. A typical power topology in a data center includes power delivery devices such as power feeds, breaker panels, branch circuits, and power distribution units (PDUs), as well as the load segments, outlet bars, and outlet components of these devices. Adding your power delivery devices to the appliance enables power management using thermal limits, rated capacity, and derated capacity.

The **Power Delivery Devices** screen describes two classes of devices:

- HP Intelligent Power Distribution Units (HP iPDUs), which the appliance can automatically discover and control.
- Other power delivery devices that the appliance cannot discover. By manually adding these devices to the appliance, they become available for tracking, inventory, and power management purposes.

Regardless of how power delivery devices are added to the appliance, the appliance automatically generates the same types of analysis (capacity, redundancy, and configuration). For iPDUs, the appliance gathers statistical data and reports errors.

Connectivity and synchronization with the appliance

The appliance monitors the connectivity status of iPDUs. If the appliance loses connectivity with an iPDU, an alert displays until connectivity is restored. The appliance will try to resolve connectivity issues and clear the alert automatically, but if it cannot, you must resolve the issue and manually refresh the iPDU to bring it in synchronization with the appliance.

The appliance also monitors iPDU to remain synchronized with changes to hardware and power connections. However, some changes to devices made outside of the control of the appliance (from iLO or the OA, for example) may cause them to become out of synchronization with the appliance. You may have to manually refresh devices that lose synchronization with the appliance.

NOTE: HP recommends that you do not use iLO or the OA to make changes to a device. Making changes to a device from its iLO or OA could cause it to lose synchronization with the appliance.

You can manually refresh the connection between the appliance and an iPDU from the **Power Delivery Devices** screen. See the online help for the **Power Delivery Devices** screen to learn more.

19.1.4 About racks

A rack is a physical structure that contains IT equipment such as enclosures, servers, power delivery devices, and unmanaged devices (an unmanaged device uses slots in the rack and consumes power or exhausts heat, but it is not managed by the appliance). You can manage your racks and the equipment in them by adding them to the appliance. Having your racks managed by the appliance enables you to use the appliance for space and power planning. The appliance also gathers statistical data and monitors the power and temperature of the racks it manages.

When you add an enclosure to the appliance, it automatically creates a rack and places the enclosure in it. The appliance places into the rack all enclosures connected by management link cables. When enclosures are added, the appliance places them in the rack from top to bottom. To accurately depict the layout of your enclosures within the rack, you must edit the rack to place the enclosure in the proper slots.

You can use the appliance to view and manage your rack configuration and power delivery topology. You can specify the physical dimensions of the rack (width, height, and depth), the number of U slots, and the location of each piece of equipment in the rack. You can specify the rack PDUs that provide power to the rack, and their physical position in the rack or on either side. You can also describe how the devices in the rack are connected to those PDUs.

NOTE: The default rack height is 42U. When the appliance discovers an HP Intelligent Series Rack, it sets the rack height to 42U if there is no managed server hardware above slot 42. If an HP Intelligent Series Rack contains server hardware above slot 42, the appliance sets the rack height to the highest slot that contains managed server hardware. If you add server hardware to a higher slot later, the appliance adjusts the rack height automatically.

After adding a rack to the appliance for management, you can add the rack to a data center to visualize the data center layout and to monitor device power and cooling data.

After the rack is under management, you can configure the power delivery topology with redundant and uninterruptible power supplies to the devices in the rack.

19.2 Managing temperature

To manage the temperature of your hardware, you must add your server hardware to racks, position it in the rack, and then add the racks to data center(s).

UI screens and REST API resources

UI screen	REST API resource
Data Centers	datacenters
Racks	racks

19.2.1 Roles

- Minimum required privileges: Infrastructure administrator or Server administrator

19.2.2 Tasks

The appliance online help provides information about using the UI and REST APIs to:

- Add a data center.
- Edit a data center.
- Manipulate the view of a data center visualization.
- Monitor data center temperature.
- Remove a data center from management.
- Set the thermal limit of a rack (edit the properties of a rack).

19.2.3 About data centers

A data center represents a physically contiguous area in which racks containing IT equipment are located.

For example, you have IT equipment in two rooms or on separate floors. You could create a data center for each of these areas.

Each server, enclosure, or power distribution device in your data center can report its power requirements, but it can be difficult to understand the power and cooling requirements for your data center as a whole. The appliance enables you to bring power and cooling management of your servers, enclosures, and power delivery devices together in a single management system.

The **Layout** view of the data center is color-coded to depict the peak temperature recorded in the last 24 hours.

Default data center: Datacenter 1

When you initialize the appliance for the first time, it creates a data center named `Datacenter 1`. The appliance provides this data center as a place to visualize your racks. You can rename or edit this data center to match the values and layout of your data center, you can use it as the basis for a planned data center model, or you can delete this data center without adverse effects.

Default rack placement

When you add a rack to the appliance for management, the appliance displays the rack in all data centers even though its actual location is not known. If you view a data center that displays unpositioned racks, a warning appears to alert you that unpositioned racks are being displayed. When you assign a rack to a data center, it is no longer displayed in other data centers.

19.2.4 Learning more

- [“About utilization graphs” \(page 181\)](#)

20 Managing users and authentication

The appliance requires users to log in with a valid user name and password, and security is maintained through user authentication and role based authorization. User accounts can be local, where the credentials are stored on the appliance or can be on a company or organizational directory (Microsoft Active Directory, for example) hosted elsewhere, where the appliance contacts the defined directory server to verify user credentials.

UI screens and REST API resources

UI screen	REST API resource
Users and Groups	users, roles, authz, logindomains, logindomains/global-settings, and logindomains/group-to-role-mapping

20.1 Roles

- Minimum required privileges: Infrastructure administrator

20.2 Tasks

The appliance online help provides information about using the user interface or the REST APIs to:

- Add a user with local authentication.
- Add a user with directory-based authentication.
- Add a group with directory-based authentication.
- Designate user privileges.
- Edit a user account, including updating a user password.
- Remove a user account.
- [Reset the administrator password.](#)
- Add an authentication directory service.
- Allow local logins.
- Disable local logins.
- Change the authentication directory service settings.
- Set an authentication directory service as the default directory.
- Remove an authentication directory service from the appliance.

20.3 About user accounts

The appliance provides [default roles](#) to separate responsibilities in an organization. A user role enables access to specific resources managed from the appliance.

Role-based access control enforces permissions to perform operations that are assigned to specific roles. You assign specific roles to system users or processes, which gives them permission to perform certain system operations. Because a user is not assigned permissions directly, but only acquires them through their role (or roles), individual user rights are managed by assigning the appropriate roles to the user. At initial appliance startup, there is a default administrator account with full access (Infrastructure administrator) privileges. For more information about the actions each role can perform, see [“Action privileges for user roles”](#) (page 144).

If you cannot see resource information or perform a resource task, your assigned role does not have the correct privileges. In this case, you should request a different role or an additional role.

20.4 About user roles

User roles enable you to assign permissions and privileges to users based on their job responsibilities. You can assign full privileges to a user, or you can assign a subset of permissions to view, create, edit, or remove resources managed by the appliance.

Table 5 Appliance role types

Role	Type of user	Associated permissions or privileges
Full	Infrastructure administrator	View, create, edit, or remove resources managed by the appliance, including management of the appliance itself through the UI or command line An Infrastructure administrator can also manage information provided by the appliance in the form of activities, notifications, and logs. Only an Infrastructure administrator can restore an appliance from a backup file.
Read only	Read only	View only access
Specialized	Backup administrator	Create and download backup files, view the appliance settings and activities. Has the authority to use scripts to log in to the appliance and run scripts to back up the appliance. NOTE: This role is specifically intended for scripted backup creation and download. HP recommends that users with this role should not initiate interactive login sessions through the HP OneView user interface.
	Network administrator	View, create, edit, or remove networks, network sets, connections, interconnects, uplink sets, and firmware bundles; view related activities, logs, and notifications
	Server administrator	View, create, edit, or remove server profiles and templates, network sets, enclosures, and firmware bundles Access the Onboard Administrator and physical servers View connections, networks, racks, power, and related activities, logs, and notifications

20.5 Action privileges for user roles

The following table lists the user action privileges associated with each user role. The `Use` privilege is a special case that allows you to associate objects to objects that you own but you are not allowed to change. For example, in a logical interconnect group, a user assigned the role of Server administrator is not allowed to define logical interconnect groups, but can use them when adding an enclosure.

Table 6 Action privileges for user roles

Category	Action privileges for user roles (C=Create, R=Read, U=Update, D=Delete, Use)				
	Infrastructure administrator	Server administrator	Network administrator	Backup administrator	Read only
activities	CRUD	CRU	CRU	—	R
alerts	RUD	RUD	RUD	—	R
appliance	CRUD	R	R	—	R
audit logs	R	R	R	—	—

Table 6 Action privileges for user roles *(continued)*

Category	Action privileges for user roles (C=Create, R=Read, U=Update, D=Delete, Use)				
	Infrastructure administrator	Server administrator	Network administrator	Backup administrator	Read only
backups	CRUD	—	—	CRD	R
debug logs	CRUD	CRU	CRU	—	R
events	CRU	CRU	CRU	—	R
global settings	CRUD	CRUD	CRUD	—	R
login sessions	CRUD	—	—	—	R
notifications	CRUD	CRD	CRD	—	R
organizations	CRUD	—	—	—	R
restores	CRUD	—	—	—	R
roles	CRUD	—	—	—	R
users	CRUD	—	—	—	R
user preferences	CRUD	—	—	—	R
connections	CRUD	CRUD	CR	—	R
connection templates	CRUD, Use	RU	CRUD	—	R
data centers	CRUD	CRUD	—	—	R
domains	CRUD	R	CR	—	R
enclosures	CRUD	CRUD	R	—	R
enclosure groups	CRUD, Use	CRUD, Use	R	—	R
enclosure types	CRUD	—	—	—	R
Ethernet networks	CRUD	R	CRUD	—	R
FC networks	CRUD	R	CRUD	—	R
firmware drivers	CRUD	CRUD	CRUD	—	R
ID range vmacs (MAC addresses)	CRUD	R	CRUD	—	R
ID range vsns (serial numbers)	CRUD	CRUD	R	—	R
ID range vwwns (World Wide Names)	CRUD	R	CRUD	—	R
networks	CRUD, Use	R	CRUD, Use	—	R
network sets	CRUD, Use	CRUD	CRUD	—	R
network templates	CRUD, Use	—	CRUD, Use	—	R
power devices	CRUD	CRUD	—	—	R
racks	CRUD	CRUD	—	—	R
server hardware	CRUD, Use	CRUD, Use	R	—	R

Table 6 Action privileges for user roles *(continued)*

Category	Action privileges for user roles (C=Create, R=Read, U=Update, D=Delete, Use)				
	Infrastructure administrator	Server administrator	Network administrator	Backup administrator	Read only
server hardware types	CRUD, Use	CRUD, Use	R	—	R
server profiles	CRUD, Use	CRUD	R	—	R
server profile templates	CRUD, Use	CRUD, Use	—	—	R
interconnects	CRUD	CR	CRUD	—	R
interconnect domains	CRUD	—	—	—	R
interconnect groups	CRUD	R	CRUD	—	R
interconnect types	CRUD	R	—	—	R
unmanaged devices	CRUD	CRUD	—	—	R
uplink sets	CRUD	R	CRUD	—	R
logical interconnects	CRUD, Use	R, Use	CRUD, Use	—	R
logical interconnects groups	CRUD, Use	R, Use	CRUD, Use	—	R

20.6 About authentication settings

Security is maintained through user authentication and role-based authorization. User accounts can be local, where the user credentials are stored on the appliance, or they can be in a directory (Microsoft Active Directory, for example) hosted elsewhere, where the appliance contacts the designated directory server to verify the user credentials.

When logging in to the appliance, each user is authenticated by the authentication directory service, which confirms the user name and password. Use the **Authentication** settings panel to configure authentication settings on the appliance, which is populated with default values during first-time setup of the appliance.

To view or make changes to **Authentication** settings, log in with Infrastructure administrator privileges. No other users are permitted to change or view these settings.

View and access the **Authentication** settings by using the UI and selecting **Settings**→**Security**→**Authentication** or with the REST APIs.

20.7 About directory service authentication

You can use an external authentication directory service (also called an enterprise directory or authentication login domain) to provide a single sign-on for groups of users instead of maintaining individual local login accounts. An example of an authentication directory service is a corporate directory that uses LDAP (Lightweight Directory Access Protocol).

Any user in the group can log in to the appliance, and each member of the group is assigned the same role. On the login window, the user:

- Enters their name (typically, the Common-Name attribute, CN).
- Enters the password for the group.
- Selects the authentication directory service. This box appears only if you have added an authentication directory service to the appliance.

In the [Session control](#), the user is identified by their name preceded by the authentication directory service. For example:

CorpDir\pat

When you add an authentication directory service to the appliance, you provide search criteria so that the appliance can find the group by its DN (Distinguished Name). For example, the following attribute values identify a group of administrators in a Microsoft Active Directory:

distinguishedName CN=Administrator,CN=Users,DC=example,DC=com

The combination of LDAP attributes that make up the DN depends on the structure of the authentication directory service, but typically, the CN attribute identifies the user or group.

NOTE: If you specify a group that contains hierarchical levels of users, only users in that group and in the next three levels lower can log in to the appliance.

A directory server is the physical or virtual machine that hosts the authentication directory service. When you add the directory server, you configure the appliance by:

- Specifying the IP address of the authentication directory service so that the appliance can access it.
- Specifying the LDAPS (LDAP over SSL) communication port.
LDAPS is the only protocol used for communication between the appliance and the authentication directory service.
- Installing a certificate to ensure integrity and authenticity between the appliance and the authentication directory service.

If you replicate the authentication directory service for high availability or disaster tolerance, add the replicated directory service as a separate directory service.

After configuring and adding a directory server, you can designate it as the default directory service.

You can:

- Allow local logins only, which is the default.
- Allow both local logins and logins for user accounts authenticated by the directory service.
- Disable local logins which restricts logins to user accounts authenticated by the directory service.

20.8 Managing user passwords

A user with Infrastructure administrator privileges can manage the passwords of all local users on the appliance using the UI or the REST APIs. Users without Infrastructure administrator privileges can manage only their own passwords.

As Infrastructure administrator, you can view all users logged in to the appliance with the **Users and Groups** screen or REST APIs. Select any user, and then edit their password or assigned role.

All other local users can edit their own passwords by using the UI or the REST APIs. In the UI, click the **Session** icon in the top banner, and then click the **Edit** icon to change their current password or contact information.

20.9 Reset the administrator password

If you lose or forget the administrator password, you can reset it by executing a command and contacting your authorized support representative by telephone.

Prerequisites

- You have access to the virtual appliance console.

Resetting the administrator password

1. From the console's appliance login screen, switch to the `pwreset` login screen by pressing **Ctrl+Alt+F1**. To return to the console's login screen, press **Ctrl+Alt+F2**.

NOTE: For VMware vSphere users, **Ctrl+Alt** is used for another function. To send the command to the console, you must press **Ctrl+Alt+Spacebar** then press **Ctrl+Alt+F1**.

2. Log in with the user name `pwreset`.

The appliance displays a challenge key. For example:

```
<hostname> login: pwreset
      Challenge = xyaay42a3a
      Password:
```

3. Telephone your authorized support representative and read the challenge key to them. They will provide you with a short-lived, one-time password based on the challenge key.

The authorized support representative uses the challenge code to generate a short-lived, one-time password based on the challenge key. It will be an easy-to-type, space-separated set of strings. For example:

```
VET ROME DUE HESS FAR GAS
```

4. Enter the password from the previous step.
The appliance displays a new randomly generated password.
5. Note the new password for the administrator account, and then press **Enter** to log out.
6. Log in as administrator using the new password through the UI or REST API.
The new password expires immediately after use; you must select a new password.

20.10 Learning more

- [“About user accounts” \(page 143\)](#)
- [“About user roles” \(page 144\)](#)
- [“Action privileges for user roles” \(page 144\)](#)
- [“Controlling access for authorized users” \(page 48\)](#)

21 Backing up an appliance

This chapter describes how to use the UI, REST APIs, or a custom-written PowerShell script to save your appliance resource configuration settings and management data to a backup file.

- ❗ **IMPORTANT:** HP recommends backing up your appliance configuration on a regular basis, preferably daily, and especially after adding hardware or changing the appliance configuration in the unlikely event you need to [restore the appliance](#).

21.1 Overview of the backup process

HP OneView provides the ability to save your configuration settings and management data to an encrypted backup file and enables you to use that backup to restore a corrupted appliance in the event of a catastrophic failure.

The backup process involves creating a backup file and then downloading that file to a secure off-appliance location for future use.

The appliance stores only one backup file at a time. Creating each subsequent backup file replaces the current backup file. To prevent a backup file from being overwritten by a new backup file, download and save the backup file to an off-appliance location before running the next backup process.

- ⚠ **CAUTION:** Do not use any hypervisor-provided capabilities or snapshots to back up an appliance because doing so can cause synchronization errors and result in unpredictable and unwanted behavior.

UI screens and REST API resources

UI screen	REST API resource
Settings → Actions	backups

For more information about backing up an appliance, see the online help for the **Settings** screen.

21.2 Roles

Users with Infrastructure administrator and Backup administrator privileges can create and download backup files, however, only the Infrastructure administrator can restore an appliance from a backup file.

The Backup administrator has the authority to use scripts to log in to the appliance and run scripts to back up the appliance. This role is specifically intended for scripted backup creation and download. HP recommends that users with this role should not initiate interactive login sessions through the HP OneView user interface.

21.3 Backup file name

The backup file name has the following format:

appliance-host-name_backup_YYYY-MM-DD_hhmmss.bkp

Example

myhost_backup_2013-10-01_092700.bkp

In this example, the backup file was created for the appliance host name *myhost* on October 1, 2013, at 9:27 a.m.

21.4 Guidelines for creating a backup file

- HP recommends performing regular backups, preferably daily, and especially after adding hardware or changing the appliance configuration.
If you added server hardware to the appliance after the backup file was created, that hardware is not in the appliance database when the restore operation completes. You must add that hardware to the appliance and then repeat any other configuration changes (such as assigning server profiles) that were made between the time the backup file was created and the restore operation completed.
- Only the Infrastructure administrator or a Backup administrator can create a backup file.
Only the Infrastructure administrator can restore the appliance from a backup file.
- HP recommends using an enterprise backup/restore product such as HP Data Protector to archive backup files. For information on HP Data Protector, see the following website:
<http://www.hp.com/go/dataprotector>
HP provides REST APIs for integration with enterprise backup/restore products.
- Only one backup operation can run at a time.
- You can back up the appliance while it is in use and while normal activity is taking place.
- You do not need to wait for tasks to stop before creating a backup file.
- Perform a backup operation before and after updating the appliance firmware.
- After you create and download the backup file, HP recommends that you encrypt it and store it in a safe place.
- To prevent the backup file from being overwritten, you must download the file before performing the next backup.
- A backup is restored by uploading it to the appliance, and then requesting that the appliance restore from the backup.

21.5 Create and download a backup file

A backup file saves the configuration settings and management data for your appliance. You can recover from a catastrophic failure by restoring your appliance from the backup file.

HP recommends performing regular backups, preferably daily, and especially after adding hardware or changing the appliance configuration.

NOTE: To reduce the size of the backup file and the time it takes to create it, the firmware bundles you have uploaded to the appliance are not included in the backup file. You must upload the appropriate firmware bundles after restoring the appliance.

Only one backup operation can run at a time.

The backup operation backs up the following:

- HP OneView Database
- System files:
 - Non-database data
 - Audit log
 - License files

The backup operation does not back up the following:

- Non-data files: Static files that are installed as part of the execution environment, and are not specific to the appliance or managed environment configuration
- Log files (except the Audit log file)
- Appliance network configuration
- First time setup configuration files
- Firmware bundles

Prerequisites

- Minimum required privileges: Infrastructure administrator, Backup administrator

Creating and downloading a backup file

1. From the **Settings** screen, select **Actions**→**Create backup**.
While the backup file is being created, a progress bar appears in the **Overview** pane.
Wait for the backup file creation to complete.
2. Optionally, click **Create backup** to the left of the progress bar for information, including the name of the backup file.
The file name has the following format:
`appliance-host-name_backup_yyyy-mm-dd_hhmmss.bkp`
3. After the backup file is created, select **Actions**→**Download backup**.
4. Save the backup file.

21.6 Using REST APIs to create and download an appliance backup file

After the backup is initiated, a `TaskResource` URI is created that you use to track the progress of the backup. When the backup is complete, you can use a `GET` REST API operation to download and change the backup file name. The latest backup is stored on the appliance and is replaced when a new backup is initiated.

Prerequisites

- Minimum required session ID privileges: Backup administrator

Creating and downloading an appliance backup file using REST APIs

1. Create the backup file.
`POST /rest/backups`
 2. Download the backup file.
`GET /rest/backups/archive/{backup URI}`
-

NOTE: After the `POST` operation is complete, a `TaskResource` URI and backup URI are returned. You can use the `TaskResource` URI to monitor the progress of the backup. Use the backup URI to refer to a specific backup when downloading the backup file or performing another operation.

21.7 Creating a custom script to create and download an appliance backup file

If you prefer to write a customized script to create and download your appliance backup file, and schedule that script to run on a schedule according to your IT policies, see [“Sample backup script” \(page 271\)](#) for a sample PowerShell script.

22 Managing the appliance

22.1 Managing appliance availability

Managing and maintaining appliance availability starts with configuring the appliance virtual machine for high availability as described in [“Planning for high availability” \(page 83\)](#), and following the best practices described in [“Best practices for managing a VM appliance” \(page 153\)](#).

In the event of an appliance shutdown, your managed resources continue to operate. For more information about how the appliance handles an unexpected shutdown, and what you can do to recover, see:

- [“How the appliance handles an unexpected shutdown” \(page 153\)](#)
- [“What to do when an appliance restarts” \(page 154\)](#)

For information about how to shut down or restart the appliance, see:

- [“Shut down the appliance” \(page 154\)](#)
- [“Restart the appliance” \(page 154\)](#)

22.1.1 Best practices for managing a VM appliance

HP recommends the following guidelines for managing your VM appliance from the virtual console:

Do	Do not
<ul style="list-style-type: none">• Use thick provisioning.• Use shares and reservations to ensure adequate CPU performance.	<ul style="list-style-type: none">• Use thin provisioning.• Update the VMware tools. If VMware Tools show Out of Date or Unmanaged, they are running correctly. These status messages are not a problem, because the tools are available and running. VMware tools are updated with each HP OneView software update.• Revert to a VM snapshot (unless under specific circumstances, as instructed by your authorized support representative).• Set the Synchronize guest time with host option in the vSphere client when the HP OneView appliance is configured to use NTP. HP OneView automatically sets the appropriate Synchronize guest time with host setting during network configuration. When HP OneView is configured to use NTP servers, the Synchronize guest time with host option is disabled. If HP OneView is not configured to use NTP servers, it synchronizes to the host VM clock and the Synchronize guest time with host option is enabled. In this case, configure the VM host to use NTP.• Reduce the amount of memory assigned to the VM.

22.1.2 How the appliance handles an unexpected shutdown

The appliance has features to enable it to automatically recover from an unexpected shutdown, and managed resources continue to operate while the appliance is offline. However, HP recommends that you use the appliance backup features to ensure that the appliance is backed up daily, and when you make significant configuration changes, such as adding or deleting a network.

Appliance recovery operations

When the appliance restarts, it performs the following operations:

- Detects tasks that were in progress and resumes those tasks, if it is safe to do so. If the appliance cannot complete a task, it notifies you that the task has been interrupted or is in some other error state.
- Attempts to detect differences between the current environment and the environment at the time the appliance shut down, and refreshes its database with the detected changes.
If you determine that the appliance data does not match the current environment, you can request that the appliance refresh the data for certain resources, such as enclosures.

Appliance recovery during a firmware update of a managed resource

If the appliance shuts down during a firmware update of a managed resource, when the appliance restarts, it detects the failed update and marks the firmware update tasks as being in an error state. To update the firmware for this resource, you must reinitiate the firmware update task.

22.1.2.1 What to do when an appliance restarts

The online help provides information about using the user interface or the REST APIs to:

- Check for critical alerts or failed tasks and follow the provided resolution instructions
- Manually refresh a resource if the resource information displayed appears to be incorrect or inconsistent
- Create a support dump (recommended for unexpected crashes to help support personnel to troubleshoot a problem)
- Update firmware for a resource, if a firmware update task was in progress when the appliance shut down.

22.1.3 Shut down the appliance

Use this procedure to perform a graceful shutdown of the appliance.

Prerequisites

- Minimum required privileges: Infrastructure administrator.
- Ensure that all tasks have been completed or stopped, and that all other users are logged off.

Shutting down the appliance

1. From the **Settings** screen, select **Actions**→**Shut down**.
A dialog box opens to inform you that all users will be logged out and ongoing tasks will be canceled.
2. Select **Yes, shut down** in the dialog box.

22.1.4 Restart the appliance

Use this procedure to perform a graceful shutdown of the appliance and restart it. You are returned to the login screen.

Prerequisites

- Minimum required privileges: Infrastructure administrator.
- Ensure that all tasks have been completed or stopped, and that all other users are logged off.

Restarting the appliance

1. From the **Settings** screen, select **Actions**→**Restart**.
A dialog box opens to inform you that all users will be logged out and ongoing tasks will be canceled.
2. Select **Yes, restart** in the dialog box.
3. Log in when the login screen reappears.

22.2 Managing the appliance settings

Appliance settings include the network settings, the clock settings, and the SNMP settings for your appliance in the data center.

If the appliance has not yet been configured when you log in, you are instructed to configure the appliance network. You can change appliance network settings at any time after they are configured.

You manage the appliance network configuration from the **Settings** screen or by using the REST APIs. The **Settings** screen enables you to manage various system-wide settings and tasks. Use the **Settings**→**Actions** menu to access various appliance and security tasks, including downloading audit logs.

UI screens and REST API resources

UI screen	REST API resource
Settings	appliance/network-interfaces, appliance/device-read-community-string, and appliance/trap-destinations

22.2.1 Roles

- Minimum required privileges: Infrastructure administrator

22.2.2 Tasks

The appliance online help provides information about using the UI or the REST APIs to:

- Change the appliance host name, IP address, subnet or CIDR mask, or gateway address.
- Change the DNS server IP address.
- Set and synchronize the appliance clock.
- Set the SNMP read community string and add SNMP trap destinations.

22.2.3 About appliance SNMP settings

Network management systems use SNMP (Simple Network Management Protocol) to monitor network-attached devices. The appliance uses SNMP to retrieve information from managed devices. The devices use SNMP to send asynchronous notifications (called traps) to the appliance.

You specify a read community string that serves as a credential to verify access to the SNMP data on the managed devices. The appliance sends the read community string to enclosures (through their OAs) and to the servers (through their iLO management processors). Some older devices require manual host OS configuration.

Install SNMP OS host agents for HP ProLiant G7 blade servers

For the appliance to monitor the health of HP ProLiant G7 blade servers, you need to configure the SNMP settings for the server and iLO3.

1. Install the host operating system on the server.
2. Install the SNMP subsystem on the server.
3. Configure SNMP on the host to use the community string and trap destination of the appliance.
4. Using the latest SPP, install the HP management agent set and associated drivers. You will be prompted for the SNMP community string and the trap destination.
5. After the HP management agent set and associated drivers are installed and running, add the HP ProLiant G7 blade server to the appliance.

If you install the agents and drivers after adding the G7 blade server, you might have to refresh the G7 blade server from the user interface or with REST APIs.

NOTE: If you change the appliance read community string, you must reconfigure all G7 blade server SNMP OS host agents to use the new read community string. The appliance cannot propagate this update to the host OS.

22.2.4 Learning more

- [“Planning the appliance configuration” \(page 82\)](#)
- [“Managing appliance availability” \(page 153\)](#)
- [“Managing the security features of the appliance” \(page 156\)](#)

22.3 Managing addresses and ID pools

A default set of virtual ID pools for MAC addresses, WWNs, and serial numbers are provided at startup. If you need additional addresses or identifiers, you can add autogenerated or custom ranges of ID pools.

You manage the ID pools from the UI **Settings** screen or by using the REST APIs.

UI screens and REST API resources

UI screen	REST API resource
Settings	id-pools

22.3.1 Roles

- Minimum required privileges: Infrastructure administrator

22.3.2 Tasks

The appliance online help provides information about using the UI or the REST APIs to:

- View a list of active ID pools and their properties.
- Add an autogenerated ID pool for MAC addresses, WWNs, or serial numbers.
- Add a custom ID pool range for MAC addresses, WWNs, or serial numbers.

22.4 Managing the security features of the appliance

To learn about the security features of the appliance, see [“Understanding the security features of the appliance” \(page 45\)](#).

22.4.1 Enabling or disabling HP support access to the appliance

This product contains a technical feature that will allow an on-site authorized support representative to access your system, through the system console, to assess problems that you have reported. This

access will be controlled by a password generated by HP that will only be provided to the authorized support representative. You can disable access at any time while the system is running.

UI screens and REST API resources

UI screen	REST API resource
Settings	appliance/settings

22.4.1.1 Roles

- Minimum required privileges: Infrastructure administrator

22.4.1.2 Tasks

The appliance online help provides information to enable or disable HP support access from either the **Settings** screen or the REST APIs.

22.4.2 Managing SSL certificates

An SSL (Secure Sockets Layer) certificate certifies the identity of the appliance. The certificate is required by the underlying HTTP server to establish a secure (encrypted) communications channel with the client web browser.

You manage certificates from the **Settings** screen or by using the appliance settings REST APIs.

UI screens and REST API resources

UI screen	REST API resource
Settings	certificates

22.4.2.1 Roles

- Minimum required privileges for all tasks except as noted: Infrastructure administrator

22.4.2.2 Tasks

The appliance online help provides information about using the UI or the REST APIs to:

- Create a self-signed certificate.
- Create a certificate signing request.
- Import a certificate.
- View the SSL certificate settings (Minimum required privileges: Infrastructure administrator, Backup administrator, or Read only).

22.4.2.3 Learning more

See [“Understanding the security features of the appliance” \(page 45\)](#).

22.4.3 Managing the HP public key

The HP public key verifies that:

- HP created its software packages (RPMs) and updates.
- The code was not modified after it was signed.

22.4.3.1 Roles

- Minimum required privileges: Infrastructure administrator

22.4.3.2 Tasks

The appliance online help provides information about managing public keys from the **Settings** screen or by using the REST APIs to:

- Acquire and install the HP public key.
- View the HP public key.

22.4.4 Downloading audit logs

The audit log helps the security administrator understand what security-related actions took place. You can gather log files and other information that your authorized support representative needs so that they can diagnose and troubleshoot an appliance.

UI screens and REST API resources

UI screen	REST API resource
Settings	audit-logs

22.4.4.1 Roles

- Minimum required privileges: Infrastructure administrator

22.4.4.2 Tasks

The appliance online help provides information how to download the audit logs from the **Settings** screen or by using the REST APIs.

22.4.4.3 Learning more

- “Understanding the audit log” (page 48)
- “Choosing a policy for the audit log” (page 80)

22.5 Managing licenses

You manage licenses from the **Settings** screen or by using the REST APIs.

UI screens and REST API resources

UI screen	REST API resource
Settings	licenses

22.5.1 Roles

- Minimum required privileges: Infrastructure administrator

22.5.2 Tasks

The appliance online help provides information about using the UI or the REST APIs to:

- Add a license key to the appliance license pool.
- Specify a license policy as part of adding an enclosure.

- Specify a license type as part of adding a rack mount server.
- View licensing status information through license graphs.
- View a list of server hardware that has been assigned a specific license type.

22.5.3 About licensing

HP OneView requires a license for each server that it manages. You can purchase server hardware and enclosures with licenses embedded (integrated) on the hardware, or you can purchase licenses separately (nonintegrated) and add them to the appliance. The appliance manages licenses in a pool where all licenses are stored and applied to server hardware as needed.

Purchasing factory-integrated (embedded) software and hardware provides the best licensing experience because the license is delivered on the hardware and is registered automatically when you register the hardware.

If you purchase nonintegrated licenses, you must activate and register the licenses using the HP licensing portal at <https://www.hp.com/software/licensing>. After you register your licenses, you add the license keys to the appliance. When you add server hardware that does not have an embedded license, it is assigned a license from the license pool.

EULA

The appliance has a EULA (End User License Agreement) that you must accept before using the appliance for the first time. You can view the EULA from the [Help sidebar](#) and online at <http://www.hp.com/go/oneview/eula>.

22.5.3.1 License types

The following types of licenses are available for HP OneView:

HP OneView	Provides an HP OneView license and an iLO Advanced license
HP OneView w/o iLO	Provides an HP OneView license only
	This license is intended for server hardware with iLOs that are already licensed, or server hardware for which you do not require an iLO license.

When you add an enclosure or rack mount server to the appliance, you must specify one of these licenses. After a 60-day trial period, the appliance displays an alert if you do not have enough licenses to support the existing servers. The alert appears on the **Dashboard** and in the **Settings** view after login and does not clear until you add enough licenses.

22.5.3.2 License delivery

License delivery depends on how the license is purchased. The license delivery methods for HP OneView are:

- Embedded on the server hardware iLO (software purchased integrated with the hardware)
- Embedded on the enclosure OA (enclosure bundle license for 16 servers)
- Standalone, nonintegrated (purchased separately from the hardware)

22.5.3.3 License reporting

Basic license reporting indicates whether your appliance has enough licenses for the number of managed server hardware in your environment.

From the **Licenses** view on the **Settings** screen, you can view the following:

- The number of available licenses
- The number of licensed servers
- The number of licenses required for compliance (all server hardware licensed)

22.5.3.4 View license status

You can view the status of your server hardware licenses using the license graphs from the **Settings** menu in the **Licenses** view.

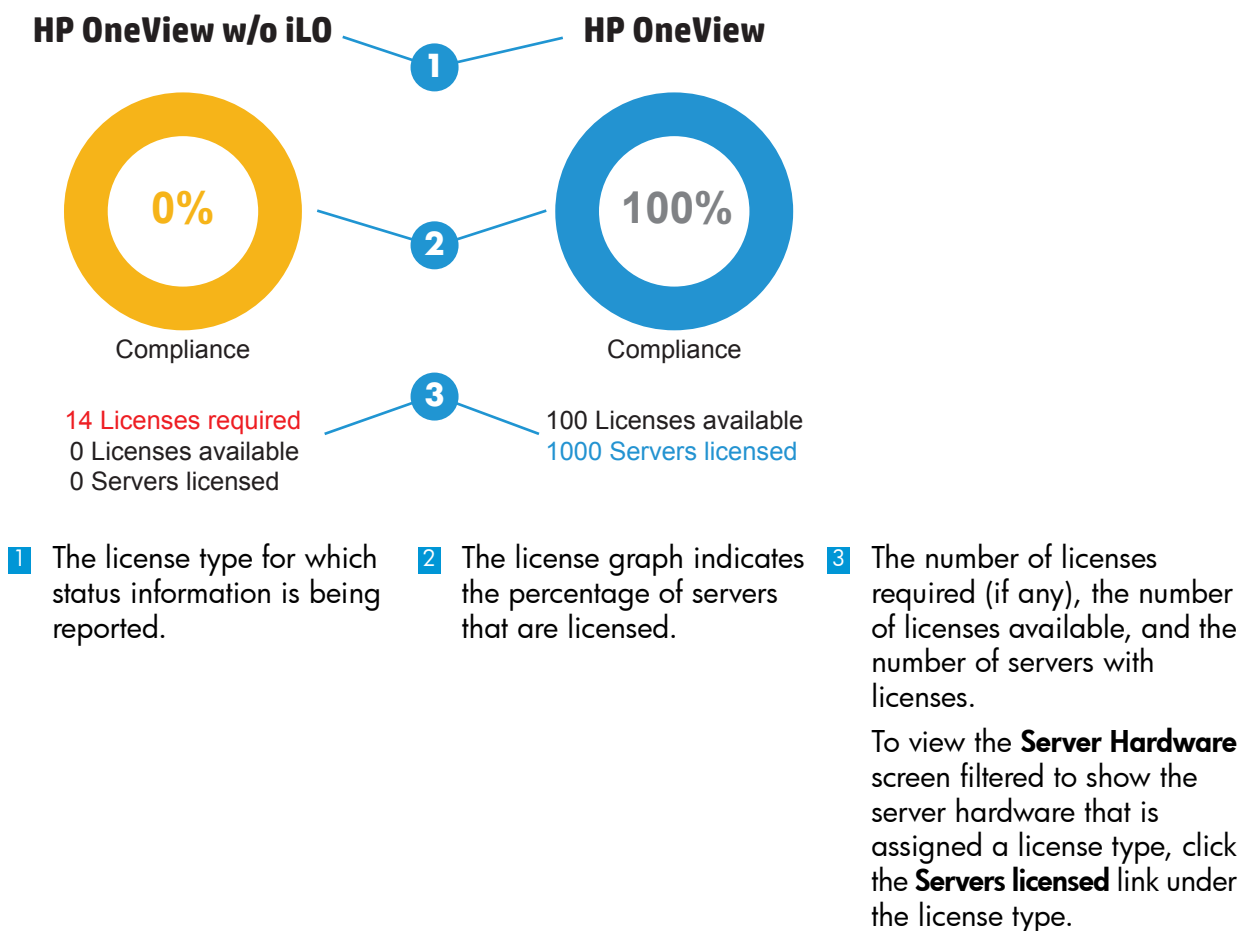
NOTE: You may have to refresh the **Licenses** screen in order for recent license assignments to show up in the license graphs.

The license graphs indicate the number of licenses available and required, and the percentage of server hardware that is in compliance (licensed). A complete blue ring indicates 100% compliance. The number of available licenses is displayed below the graph. The number of licenses required, if any, is displayed in red text.

Table 7 License graph colors

Color	Description
Yellow	Indicates the percentage of server hardware without a license
Blue	Indicates the percentage of server hardware that is licensed
Light Gray	Indicates licenses that are available but have not been assigned

Figure 13 Sample license graphs



22.5.4 Server hardware licensing

The appliance uses server-based licensing, but server blades and rack mount servers are managed differently. Server blade licenses are managed at the enclosure level, and rack mount server licenses are managed at the server level. When you add an enclosure, you specify a license policy for all

server blades in the enclosure. When you add a rack mount server, you specify a license type for that server. Both *policy* and *type* refer to either of the two licenses: HP OneView or HP OneView w/o iLO.

NOTE: The appliance applies embedded (integrated) licenses to the server hardware on which they reside, regardless of the license policy or type you choose.

Licensed features

An HP OneView w/o iLO license provides support for all server hardware features on the appliance, with the following exceptions:

- Server hardware without an iLO Advanced license does not display utilization data.
- Rack mount servers without an iLO Advanced license cannot access the remote console.

22.5.4.1 Server blade licensing at the enclosure level

A server blade licensing policy at the enclosure level is an efficient way to handle licensing for all servers in an enclosure.

When you add an enclosure to the appliance, you must choose a server hardware license policy. This sets the licensing policy for all server hardware in the enclosure. You cannot change the policy for an enclosure unless you remove and re-add the enclosure.

NOTE: A license embedded on a server blade will override the enclosure license policy. If you add a server blade with an embedded license, the appliance assigns the embedded license to that server, regardless of the enclosure license policy.

Enclosure licensing policy behavior

When you add an enclosure to the appliance:

- You must choose a licensing policy: HP OneView or HP OneView w/o iLO.
- A license embedded on the OA is added to the appliance license pool.
- If the server blade does not have an embedded license, the appliance attempts to assign a license from the pool.
- If there are not enough licenses to satisfy the policy, a notification is displayed that instructs you on how to address the issue.
- If you add server blades to the enclosure after it has been added to the appliance, the server hardware will use the enclosure license policy.
- There is no guarantee that an embedded OA license will be applied to the server blades in the enclosure that contains the embedded license.
- Licenses embedded on a server iLO are automatically added to the appliance and applied to the server hardware on which they are embedded.
- If the server hardware has an existing permanent iLO Advanced license, the appliance assigns an HP OneView w/o iLO license, regardless of the license type you choose.
- To change the server hardware license policy of an enclosure, you must remove the enclosure from management and then re-add it with the new license policy.
- When you add server hardware to the appliance, the iLO Advanced license that is part of the HP OneView license is applied to the server hardware iLO.
- If a server blade does not have an iLO license and there are not enough of the selected license type available, the appliance will attempt to apply a demo iLO license to the server blade.

22.5.4.2 Rack mount server licensing

Rack mount server licensing is managed at the server level.

When you add a rack mount server to the appliance, you must choose a license type. You cannot change the license type for a rack mount server unless you remove and re-add it.

NOTE: Embedded licenses take precedent over the license type you choose. If you add a rack mount server with an embedded license, the appliance assigns the license to that rack mount server, regardless of the license type you choose.

Remote console support is not enabled if the rack mount server does not have an iLO license.

Rack mount server licensing behavior

When you add a rack mount server to the appliance:

- You must choose a license type: HP OneView or HP OneView w/o iLO.
- A license embedded on the rack mount server iLO is automatically added to the appliance and applied to the rack mount server.
- If the server hardware has an existing permanent iLO Advanced license, the appliance assigns an HP OneView w/o iLO license, regardless of the license type you choose.
- If the rack mount server does not have an embedded license, the appliance attempts to assign a license from the license pool.
- If there are not enough licenses available, a notification is displayed that instructs you on how to address the issue.
- The iLO Advanced license that is part of your HP OneView license is applied to the iLO when you add a rack mount server.
- To change the license type of a rack mount server that does not have an embedded license, you must remove the rack mount server from management and then re-add it with the new license type.

22.5.4.3 Licensing and utilization statistics

The appliance gathers and reports utilization statistics for server hardware that has an iLO license. Utilization statistics are not available for server hardware that does not have an iLO license.

22.5.4.4 Licensing scenarios

The way in which the appliance handles license assignments depends on the following:

- Whether the enclosure or server hardware has an embedded license
- The license type you choose when you add the enclosure or server hardware
- Whether there are available licenses in the appliance license pool (for server hardware without an embedded license)

The following table describes how the appliance handles licensing for different user actions.

Table 8 Licensing scenarios

User action	License policy or type	Result	Notes
Add enclosure with embedded HP OneView or HP OneView w/o iLO license.	The embedded license takes precedent over the enclosure license policy you select.	Embedded OA licenses are added to the appliance pool and applied to server hardware that is not licensed.	There is no guarantee that licenses embedded on an enclosure will be applied to the server hardware in the enclosure; they might be applied to other server hardware managed by the appliance.
Add server hardware with embedded HP OneView or HP OneView w/o iLO license.	Embedded licenses are applied to the server hardware regardless of the license type you select.	Embedded licenses are assigned to the server hardware on which they reside.	
Add server hardware with an existing, permanent iLO Advanced license.	The server hardware will be assigned an HP OneView w/o iLO license regardless of the license policy or type.	<p>HP OneView w/o iLO Licenses available in the pool</p> <p>The appliance assigns a license to the server hardware.</p> <p>No HP OneView w/o iLO licenses available in the pool</p> <p>The appliance issues a warning that there are not enough licenses to satisfy the policy.</p>	
Add enclosure or server hardware with no embedded license.	Any	<p>Licenses available in the pool</p> <p>The appliance assigns a license to the server hardware.</p> <p>No licenses available in the pool</p> <p>The appliance issues a warning that there are not enough licenses to satisfy the policy.</p>	After the 60-day trial period, a message notifies you when there are not enough licenses for the number of managed server hardware.
Remove server hardware.	HP OneView (applied to server hardware).	The license remains assigned to the server hardware.	<p>If the server hardware is re-added, it will be assigned the same license.</p> <p>Removing server hardware with licenses assigned to them can cause the number of licensed servers shown in the licensing graphs to be greater than the number of servers currently being managed because the licenses are still being counted as assigned to server hardware.</p>
Remove server hardware.	HP OneView w/o iLO or HP OneView (license not yet applied to server).	The license is unassigned from the server hardware.	

22.6 Updating the appliance

The appliance runs a combination of software and firmware. Keeping the appliance up to date fixes problems, improves performance, and adds any new features to the appliance.

The appliance does not check for updates automatically. View the installed version of the appliance firmware from the **Appliance General** view of the **Settings** screen or by using the REST APIs, and

then verify if a newer version of an appliance update file is available to download from <http://www.hp.com/go/oneviewupdates>. Before you install an appliance update, you can examine the release notes to determine new features, restrictions, and whether or not you must restart the appliance after you install the update.

NOTE: The release notes for an update are not available after you install the update and should be printed off for future reference.

You manage appliance updates from the **Settings**→**Actions**→**Update appliance** menu or by using the REST APIs. An appliance update is installed from a single file during the update process. You can either download the file directly to the appliance or to another computer and then transfer the file to the appliance.

UI screens and REST API resources

UI screen	REST API resource
Settings	appliance/firmware

22.6.1 Roles

- Minimum required privileges: Infrastructure administrator

22.6.2 Tasks

Updating the appliance requires a single user accessing the appliance and causes the appliance to restart. This does not disrupt the operation of the devices under management, but does result in an outage of the appliance.

The appliance online help provides information about using the UI or the REST APIs to:

- Determine if a newer appliance update is available. (Minimum required privileges: Read only, Network administrator, or Infrastructure administrator)
- Update the appliance. (Minimum required privileges: Infrastructure administrator)

22.6.3 Learning more

For more information about obtaining software updates, see [“Support and other resources”](#) (page 227).

23 About unsupported and unmanaged hardware

Unmanaged and unsupported devices are devices that the appliance does not manage. Adding unmanaged and unsupported devices to the appliance allow tracking, inventory, and power management.

23.1 How the appliance handles unsupported hardware

Unsupported hardware is any device that the appliance cannot manage. Unsupported devices are similar to unmanaged devices in that all unsupported devices are not managed by the appliance. The difference is that you can bring unmanaged devices under management of the appliance if you take the appropriate actions or properly configure them. Unsupported hardware can never be managed by the appliance.

The appliance detects the unsupported hardware and displays the model name and other basic information that it obtains from the device for inventory purposes. The appliance also accounts for the physical space unsupported devices occupy in enclosures and racks.

To account for the space a device occupies, the appliance represents unsupported hardware the same way it represents unmanaged devices.

The only action available for unsupported hardware is **Remove**.

23.2 About unmanaged devices

An unmanaged device is a device, such as a server, enclosure, KVM (keyboard, video and mouse) switch, in-rack monitor/keyboard, or router, that occupies space in a rack and/or consumes power but is not managed by the appliance.

Unmanaged devices are created automatically to represent devices that are attached to an HP Intelligent Power Distribution Unit (iPDU) using HP Power Discovery Services connections. BladeSystem enclosures and HP ProLiant DL series servers are shown in the `unmanaged` or `unsupported` state in the **Enclosures** and **Server Hardware** in the master pane, respectively. These will be represented as unmanaged enclosures and servers; as such, they are not included in the **Unmanaged Devices** resource list.

When creating an unmanaged device, you provide its name, model description, height in U-slots and maximum power requirements. These values are used in power and cooling capacity analysis and enables alerts to be generated identify potential power and cooling issues.

Because there is no communication to the unmanaged device, it is always shown with `disabled` status unless appliance-generated alerts identify issues to be addressed.

For purposes of power configuration, unmanaged devices are assumed to have two power supply connections to support redundant power. These are identified as power supplies 1 and 2. If an unmanaged device does not support redundant power, connect only power supply 1, then clear the alert about lack of redundant power to the device.

For devices that are not discovered through HP Power Discovery Services connections, you can manually add these devices to the appliance for tracking, inventory, and power management purposes.

Part V Monitoring

The chapters in this part describe using the appliance to monitor your data center. You use the information in this part after the appliance has been configured and the data center resources have been added to the appliance.

24 Monitoring data center status, health, and performance

This chapter describes the recommended best practices for monitoring data center status, health, and performance using HP OneView.

24.1 Daily monitoring

As part of the daily monitoring of your data center, it is important to be able to quickly scan the appliance-managed resources to assess the overall health of your data center. By reviewing the UI screens, you are able to rapidly analyze the state and condition of your data center.

24.1.1 Initial check: the **Dashboard**

The **Dashboard** provides an at-a-glance visual health summary of the appliance resources you are authorized to view. The **Dashboard** can display a health summary of the following:

- Server Profiles
- Server Hardware
- Enclosures
- Logical Interconnects
- Appliance alerts

The status of each resource is indicated by a color: green indicates OK, yellow indicates a warning, and red indicates a critical condition. You can link to the resource screens in the UI for more information by clicking on the status icons displayed for each resource.

To learn more about the **Dashboard** screen, see [“Using the Dashboard screen” \(page 176\)](#).

24.1.2 Activities

The **Activity** screen provides a log of health and status notifications. The appliance verifies the current activity of resources in your environment, and posts alerts to the **Activity** screen and to the associated resource screens for you to review.

The **Activity** screen is also a database of all tasks that have been run, either synchronously or asynchronously, and initiated by the user or system. It is similar to an audit log, but provides more detail and is easily accessed from the UI.

To learn more about activities, see [“About activities” \(page 173\)](#).

24.1.3 Utilization graphs

For certain resources, the appliance collects CPU, power, and temperature utilization statistics from management processors (the iLO, Onboard Administrator, and iPDU). Utilization graphs enable you to understand recent utilization statistics relative to available capacity, see utilization trends over time, and see historical utilization over time. Hover over the utilization area in the UI to display tool tips.

The Enclosures screen	View historical metrics of power consumption (average, peak, and power cap) and temperature.
The Server Hardware screen	View historical metrics of CPU utilization/CPU frequency, power consumption (average, peak, and power cap), and temperature.
The Power Delivery Devices screen	View historical metrics of power consumption (average and peak and previous 5 minutes, previous 24 hours).
The Interconnects screen	View uplink port statistics of the bit transfer rates (transmitted and received).

To learn more about utilization graphs, see [“Monitoring power and temperature”](#) (page 179).

24.1.4 Monitor data center temperature

The appliance provides detailed monitoring data that you can use to determine the power and cooling capabilities of the devices in your data center. The overall cooling in your data center might be sufficient; however, there might be areas that are insufficiently cooled due to conditions such as poor airflow, concentration of excessive heat output, or wrap-around airflow at the ends of aisles. To easily identify temperature issues and look for thermal hotspots in all areas in your data center, use the 3D visualization features provided by the Data Centers UI screen.

To learn more about temperature, see [“Monitoring power and temperature”](#) (page 179).

24.2 Best practices for monitoring data centers

The following are recommended best practices for using HP OneView appliance to ensure the health of the managed components in your data center environment.

24.2.1 Best practices for monitoring health with the appliance UI

HP recommends the following best practices to monitor the health of the managed resources in your environment.

NOTE: The status represented for all HP OneView resources represents the status for that single resource and does not represent the roll-up status of sub-components. For example, the status for an enclosure does not aggregate status for all blades and servers, but rather just the status of the enclosure (Onboard Administrator, fans, and power supplies).

General health monitoring steps

Monitoring step	Related information
1. Navigate to the Activity screen and filter activities, using the filtering options that work best for the situation. You can also start from the Dashboard screen to see alerts for specific resources.	“About activities” (page 173) “Using the Dashboard screen” (page 176)
2. Navigate to a specific resource screen to view the specific activities for that resource. On the resource screen, verify the state of the resource instances via health status icons.	“Icon descriptions” (page 62)
3. Investigate each resource instance with a warning or error status.	
4. Expand critical and warning alerts to see their full descriptions, and click Event details to view additional information about the event(s) that caused the alert.	
5. Follow the instructions in the recommended resolution (if any) or research the alert to correct the problem.	

Server hardware health monitoring

For server hardware with a **Critical** or **Warning** status, the associated server profile might be in failed state, so you need to verify it as well.

Monitoring step	Related information
1. Expand the server hardware alert to see more information. You can view alerts from the Server Hardware screen, Activity screen, or the Dashboard screen.	See the UI help for Server Hardware and “About activities” (page 173).
2. Follow the instructions in the recommended resolution (if any) or research the alert to correct the problem.	
3. Ensure the server profile was properly assigned to the server hardware.	See the UI help for Server Profiles .

Network health monitoring

To monitor the current health of a network, navigate to the **Interconnects** and **Logical Interconnects** resources to view recent activity, alerts and notifications, and current health status.

- For interconnects, a healthy state is **Configured**
- For logical interconnects, a healthy state for stacking is **Redundantly Connected**

Monitoring step	Related information
1. View the activities and states for logical interconnects. View the health of Downlink ports and Uplink ports on the Interconnects screen. View the Stacking mode of the interconnects on the Logical Interconnects screen.	See the UI help for Logical Interconnects .
2. Follow the instructions in the recommended resolution (if any) or research the alert to correct the problem.	“About activities” (page 173)

24.2.2 Best practices for monitoring health using REST APIs

To ensure the health of the managed components in your data center environment, follow these best practices.

- Overall health monitoring
- Server hardware health monitoring
- Network health monitoring

Overall health monitoring

Monitoring step
<ul style="list-style-type: none">• Filter alerts based on severity or date to view current health issues. <pre>GET /rest/alerts?filter="severity='{UNKNOWN, OK, WARNING, CRITICAL}'"&filter="created='{YYYY-MM-DDThh:mm:ssZ}'"</pre>NOTE: The DISABLED severity is not applicable to alerts. See the <i>REST API scripting</i> chapter in the online help for more information about alerts.
<ul style="list-style-type: none">• Get alerts for a specific physical resource type, such as server hardware. <pre>GET /rest/alerts?filter="physicalResourceType='{physical_server}'"</pre> See the <i>REST API scripting</i> chapter in the online help for more information about server hardware.

Monitoring step

View the originating event(s) that caused a specific alert.

1. Select an alert.

```
GET /rest/alerts/
```

2. Get a specific alert using the alert ID.

```
GET /rest/alerts/{id}
```

3. Get the associated event(s).

```
GET /rest/events/{id}
```

- Fix the problem. Use the recommended fix (perform a GET operation on the specific alert resource and view the `correctiveAction` attribute), or research the alert.

Server hardware health monitoring

A server or servers turn to a warning or critical status when something is not correct within the appliance. If a server profile has been applied to a failed server, the server profile will also be in a failed status.

Monitoring step

- Use details from the alert to fix the problem. When available, attempt the recommended fix first. In some cases, additional research of the alert might be needed to best determine the fix.

```
GET /rest/alerts?filter="physicalResourceType='{physical_servers}'"&filter="severity='{WARNING, CRITICAL}'"
```

See the *REST API scripting* chapter in the online help for more information on alerts.

- Make sure that server profiles are appropriately assigned to the server hardware.

See the *REST API scripting* chapter in the online help for more information on server profiles.

Network health monitoring

To determine the current health of a network or networks on the appliance, view alerts for interconnects and logical interconnects to verify the correct connections. To list alerts, you can

perform a GET operation on alerts and filter for alerts related to interconnects. To list states, you can perform a GET operation on interconnects and logical interconnects and filter for an OK state.

Monitoring step
<p>View alerts for interconnects.</p> <ol style="list-style-type: none">1. Select an interconnect alert. <pre>GET /rest/alerts?filter="physicalResourceType='{interconnect}'"&filter="severity='{WARNING, CRITICAL}' "</pre>2. Get a specific alert using the alert ID. <pre>GET /rest/alerts/{id}</pre> <p>See the <i>REST API scripting</i> chapter in the online help for more information on interconnects.</p>
<p>Filter for logical interconnects with unhealthy stacking.</p> <ol style="list-style-type: none">1. Get unhealthy logical interconnect. <pre>GET /rest/logical-interconnects?filter="stackingHealth='{Unknown, Disconnected}' "</pre>2. View specific unhealthy interconnect using the interconnect ID. <pre>GET /rest/logical-interconnects/{id}</pre> <p>See the <i>REST API scripting</i> chapter in the online help for more information on logical interconnects.</p>
<ul style="list-style-type: none">• Use information provided in the alert to fix the problem. Use the recommended fix if there is one, or research the alert. <p>See the <i>REST API scripting</i> chapter in the online help for more information on alerts.</p>

24.3 Managing activities

The appliance online help provides information about using the UI or the REST APIs to:

- View activities for a resource.
- Filter activities by health and status.
- Filter activities by date.
- Assign an owner to an alert.
- Add a note to an alert.
- Clear an alert.
- Restore a cleared activity to the active state.

24.3.1 About activities

An activity is a record of a user- or system-initiated action or task or an alert message to inform you that an event occurred that requires your attention.

An alert message is an important troubleshooting tool. It indicates when an event occurred and which resource reported it. An alert message provides details about the event and suggests a solution.

If a user- or system-initiated action is complete, there is a record for it. If an action is not complete, you can see which subtasks were completed or are still running and which subtasks are interrupted or stopped.

The appliance interleaves tasks, alerts, and administrator's notes into a single view, which simplifies the correlation of user activity with system health.

You can view all activities, filter the activities by several criteria to view only those you want to see, or search for a specific activity.

You can assign alerts to the appropriate administrator for their timely resolution. When issues are investigated and resolved, you can clear them so they no longer require your attention.

You can annotate alert messages to keep an historical record of issues and their resolutions, or you can note a decision that affected the alert resolution.

24.3.1.1 Activity types: alerts and tasks

24.3.1.1.1 About alerts

The appliance uses alert messages to report issues with the resources it manages. An alert represents an event for a given resource that typically originates from the resource.

An event describes a single problem or change that occurred on a resource. For example, an event might be an SNMP trap received from a server's Integrated Lights-Out (iLO) management processor.

Each alert has a severity, a state, a description, and an urgency. A user with the proper privileges can clear alerts, assign owners to alerts, and add notes to alerts.

Resources generate alerts to notify you that some action is required.

Alerts contribute to a resource's overall displayed status, but only if the alerts are still active (that is, you have not changed their state to `Cleared`).



IMPORTANT:

The appliance stores up to 75,000 alert messages. Every 500 alert messages, the appliance determines if the maximum of 75,000 was exceeded. If it has, an auto-cleanup occurs. The auto-cleanup deletes alert messages in the following order until the total number is fewer than 74,200:

- Oldest cleared alerts
- Oldest alerts by severity

These stored alert messages differ from the database of stored tasks.

24.3.1.1.2 About tasks

All user- or system-initiated tasks are reported as activities:

- User-initiated tasks are created when a user adds, creates, removes, updates, or deletes resources.
- Other tasks are created by processes running on the appliance, such as gathering utilization data for a server.

The task log provides a valuable source of monitoring and troubleshooting information that you can use to resolve an issue. You can determine the type of task performed, whether the task was completed, when the task was completed, and who initiated the task.

The types of tasks are:

Task type	Description
User	A user-initiated task, such as creating, editing, or removing an enclosure group or a network set
Appliance	An appliance-initiated task, such as updating utilization data
Background	A task performed in the background. This type of task is not displayed in the log.

- ❗ **IMPORTANT:** The appliance maintains a tasks database that holds information for approximately 6 month's worth of tasks or 50,000 tasks. If the tasks database exceeds 50,000 tasks, blocks of 500 tasks are deleted until the count is fewer than 50,000. Tasks older than 6 months are removed from the database.

The tasks database is different from the stored alerts.

24.3.1.2 Activity states

Activity	State	Description
Alert	Active	The issue or problem still exists A resource's active alerts help determine its health status. Active alerts contribute to the count summaries.
	Locked	An Active alert that was set (locked) by an internal resource manager. You cannot manually clear a Locked alert. Examine the corrective action associated with an alert to determine how to fix the problem. After the problem is fixed, the resource manager moves the alert to the Active state. At that time, you can clear or delete the alert. A resource's locked alerts contribute to its overall status.
	Cleared	The alert is no longer a concern and does not affect the resource health status. Cleared activities are not counted in the displayed summaries.
Task	Completed	The task started and ran to completion.
	Running	The task started and is running, but has not yet completed.
	Pending	The task has not yet run.
	Interrupted	The task ran, but was interrupted; for example, it could be waiting for a resource
	Error	A task failed or generated a Critical alert. Investigate Error states immediately.
	Warning	An event occurred that might require your attention. It can mean that something is not correct within the appliance. Investigate Warning states immediately.

24.3.1.3 Activity statuses

Status	Description
Critical	A critical alert message was received, or a task failed or was interrupted. Investigate Critical status activities immediately.
Warning	An event occurred that might require your attention. It can mean that something is not correct within the appliance and it needs your attention. Investigate Warning status activities immediately.
OK	For an alert, OK indicates normal behavior or information from a resource. For a task, OK indicates that it completed successfully.

Status	Description
Unknown	The status of the alert or task is unknown. The status of a task that is set to run at a later time is <code>Unknown</code> .
Disabled	A task was prevented from continuing or completing; for example, this could indicate a canceled file upload.

24.4 Using the Dashboard screen

24.4.1 About the Dashboard

The **Dashboard** provides a graphical representation of the general health status of several managed resources in your data center. From the **Dashboard**, you can immediately see the areas that need your attention. For direct access to resources needing your attention, select the resource name for a filtered view.

Each time you log in to the appliance, the **Dashboard** is the first screen you see. To view the dashboard graphs, select **Dashboard** from the [main menu](#).

Only those resources you are authorized to view or manage appear on the **Dashboard**.

See [“How to interpret the Dashboard graphs” \(page 176\)](#) to learn more about the resource health and capacity information that appears on the **Dashboard**.

24.4.2 Dashboard screen details

Hover your pointing device on a graph slice to view the count of resource instances being represented by that slice. Hovering your pointing device on a graph slice changes the text and count displayed in the center of the graph.

The following graphs appear on the **Dashboard**:

Graph name	Description
Status	<p>The Status graphs summarize the health status of several resources.</p> <p>The number displayed next to the resource name indicates the total number of instances of that resource that are known to the appliance. To learn more about a resource, click the resource name to display its main screen.</p> <p>In Status graphs, the dark gray color indicates the number of resources that are not reporting information because they are either disabled or are not being managed by the appliance.</p> <p>To filter the view of a resource based on its status, click the status icon.</p> <p>To learn more about health status and severity icons, see “Icon descriptions” (page 62).</p>
Servers with profiles for Server Hardware	The default view of the Servers with profiles graph reports the count of server hardware instances with assigned server profiles. If the graph is not solid blue, hover your pointing device on the light gray graph slice to see the count of servers without profiles.
Populated blade bays for Enclosures	The default view of the Populated blade bays graph reports the count of server hardware instances in all managed enclosure bays. If the graph is not solid blue, hover your pointing device on the light gray graph slice to see the count of empty blade bays.

24.4.3 How to interpret the Dashboard graphs

Dashboard graph colors provide a quick way to visually interpret the data being reported.

Table 9 Dashboard graph colors

Color	Indication
Green	A healthy status
Yellow	An event has occurred that might require your attention

Table 9 Dashboard graph colors *(continued)*

Color	Indication
Red	A critical condition that requires your immediate attention
Blue	The percentage of resource instances that match the data being measured (a solid blue graph indicates 100%)
Light gray	The remainder of resource instances that do not match the data being measured (used in combination with blue)
Dark gray	Resource instances reporting status other than OK, Warning, or Critical, that is, they are Disabled or Unknown

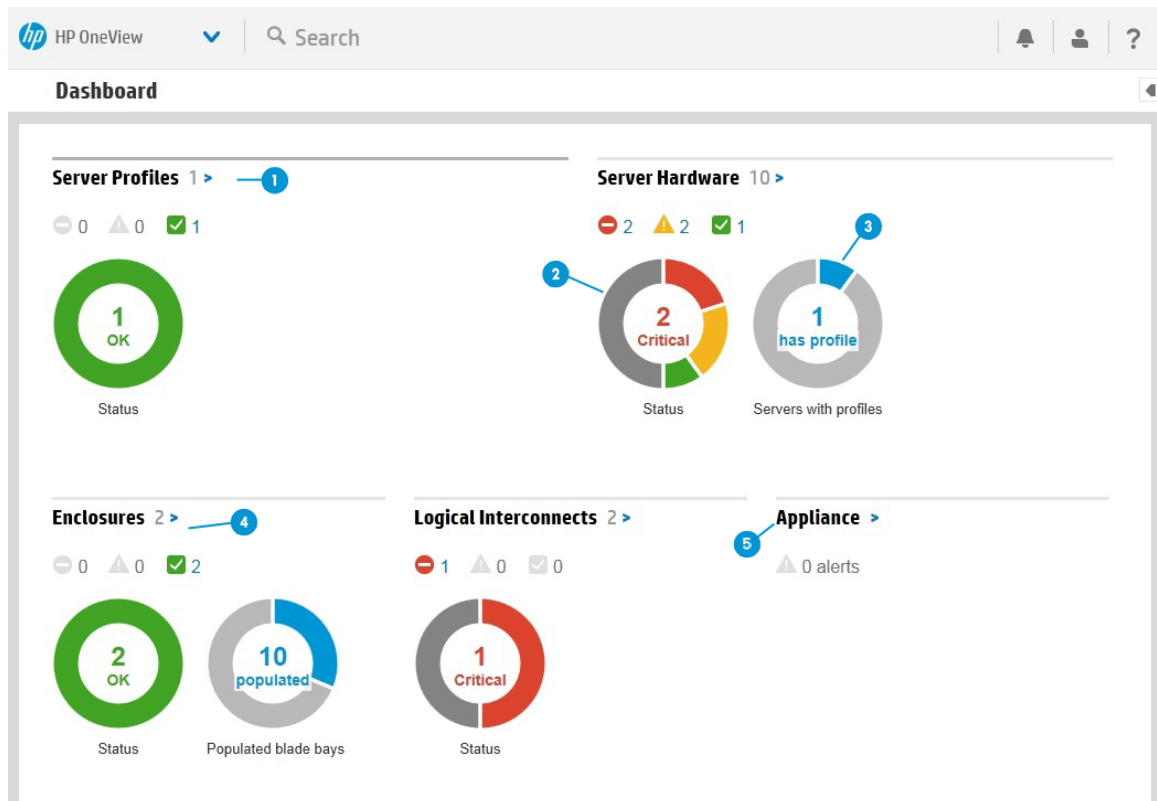
Status icons

To assist you in identifying resources that are not in a healthy state, status icons indicate the number of resources with a status of OK (✓), Warning (⚠), or Critical (✖).

You can select a status icon to view the resource's main screen, with resource instances filtered by that status. If no resources are defined or if no resource instances are detected with a particular status (indicated by the number zero), the associated icon is nearly colorless (very pale gray).

To learn how to interpret the data displayed on the graphs, see the numbered descriptions that appear after the sample dashboard.

Figure 14 Sample Dashboard



- 1 Click a resource name to view the resource's main screen for more information. The adjacent number identifies how many instances of that resource are being managed by the appliance. In this example, one server profile has been created on the appliance, and it is in a healthy state.
- 2 On a **Status** graph, a dark gray slice represents the count of resources that are reporting a status of Disabled and Unknown.

The sample graph for the **Server Hardware** resource shows a total of ten instances of managed server hardware, of which half are either disabled or are unknown devices. Hover your pointing device on the dark gray slice to see a count of server hardware instances with a **Disabled** and **Unknown** status.

Two instances of server hardware are in a **Critical** state, and two have a **Warning** associated with them. Click the status icon to open the **Server Hardware** to begin investigating the cause, perhaps from the resource **Activity** or **Map** views.

- 3 On the **Servers with profiles** graph, the color blue reports the count of server hardware instances with server profiles assigned to them. In this example, one server has a profile assigned to it, the other instances do not. Hover your pointing device over the light gray graph slice to see a count of server hardware instances without profiles assigned.
- 4 For the **Enclosures** resource, two enclosures (with a capacity of 32 server blades) are being managed and are reporting a healthy status. Ten enclosure bays are populated with server hardware. Hover your pointing device over the grey graph slice to see how many bays are empty.
- 5 The **Appliance** panel provides important appliance-related alerts, typically backup and licensing issues. Alerts related to other resources are not included.

If one appliance alert is detected, the alert text appears here. For multiple alerts, the number of alerts are shown, and you can click **Appliance** to go directly to the **Activity** screen to see a filtered view of all appliance-related alerts.

See [“About activities” \(page 173\)](#) to learn more about alerts.

25 Monitoring power and temperature

HP OneView enables you to monitor the power and temperature of your hardware environment.

Power and temperature monitoring feature overview

The appliance:

- Displays 3D color-coded hardware temperature visualization (UI only)
- Collects and reports power metric statistics
- Collects and reports temperature metric statistics
- Displays utilization statistics using customizable utilization graphs (UI only)

Power and temperature monitoring features by resource

- **Data Centers**
 - Color-coded temperature visualization of racks and the server hardware in them
- **Enclosures and Server Hardware**
 - Alerts for degraded and critical temperature and power
 - Proactive analysis and alerting for power configuration errors
 - Utilization graphs for power and temperature statistics
- **Power Delivery Devices**
 - Alerts on power thresholds
 - Proactive analysis and alerting for power configuration errors
- **Racks**
 - Proactive analysis and alerting for power configuration errors

25.1 UI power and temperature monitoring

Data Centers screen

Data Centers screen provides a [3D visualization](#) of your hardware environment, and uses a color-coded system to display temperature data for your hardware.

The [Utilization panel](#) and [Utilization graphs](#)

Utilization [power](#) and [temperature](#) statistics are displayed on the **Utilization** panel and via utilization graphs in the **Utilization** view on the **Enclosures**, **Interconnects** (utilization graphs only), **Power Delivery Devices**, and **Server Hardware** screens.

25.1.1 Monitoring data center temperature

The **Data Centers** resource provides a visualization of the racks in your data center and displays their peak temperature using a color-coded system. To enable this, you must first specify the physical positions of your racks and the position of the components in them using the **Data Centers** resource. You can use temperature visualization to identify over-cooled areas of your data center. You can close vent tiles in areas that have low peak temperatures to increase airflow to areas that have insufficient cooling. If the entire data center is over-cooled, you can raise the temperature to save on cooling costs.

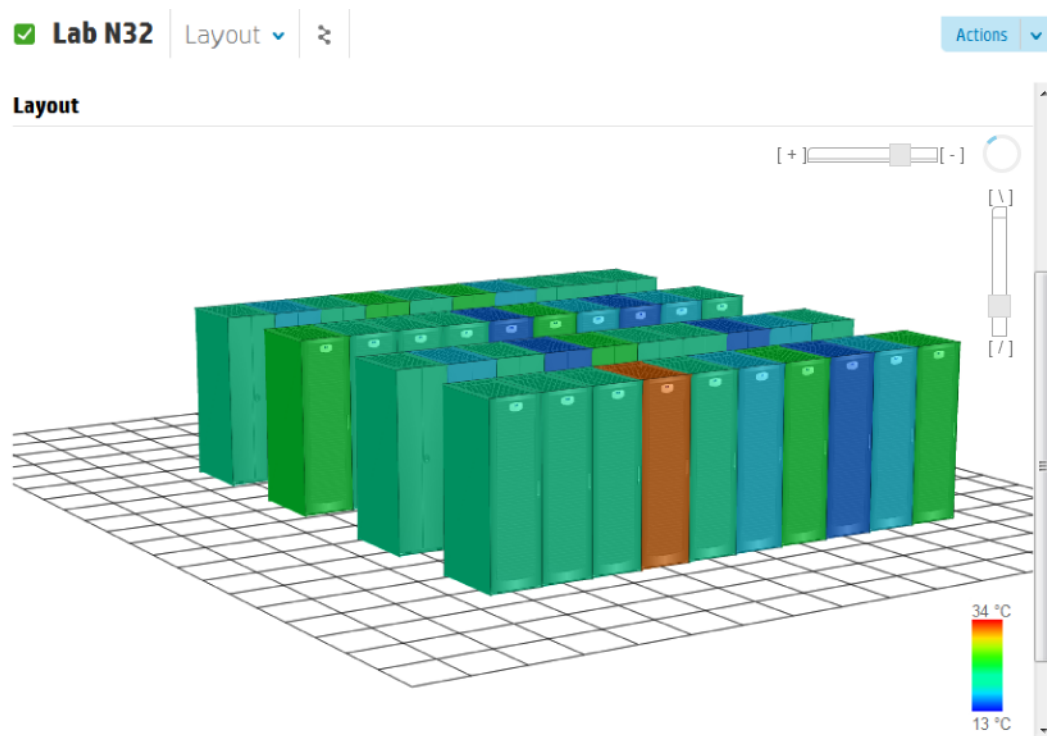
Prerequisites

- Minimum required privileges: Server administrator.
- You have created a data center and positioned your racks in it.
- The placement of racks in your data center accurately depicts their physical locations.
- You have specified a thermal limit for your rack using the **Racks** screen, if your policy dictates a limit (optional).

Temperature collection and visualization details

- The visualization displays peak rack temperature using a color-coded system. The rack is colored based on the highest peak temperature (over the last 24 hours) of the device in the rack with the highest peak temperature recorded (of devices which support ambient temperature history reporting).
- Temperatures are determined using the temperature utilization data collected from each device.
- Background data collection occurs at least once a day, so the reported peak temperature for a rack will be within the past 48 hours.
- Racks without an observed peak temperature with 48 hours are depicted without color coding (gray).

Figure 15 3D data center visualization



25.1.1.1 Manipulating the view of the data center visualization

You can zoom in or zoom out and adjust the viewing angle of the data center from the **Overview** view or **Layout** view of the **Data Centers** screen.

Prerequisites

- Minimum required privileges: Server administrator

NOTE: The data center view controls do not appear in the **Layout** panel of the **Overview** view until you hover your pointing device over the panel.

Manipulating the view of the data center visualization

To change the data center view, do one or more of the following:

- Move the horizontal slider left to zoom in and right to zoom out.
- Move the vertical slider up and down to change the vertical viewing angle.
- Click and drag the rotation dial to change the horizontal viewing angle.

25.1.2 Monitoring power and temperature utilization

Utilization statistics for power and temperature are displayed on:

- The [Utilization panel](#)
- [Utilization graphs](#) in the **Utilization** view
 - [Power utilization metrics](#)
 - [Temperature utilization metrics](#)

25.1.2.1 About the Utilization panel

The **Enclosures**, **Power Delivery Devices**, and **Server Hardware** screens display a **Utilization** panel in the **Overview** for each resource.

The possible states of the **Utilization** panel are:

Panel contents	Reason
Utilization meters display utilization data.	The appliance has collected data and it is being displayed.
A licensing message is displayed.	Server hardware without an iLO Advanced license will not display utilization data.
no data is displayed.	The appliance has not collected data during the previous 24 hours.
not set is displayed (a gray meter with hash marks).	The meter might not be set for the following reasons: <ul style="list-style-type: none">• The page is loading and the data is not yet available.• There is no utilization data prior to the most recent 5-minute collection period. There may be historic data in the utilization graphs.• Enclosures will not display temperature data if none of the server blades are powered on.
not supported is displayed.	Utilization data gathering is not supported on the device.

See the online help for **Utilization** for more information.

25.1.2.2 About utilization graphs

The appliance gathers and reports CPU, power consumption, and temperature data for certain resources via utilization graphs.

NOTE: The minimum data collection interval is five minutes (averaged) and the maximum is one hour (averaged).

Utilization graphs can display a range of data up to a maximum of three years.

Table 10 Utilization statistics gathered by resource

Resource	Utilization metric			
	CPU	Power	Temperature	Custom
Enclosures		✓	✓	✓
Power Delivery Devices		✓		
Server Hardware	✓	✓	✓	✓

NOTE: You can use the **Interconnects** screen to view utilization graphs that display data transfer statistics for interconnect ports. See the online help for the **Interconnects** screen.

Utilization statistics and licensing

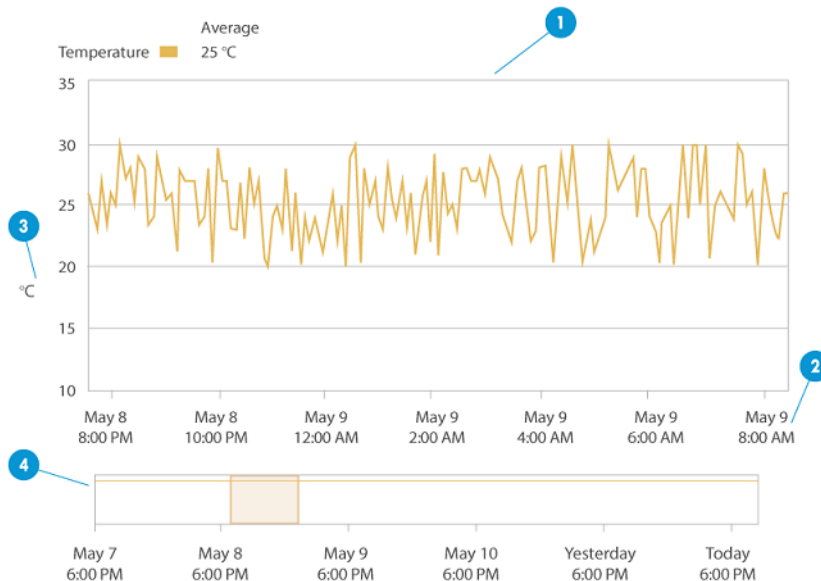
Utilization statistics and graphs are disabled for server hardware that does not have an iLO license assigned. See [“About licensing”](#) (page 159) to learn more.

If utilization is disabled, the **Utilization** panel displays a message stating the reason it is disabled in the details pane for the unlicensed resource.

Utilization graphs

Utilization

▼ Temperature



1 Primary graph: The large primary utilization graph displays metric data (vertical axis) for your devices over an interval of time (horizontal axis) using a line to graph data points.

2 Horizontal axis: The horizontal axis on the primary utilization graph depicts the time interval for the data being displayed,

3 Vertical axis: The vertical axis on the primary utilization graph depicts the interval for the metric displayed in the corresponding unit of measurement down the left side of the graph. The interval for each unit of measurement is fixed and cannot be changed. Graphs that display two metrics with

4 Navigation graph: The navigation graph below the primary graph displays the maximum time interval of available data. Use the navigation graph to select the time interval you want to display in the primary graph by highlighting the interval with your pointing device.

with the most recent interval data on the right. The minimum time interval is two minutes and the maximum is five days.

different units of measurement have a second interval down the right side of the graph. The measurement value at the top of the graph represents the maximum utilization capacity for a given metric.

See the online help for more information on creating a custom utilization graph and how to change the level of detail that the graph displays.

25.1.2.2.1 Power utilization metrics

Power capacity is the calibrated maximum power that a device can consume. Use this data to determine how much power your facility is consuming and the resources that are consuming it. The appliance reports Alerts for devices that exceed their power capacity.

Metric	Description						
Average power	The average amount of power the resource is consuming						
Peak power	The peak amount of power consumed by the resource						
Power cap	<div>Most server hardware and enclosures support control of power consumption through a Dynamic Power Cap. When reporting power utilization, the appliance includes both average and peak power consumption as well as Dynamic Power Cap settings in its graphs. The appliance controls power caps through iLO or enclosure OA.</div> <table><tr><th>Resource</th><th>Description</th></tr><tr><td>Enclosures</td><td><div>The power consumption or cooling limitation on the enclosure.</div><div>When you set the Dynamic Power Cap on an enclosure, it keeps the power used by the enclosure under the cap by managing the power consumption of server hardware.</div><div>To set power limits on an enclosure, select the Power thermal→Power management menu item on the enclosure OA.</div><div>The Dynamic Power Cap limits the enclosure power consumption based on a cooling limit that might be lower than the Derated circuit capacity.</div><div>The Average power cannot exceed the Power cap or the Derated circuit capacity.</div><div>The Peak power cannot exceed the Rated circuit capacity.</div></td></tr><tr><td>Server Hardware</td><td>The limitation on power consumption enforced by the management processor, in watts.</td></tr></table>	Resource	Description	Enclosures	<div>The power consumption or cooling limitation on the enclosure.</div> <div>When you set the Dynamic Power Cap on an enclosure, it keeps the power used by the enclosure under the cap by managing the power consumption of server hardware.</div> <div>To set power limits on an enclosure, select the Power thermal→Power management menu item on the enclosure OA.</div> <div>The Dynamic Power Cap limits the enclosure power consumption based on a cooling limit that might be lower than the Derated circuit capacity.</div> <div>The Average power cannot exceed the Power cap or the Derated circuit capacity.</div> <div>The Peak power cannot exceed the Rated circuit capacity.</div>	Server Hardware	The limitation on power consumption enforced by the management processor, in watts.
Resource	Description						
Enclosures	<div>The power consumption or cooling limitation on the enclosure.</div> <div>When you set the Dynamic Power Cap on an enclosure, it keeps the power used by the enclosure under the cap by managing the power consumption of server hardware.</div> <div>To set power limits on an enclosure, select the Power thermal→Power management menu item on the enclosure OA.</div> <div>The Dynamic Power Cap limits the enclosure power consumption based on a cooling limit that might be lower than the Derated circuit capacity.</div> <div>The Average power cannot exceed the Power cap or the Derated circuit capacity.</div> <div>The Peak power cannot exceed the Rated circuit capacity.</div>						
Server Hardware	The limitation on power consumption enforced by the management processor, in watts.						

25.1.2.2.2 Temperature utilization metrics

Temperature utilization graphs display the ambient/inlet air temperature of your data center. The air temperature is detected by sensors embedded on the front of enclosures and other hardware devices.

The operating threshold is 10°C to 35°C (50°F to 95°F). When the device reaches a threshold, it generates temperature alerts. The appliance displays these alerts in the notification banner and in the **Activity** sidebar.

NOTE: The temperature is displayed in degrees Celsius or Fahrenheit, depending upon the locale setting of your browser.

25.2 REST API power and temperature monitoring

25.2.1 Update enclosure power capacity settings

To update the enclosure capacity settings, perform a `PUT` operation that includes only the `calibratedMaxPower` attribute. View the enclosure capacity settings attributes by using a `GET` operation, edit the `calibratedMaxPower` attribute, and then perform a `PUT` operation that includes only the edited `calibratedMaxPower` attribute.

Prerequisites

- Minimum required session ID privileges: Server administrator

Updating enclosure capacity settings using REST APIs

1. Select an enclosure URI.
`GET /rest/enclosures`
 2. Get the enclosure capacity using the URI from step 1.
`GET {enclosure URI}/environmentalConfiguration`
 3. Edit the enclosure capacity. The only attribute to send in the response body is `calibratedMaxPower`. Do not send all attributes from the `GET` operation.
 4. Update the enclosure capacity.
`PUT {enclosure URI}/environmentalConfiguration`
-

25.2.2 Update server hardware power capacity settings

To update server hardware capacity settings, perform a `PUT` operation that includes only the `calibratedMaxPower` attribute. View server hardware capacity settings attributes by using a `GET` operation, edit the `calibratedMaxPower` attribute, and then perform a `PUT` operation that includes only the edited `calibratedMaxPower` attribute.

Prerequisites

- Minimum required session ID privileges: Server administrator

Updating server hardware capacity settings using REST APIs

1. Select a server hardware URI.
`GET /rest/server-hardware`
 2. Get the current server hardware capacity using the URI from step 1.
`GET {server hardware URI}/environmentalConfiguration`
 3. Edit the server hardware capacity. The only attribute to send in the response body is `calibratedMaxPower`. Do not send all attributes from the `GET` operation.
 4. Update the server hardware capacity.
`PUT {server hardware URI}/environmentalConfiguration`
-

26 Using the State-Change Message Bus (SCMB)

The State-Change Message Bus (SCMB) is an interface that uses asynchronous messaging to notify subscribers of changes to managed resources—both logical and physical. For example, you can program applications to receive notifications when new server hardware is added to the managed environment or when the health status of physical resources changes—without having to continuously poll the appliance for status using the REST APIs.

HP OneView resources publish messages to the SCMB when they are created, updated, or deleted. The message content is sent in JSON format and includes the resource's Data Transfer Object.

To use the SCMB, you must:

1. Use REST APIs to create and download an AMQP certificate from the appliance.
2. Connect to the SCMB using one or both of these methods:
 - Use the "EXTERNAL" authentication mechanism
 - Connect without sending a user name and password

Using one of these methods ensures that certificate-based authentication is used.

3. Set up a queue with an empty queue name.
4. AMQP generates a unique queue name.

You use this queue name to bind to exchanges and receive messages.

To view the list of HP OneView resources that publish messages, see the *HP OneView REST API Reference* in the online help.

26.1 Connect to the SCMB

Before you connect a client to the SCMB, you must create and download an AMQP certificate from the appliance. After you connect the client to the SCMB, you can [create a queue and listen for messages](#).

Prerequisites

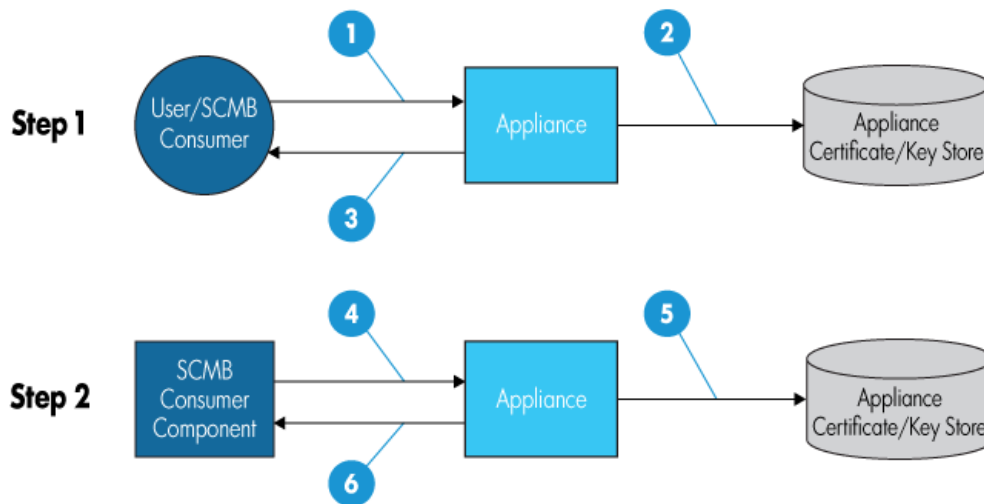
- Minimum required session ID privileges: Infrastructure administrator

Create and download the AMQP client certificate

Creating and downloading the client certificate, private key, and root CA certificate using REST APIs

1. Create the certificate.
`POST /rest/certificates/client/rabbitmq`
Request body: { "commonName":"default" }
 2. Download the certificate and private key.
`GET /rest/certificates/client/rabbitmq/keypair/default`
 3. Download the root CA certificate.
`GET /rest/certificates/ca`
-

Figure 16 Connecting the client to the SCMB



- 1 The SCMB consumer requests a client certificate as part of the registration process.
- 2 The appliance manages the client certificates in a JVK (Java KeyStore) file.
- 3 The appliance issues a client certificate to the SCMB consumer.
- 4 The SCMB client provides an SSL client certificate to create a connection with the appliance.
- 5 The appliance can revoke the SCMB client certificate to deny access to the SCMB client. The client is managed into a CRL (Certificate Revocation List) file.
- 6 The appliance authenticates the SCMB client using the client certificate.

26.2 Set up a queue to connect to the HP OneView SCMB exchange

The state change messages are published to the HP OneView SCMB exchange name. To subscribe to messages, you must create a queue or connect to an existing queue that receives messages from the SCMB exchange based on a routing key.

When you create a queue, you define the routing key associated with the queue to receive specific messages.

NOTE: The routing key is case sensitive. The *change-type* requires an initial capital letter. The *resource-category* and *resource-uri* are lower-case.

For example, if you set the *change-type* in the routing key to *created* instead of *Created*, you do not receive any messages.

The routing key syntax is:

`scmb.resource-category.change-type.resource-uri` where:

<code>scmb</code>	The HP OneView exchange name.
<code>resource-category</code>	The category of resource. For a complete list of resources, see the <i>HP OneView REST API Reference</i> chapter in the online help.
<code>change-type</code>	The type of change that is reported. Valid values are <i>Created</i> , <i>Updated</i> , and <i>Deleted</i> .
<code>resource-uri</code>	The URI of the specific resource associated with the state-change message.

NOTE: The *task* resources routing key syntax is `scmb.resource-category` and does not use `change-type` and `resource-uri`. To receive messages about all *task* resources:

- `scmb.#`
- `scmb.tasks`

Sample queues

Subscription	Example
Receive all SCMB messages for physical servers	<code>scmb.server-hardware.#</code> NOTE: To match everything after a specific point in the routing key, use the pound sign (#). This example uses # in place of <code>resource-uri</code> . The message queue receives all <code>server-hardware</code> resource URIs.
Receive all messages for created connections	<code>scmb.connections.Created.#</code>
Receive all messages for the enclosure with the URI <code>/rest/enclosures/Enc1234</code>	<code>scmb.enclosures.*./rest/enclosures/Enc1234</code> NOTE: To match everything for an individual field in the routing key, use the asterisk (*). This example uses * in place of <code>change-type</code> . The message queue receives all change types: <code>Created</code> , <code>Updated</code> , and <code>Deleted</code> .
Receive all created messages (for all resource categories and types)	<code>scmb.*.Created.#</code>

26.3 JSON structure of message received from the SCMB

The following table lists the attributes included in the JSON payload of each message from the SCMB. The resource model for the HP OneView resource is included in the `resource` attribute. To view all resource models, see the *HP OneView REST API Reference* chapter in the online help.

Attribute	Data type	Description
<code>resourceUri</code>	String	The URI for the resource
<code>changeType</code>	String	The state-change type: <code>Created</code> , <code>Updated</code> , or <code>Deleted</code> . For details, see “ChangeType values” (page 188) .
<code>newState</code>	String	The new state of the resource.
<code>eTag</code>	String	The ETag for the resource when the state change occurred.
<code>timestamp</code>	String	The time the message was sent.
<code>newSubState</code>	String	If substate messages are required (for substate machines associated with a primary state), this is the resource-specific substate.
<code>resource</code>	Object	The resource model.
<code>associatedTask</code>	String	If a task is not associated with this message, the value is <code>null</code> .
<code>userInitiatedTask</code>	String	The value of the <code>userInitiated</code> attribute included in the <code>associatedTask</code> attribute.
<code>changedAttributes</code>	Array	A list of top-level attributes that have changed based on the <code>POST</code> or <code>PUT</code> call that caused the state-change message to be sent.
<code>data</code>	Object	Additional information about the resource state change.

ChangeType values

ChangeType value	Description
Created	The resource is created or is added to HP OneView.
Updated	The resource state, attributes, or both are updated.
Deleted	The resource is permanently removed from HP OneView.

Example 2 JSON example

```
{
  "resourceUri" : "/rest/enclosures/123xyz",
  "changeType" : "Created",
  "newState" : "Managed",
  "eTag" : "123456",
  "timestamp" : "2013-07-10T18:30:44Z",
  "newSubState" : "null",
  "resource" : {
    "category" : "enclosures",
    "created" : "2013-07-10T18:30:00Z",
    ...
  },
  "associatedTask" : "/rest/tasks/4321",
  "userInitiatedTask" : "true",
  "changedAttributes" : [],
  "data" : {},
}
```

26.4 .NET C# code example

The .NET C# code examples show how to connect and subscribe to the SCMB. In addition to completing the prerequisites, you must complete the example-specific prerequisites before using the .NET C# code examples.

Prerequisites

Before you can use the .Net C# code examples, you must add the CA root certificate, the client certificate, and the private key to the Windows certificate store.

1. Download the root CA certificate.

```
GET /rest/certificates/ca
```

2. Save the contents in the response body into a text file named `rootCA.crt`. You must copy and paste everything from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----`, including the dashes, but not including the quotes.

3. Import the `rootCA.crt` file into the Windows certificate store under Trusted Root Certification Authorities.

4. Download the client certificate and private key.

```
GET /rest/certificates/client/rabbitmq/keypair/default
```

5. Save the contents of the client certificate and private key in the response body into a text file named `scmb.crt`.

You must copy and paste everything from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----` for the client certificate. Next, copy and paste everything from `-----BEGIN RSA PRIVATE KEY-----` to `-----END RSA PRIVATE KEY-----` for the private key. You must include the dashes, but do not include the quotes.

Additional example-specific prerequisites

Example 1

Convert the client certificate and private key to PKCS format for .Net.

```
openssl.exe pkcs12 -passout pass:default -export -in scmb.crt -out scmb.p12
```

Example 2

Import the `scmb.crt` into your preferred Windows certificate store.

Examples

Example 3 .Net C# code example 1 (directly referencing client certificate)

```
public void Connect()
{
    string exchangeName = "scmb";
    string hostName = "OneView.domain";
    string queueName = "";
    string routingKey = "scmb.#";

    ConnectionFactory factory = new ConnectionFactory();
    factory.AuthMechanisms = new RabbitMQ.Client.AuthMechanismFactory[] { new ExternalMechanismFactory() };

    factory.HostName = hostName;
    factory.Port = 5671;
    factory.Ssl.CertPath = @".\scmb.p12";
    factory.Ssl.CertPassphrase = "default";
    factory.Ssl.ServerName = hostName;
    factory.Ssl.Enabled = true;

    IConnection connection = factory.CreateConnection();
    IModel model = connection.CreateModel();

    queueName = model.QueueDeclare(queueName, false, false, false, null);
    model.QueueBind(queueName, exchangeName, routingKey, null);

    using (Subscription sub = new Subscription(model, queueName))
    {
        foreach (BasicDeliverEventArgs ev in sub)
        {
            DoSomethingWithMessage(ev);
            sub.Ack();
        }
    }
}
```

Example 4 .Net C# code example 2 (Microsoft Windows certificate store)

```
public void Connect()
{
    string exchangeName = "scmb";
    string hostName = "OneView.domain";
    string queueName = "";
    string routingKey = "scmb.#";
    string userName = "rabbitmq_readonly";

    X509Store store = new X509Store(StoreName.Root, StoreLocation.LocalMachine);
    store.Open(OpenFlags.ReadWrite);

    X509Certificate cert = store.Certificates
        .Find(X509FindType.FindBySubjectName, userName, false)
        .OfType<X509Certificate>()
        .First();

    ConnectionFactory factory = new ConnectionFactory();
    factory.AuthMechanisms = new RabbitMQ.Client.AuthMechanismFactory[] { new ExternalMechanismFactory() };

    factory.HostName = hostName;
    factory.Port = 5671;
    factory.Ssl.Certs = new X509CertificateCollection(new X509Certificate[] { cert });
    factory.Ssl.ServerName = hostName;
    factory.Ssl.Enabled = true;

    IConnection connection = factory.CreateConnection();
    IModel model = connection.CreateModel();

    queueName = model.QueueDeclare(queueName, false, false, false, null);
    model.QueueBind(queueName, exchangeName, routingKey, null);

    using (Subscription sub = new Subscription(model, queueName))
    {
        foreach (BasicDeliverEventArgs ev in sub)
        {
            DoSomethingWithMessage(ev);
            sub.Ack();
        }
    }
}
```

NOTE: .Net C# code example 2 (Microsoft Windows certificate store) is referencing the Trusted Root Certificate Authorities store, located under Local Computer.

- `StoreName.Root = Trusted Root Certificate Authorities`
 - `StortLocation.LocalMachine = Local Computer`
-

26.5 Java code example

The Java code example shows how to connect and subscribe to the SCMB.

Prerequisites

1. Download the client certificate and private key.

```
GET /rest/certificates/client/rabbitmq/keypair/default
```

2. Save the contents of the client certificate in the response body into a text file named `default-client.crt`.

You must copy and paste everything from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----`, including the dashes, but not including the quotes.

3. Save the contents of the private key in the response body into a text file named `default-client.key`.

You must copy and paste everything from `-----BEGIN RSA PRIVATE KEY-----` to `-----END RSA PRIVATE KEY-----`, including the dashes, but not including the quotes.

4. Create a PKCS12 keystore from the private key and the public certificate.

```
openssl pkcs12 -export -name myclientcert -in default-client.crt -inkey default-client.key -out myclient.p12
```

5. Convert the PKCS12 keystore into a JKS keystore.

```
keytool -importkeystore -destkeystore c:\\MyKeyStore -srckeystore myclient.p12 -srcstoretype pkcs12 -alias myclient
```

Example 5 Java code example

```
//c://MyKeyStore contains client certificate and private key. Load it into Java Keystore
final char[] keyPassphrase = "MyKeyStorePassword".toCharArray();
final KeyStore ks = KeyStore.getInstance("jks");
ks.load(new FileInputStream("c://MyKeyStore"), keyPassphrase);
final KeyManagerFactory kmf = KeyManagerFactory.getInstance("SunX509");
kmf.init(ks, keyPassphrase);

//c://MyTrustStore contains CA certificate. Load it into Java Trust Store
final char[] trustPassphrase = "MyTrustStorePassword".toCharArray();
final KeyStore ks = KeyStore.getInstance("jks");
tkf.load(new FileInputStream("c:\\MyTrustStore"), trustPassphrase);
final TrustManagerFactory tmf = TrustManagerFactory.getInstance("SunX509");
tmf.init(tks);

//load SSLContext with keystore and truststore.
final SSLContext c = SSLContext.getInstance("SSL");
c.init(kmf.getKeyManagers(), tmf.getTrustManagers(), new SecureRandom());

final ConnectionFactory factory = new ConnectionFactory();
factory.setHost("192.168.2.144");

//Set Auth mechanism to "EXTERNAL" so that commonName of the client certificate is mapped to AMQP user name.
Hence, No need to set userId/Password here.
factory.setSaslConfig(DefaultSaslConfig.EXTERNAL);
factory.setPort(5671);
factory.useSslProtocol(c);

final Connection conn = factory.newConnection();
final Channel channel = conn.createChannel();

//do not specify queue name. AMQP will create a queue with random name starting with amq.gen* e.g.
amq.gen-32sfQz95QJ85K_lMBhU6HA
final DeclareOk queue = channel.queueDeclare("", true, false, true, null);

//Now get the queue name from above call and bind it to required Exchange with required routing key.
channel.queueBind(queue.getQueue(), "scmb", "scmb.#");

//Now you should be able to receive messages from queue
final GetResponse chResponse = channel.basicGet(queue.getQueue(), false);
if (chResponse == null)
{
    System.out.println("No message retrieved");
}
else
{
    final byte[] body = chResponse.getBody();
    System.out.println("Received: " + new String(body));
}

channel.close();
conn.close();
```

26.6 Python code example

The Python code examples show how to connect and subscribe to the SCMB. For more information about Python (Pika AMQP client library), see <http://pika.readthedocs.org> and <https://pypi.python.org/pypi/pika>.

Example 6 Python code example (pika)

```
import pika, ssl
from pika.credentials import ExternalCredentials
import json
import logging

logging.basicConfig()

#####
# Callback function that handles messages
def callback(ch, method, properties, body):
    msg = json.loads(body)
    timestamp = msg['timestamp']
    resourceUri = msg['resourceUri']
    resource = msg['resource']
    changeType = msg['changeType']

    print
    print ("%s: Message received:" %(timestamp))
    print ("Routing Key: %s" %(method.routing_key))
    print ("Change Type: %s" %(changeType))
    print ("Resource URI: %s" %(resourceUri))
    print ("Resource: %s" %(resource))

# Setup our ssl options
ssl_options = ({ "ca_certs": "caroot.pem",
                  "certfile": "client.pem",
                  "keyfile": "key.pem",
                  "cert_reqs": ssl.CERT_REQUIRED,
                  "server_side": False})

# Connect to RabbitMQ
host = "example.com"
connection = pika.BlockingConnection(
    pika.ConnectionParameters(
        host, 5671, credentials=ExternalCredentials(),
        ssl=True, ssl_options=ssl_options))

# Create and bind to queue
EXCHANGE_NAME = "scmb"
ROUTING_KEY = "scmb.#"

channel = connection.channel()
result = channel.queue_declare()
queue_name = result.method.queue

channel.queue_bind(exchange=EXCHANGE_NAME, queue=queue_name, routing_key=ROUTING_KEY)

channel.basic_consume(callback,
                      queue=queue_name,
                      no_ack=True)

# Start listening for messages
channel.start_consuming()
```

Example 7 Python code example (amqplib)

```
#!/usr/bin/env python

from optparse import OptionParser
from functools import partial

import amqp

def callback(channel, msg):
    for key, val in msg.properties.items():
        print ('%s: %s' % (key, str(val)))
    for key, val in msg.delivery_info.items():
        print ('> %s: %s' % (key, str(val)))

    print ('')
    print (msg.body)
    print ('-----')
    print msg.delivery_tag
    channel.basic_ack(msg.delivery_tag)

    #
    # Cancel this callback
    #
    if msg.body == 'quit':
        channel.basic_cancel(msg.consumer_tag)

def main():
    parser = OptionParser()
    parser.add_option('--host', dest='host',
        help='AMQP server to connect to (default: %default)',
        default='localhost',
    )

    options, args = parser.parse_args()
    ssl_options = ({ "ca_certs": "caroot.pem",
        "certfile": "client.pem",
        "keyfile": "key.pem",
        "cert_reqs": CERT_REQUIRED,
        "server_side": False})

    #

    print ('Connecting to host %s' %options.host)

    conn = amqp.Connection(options.host, login_method='EXTERNAL',
        ssl=ssl_options)

    print ('Successfully connected, creating and binding to queue')

    ch = conn.channel()

    qname, _, _ = ch.queue_declare()
    ch.queue_bind(qname, 'scmb', 'scmb.#')
    ch.basic_consume(qname, callback=partial(callback, ch))

    print ('Successfully bound to queue, waiting for messages')

    #pyamqp://

    #
    # Loop as long as the channel has callbacks registered
    #
    while ch.callbacks:
        ch.wait()
```

```
ch.close()
conn.close()

if __name__ == '__main__':
    main()
```

26.7 Re-create the AMQP client certificate

If you change the appliance name, you must re-create the AMQP client certificate.

Prerequisites

- Minimum required session ID privileges: Infrastructure administrator

Re-creating and downloading the client certificate, private key, and root CA certificate using REST APIs

1. Revoke the certificate.

```
DELETE /rest/certificates/ca/rabbitmq_readonly
```

Request body is not required.

NOTE: When you revoke the default client certificate, the appliance re-generates the CA certificate, AMQP server certificate, and the default client certificate.

2. Download the certificate and private key.

```
GET /rest/certificates/client/rabbitmq/keypair/default
```

3. Download the root CA certificate.

```
GET /rest/certificates/ca
```

Part VI Troubleshooting

The chapters in this part include information you can use when troubleshooting issues in your data center, and information about restoring the appliance from a backup file in the event of a catastrophic failure.

27 Troubleshooting

HP OneView has a variety of troubleshooting tools you can use to resolve issues. By following a combined approach of examining screens and logs, you can obtain a history of activity and of the errors encountered along the way. For specific troubleshooting instructions, select a topic from the following list.

Category

- [Appliance](#)
- [Enclosures and enclosure groups](#)
- [Firmware bundles](#)
- [Interconnects](#)
- [Licensing](#)
- [Logical interconnects](#)
- [Networks](#)
- [Server hardware](#)
- [Server profiles](#)
- [User accounts and groups](#)

Learn more

- [“Basic troubleshooting techniques” \(page 200\)](#)
- [“Create a support dump file” \(page 201\)](#)
- [“Create a support dump for authorized technical support using REST API scripting” \(page 202\)](#)
- [“Using the virtual appliance console” \(page 269\)](#)

27.1 Basic troubleshooting techniques

HP OneView has a variety of troubleshooting tools you can use to resolve issues. By following a combined approach of examining screens and logs, you can obtain a history of activity and the errors encountered along the way.

- The [Activity screen](#) displays a log of all changes made on the appliance, whether user-initiated or appliance-initiated. It is similar to an audit log, but with finer detail and it is easier to access from the UI.

The **Activity** screen also provides a log of health alerts and status notifications.

- [Download an audit log](#) to help an administrator understand what security relevant actions took place on the system.
- [Create a support dump file](#) to gather logs and other information required for debugging into an encrypted, compressed file that you can send to your authorized support representative for analysis.

Recommendation	Details
Look for a message	<p>About syntax errors:</p> <ul style="list-style-type: none">• The user interface checks for syntax when you enter a value. If you make a syntax error, an instructional message appears next to the entry. The user interface or command line continues to display messages until you enter the correct value. <p>About network setup errors:</p> <ul style="list-style-type: none">• Before applying them, the appliance verifies key network parameters like the IP address and the fully qualified domain name (FQDN), to ensure that they have the proper format.• After network settings are applied, the appliance performs additional validation, such as reachability checks and host name to IP lookup. If a parameter is incorrect, the appliance generates an alert that describes validation errors for the Network Interface Card (NIC), and the connection between the browser and the appliance can be lost. <p>About reported serious errors:</p> <ul style="list-style-type: none">• Check connectivity to the enclosure from the appliance.• Create a support dump and contact your HP support representative.
Examine the Activity screen	<p>To find a message for an activity:</p> <p>NOTE: You might need to perform these steps from the virtual console.</p> <ol style="list-style-type: none">1. Locate recent activities with a Critical or Warning status.2. Expand the activity to see recommendations on how to resolve the error.3. Follow the instructions.
Examine the virtual machine	

Recommendation	Details
	<p>When VM host is down or nonresponsive:</p> <ol style="list-style-type: none"> From the local computer, use the <code>ping</code> command to determine if you can reach the appliance. <ul style="list-style-type: none"> If the <code>ping</code> command is successful, determine that the browser settings, especially the proxy server, are correct. Consider bypassing the proxy server. If the <code>ping</code> command did not reach the appliance, ensure that the local computer is connected to the network. Log onto hypervisor to verify that it (the hypervisor) is running. Verify that the virtual guest for the appliance is operational. Ensure that the VM host's configuration is valid. Verify the accuracy of the IP address and other network parameters for the VM host. From the management console, ensure that the appliance network settings are accurate. Examine the hypervisor's performance data. If the appliance is running at 100% utilization, restart the hypervisor.

27.2 Create a support dump file

Some error messages recommend that you create a support dump of the appliance to send to an authorized support representative for analysis. The support dump process:

- Deletes any existing support dump file
- Gathers logs and other information required for debugging
- Creates a compressed file

Unless you specify otherwise, all data in the support dump file is encrypted so that it is accessible only by an authorized support representative. You might choose not to encrypt the support dump file if you have an onsite, authorized support representative or if your environment prohibits outside connections. You can also validate the contents of the support dump file and verify that it does not contain sensitive data such as passwords.

- ❗ **IMPORTANT:** If the appliance is in an error state, you can still create an encrypted support dump file without logging in or other authentication.

The support dump file contains the following:

- Operating system logs (from `/var/log`)
- Product logs (from `/ci/logs`)
- The results of certain operating system and product-related commands

Items logged in the support dump file are recorded in UTC (Coordinated Universal Time).

Prerequisites

- Minimum required privileges: Infrastructure administrator

Creating a support dump file

- From the main menu, select **Settings**→**Actions**→**Create support dump**.

To include logical interconnect support dump information, select **Logical Interconnects**→**Actions**→**Create support dump**. The logical interconnect support dump file is incorporated into the appliance support dump file and the entire bundle of files is compressed into a zip file and encrypted for downloading.

- If you do not want to encrypt the support dump file, clear the **Enable support dump encryption** check box.

3. Click **Yes, create**.

You can continue doing other tasks while the support dump file is created.

The support dump file name has the following format:

hostname-CI-timestamp.sdmp

4. The support dump file is downloaded when this task is completed. If your browser settings specify a default download folder, the support dump file is placed in that folder. Otherwise, you are prompted to indicate where to download the file.
5. Contact your authorized support representative for instructions on transferring the support dump file to HP. For information on contacting HP, see [“How to contact HP” \(page 227\)](#).

- ❗ **IMPORTANT:** Unless you specify otherwise, the support dump file is encrypted so that only authorized support personnel can view its contents.

In accordance with the HP data retention policy, support dump files sent to HP are deleted after use.

27.3 Create a support dump for authorized technical support using REST API scripting

Some error messages recommend that you create a support dump of the appliance to send to an authorized support representative for analysis. The support dump process:

- Deletes any existing support dump file
- Gathers logs and other information required for debugging
- Creates a compressed file

Unless you specify otherwise, all data in the support dump file is encrypted so that it is accessible only by an authorized support representative. You might choose not to encrypt the support dump file if you have an onsite, authorized support representative or if your environment prohibits outside connections. You can also validate the contents of the support dump file and verify that it does not contain sensitive data such as passwords.

- ❗ **IMPORTANT:** If the appliance is in an error state, you can still create an encrypted support dump file without logging in or other authentication.

The support dump file contains the following:

- Operating system logs (from `/var/log`)
- Product logs (from `/ci/logs`)
- The results of certain operating system and product-related commands

Items logged in the support dump file are recorded in UTC (Coordinated Universal Time).

Prerequisites

- Minimum required session ID privileges: Infrastructure administrator

Creating a support dump using REST APIs

1. Create support dump.

POST `/rest/appliance/support-dumps`

2. Download the support dump file.

GET `/rest/appliance/support-dumps/{file name}`

- ❗ **IMPORTANT:** Unless you specify otherwise, the support dump file is encrypted so that only authorized support personnel can view its contents.
- In accordance with the HP data retention policy, support dump files sent to HP are deleted after use.

27.4 Troubleshooting the appliance

27.4.1 First time setup

Symptoms	Possible causes and recommendations
Appliance cannot access network	Appliance network settings are not properly configured <ol style="list-style-type: none">1. Minimum required privileges: Infrastructure administrator2. Access the appliance console.3. Examine the alerts on the Activity screen to help diagnose the problem.4. On the Settings screen, verify that the following entries are correct:<ul style="list-style-type: none">• Host name (if DNS is used, ensure that the appliance host name is a fully qualified domain name)• IP address• Subnet mask• Gateway address5. For manual DNS assignment, verify the IP addresses you entered for the primary and secondary DNS servers and correct as needed.6. Verify that your local router is working.7. Verify that the network is up and running.
Appliance is configured correctly but cannot access network	External difficulties <ol style="list-style-type: none">1. Verify that your local router is working.2. Verify that the network is up and running.

27.4.2 Appliance cannot access the network

Symptom	Possible cause and recommendation
Appliance cannot access the network.	Appliance network not properly configured <ol style="list-style-type: none">1. Minimum required privileges: Infrastructure administrator2. Verify that the IP address assignment is correct.3. Verify that the DNS IP address is correct.4. Verify that the DNS server is running.

27.4.3 Unexpected appliance shutdown

Symptom	Possible cause and recommendation
Appliance crash	Actions to take after a crash <ul style="list-style-type: none">• Check for critical alerts or failed tasks. Follow the resolution instructions, if provided.• Manually refresh a resource (Actions→Refresh) if the resource information displayed appears to be incorrect or inconsistent.• Create a support dump (Settings→Actions→Create support dump) for unexpected shutdowns to help your authorized support representative troubleshoot the problem.

27.4.4 Appliance update is unsuccessful

Any blocking or warning conditions affecting the appliance update are displayed prior to the update operation.

Symptom	Possible cause and recommendation
Resource state or health status changes	<ol style="list-style-type: none">1. Verify that all prerequisites are met.2. Correct all degraded health and other blocking conditions that have been identified in notification messages before retrying the update.

27.4.5 Support dump file creation action fails

Symptom	Possible cause and recommendation
Support dump file not created	Insufficient time <ol style="list-style-type: none">1. Minimum required privileges: Infrastructure administrator2. Wait. Creating a support dump file can take several minutes. If the log files are large or if the system is extensive, creating a support dump file can take even longer.3. Retry the create support dump action.

27.4.6 Certificate action fails

Follow the recommendation if any of these certificate actions fails:

- Create a self-signed certificate
- Create a certificate signing request
- Import certificate

Symptom	Possible cause and recommendation
Certificate action failed	Appliance lost connection with web server <ol style="list-style-type: none">1. Minimum required privileges: Infrastructure administrator2. When creating a certificate signing request or importing a certificate, verify that the networking is working properly.3. Wait for the web server to restart, then try the action again.

27.4.7 Backup file creation, download, or restore action fails

Symptom	Possible cause and recommendation
Backup file not created	<p>Other related operations are in progress</p> <p>Only one backup file can be created at a time. A backup file cannot be created during a restore operation or while a previous backup file is being uploaded or downloaded.</p> <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Verify that another backup or restore operation is running. If so, there is a progress bar in the Settings screen. A completion is noted in the Activity sidebar. 3. Wait until the operation is complete. 4. Retry the create backup file operation. <p>Backup file creation is still in progress</p> <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Verify the operation is complete. If the operation is ongoing, there is a progress bar in the Settings screen. 3. Wait until the backup file creation completes. Creating a backup file can take several minutes. If the log files are large or if the system is extensive, creating a backup file can take even longer. When the operation is complete, it is noted in the Activity sidebar. 4. If needed, retry the create backup file action.
Cannot download backup file	<p>The appliance network is down</p> <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Ensure that the network is correctly configured and performing as expected. <p>Other related operations are in progress</p> <p>A backup file cannot be uploaded or downloaded while a backup file creation or restore operation is in progress.</p> <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Ensure that another backup or restore operation is not running. They are indicated with a progress bar in the Settings screen. <p>Insufficient time</p> <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Wait. Downloading a large backup file can take several minutes, perhaps more depending on the complexity of the appliance configuration. 3. Consider installing cURL to improve performance for future downloads.
Cannot restore appliance from backup file	<p>The backup file is incompatible</p> <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Retry the restore operation with a recent backup file that: <ul style="list-style-type: none"> • Has a firmware version that is compatible with the appliance (that is, the first two components of the version number must be the same) • Was created with the same version of HP OneView as the appliance 3. Reconcile any discrepancies that the restore operation could not resolve automatically.
Booting from wrong device or incorrect BIOS settings	<p>BIOS, firmware, and boot settings were changed after the backup and before the restore operations</p> <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Verify the BIOS firmware, and boot settings. 3. Unassign the profiles. 4. Reassign each profile to its corresponding server.

Symptom	Possible cause and recommendation
Duplicate GUIDs in the network and a server with settings from a previous profile	A profile operation was running during the backup <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Identify the server affected. 3. Unassign the profile from the server. 4. Reassign the profile to the server. 5. Create a support dump file. 6. Report this issue to your authorized support representative.
Error messages: 1. The operation was interrupted and 2. The configuration is inconsistent.	A profile operation was running during the backup <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Unassign the profile. 3. Reassign the profile. 4. Create a support dump file. 5. Determine any factors (not related to HP OneView) that contributed to this condition, such as: <ul style="list-style-type: none"> • Was the server moved? • Was the server power turned off?
Restore operation does not restore server profile	Restore operation fails or times out <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Create a support dump file. 3. Do one of the following: <ol style="list-style-type: none"> a. Retry the restore operation with the same backup file. b. Retry the restore operation with a different backup file. 4. Verify that all the necessary actions were followed to put the profiles back in-line with the environment. If there is a profile still in an inconsistent state, there might be incorrect behavior in the data center.

27.4.8 Restart or shutdown failure

Symptom	Possible cause and recommendation
The appliance did not shut down	Internal server error <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Retry the shutdown action. 3. If the problem persists, create a support dump. 4. Contact your authorized support representative and provide them with the support dump. For information on contacting HP, see "How to contact HP" (page 227).
Cannot restart the appliance after a shutdown	Internal server error <ol style="list-style-type: none"> 1. Minimum required privileges: Infrastructure administrator 2. Retry the restart action. 3. If the problem persists, create a support dump. For information, see "Create a support dump file" (page 201). 4. Contact your authorized support representative and provide them with the support dump. For information on contacting HP, see "How to contact HP" (page 227).

27.4.9 VM does not restart when VM host time is manually set

Symptom	Possible cause and recommendation
The appliance VM does not restart and the following error appears in the vSphere virtual console: The superblock last mount time is in the future UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY.	<p>You are not using NTP and the VM host's time was incorrectly set to a time in the past.</p> <ul style="list-style-type: none">Reset the time settings on the VM host to the correct time, and then restart the VM appliance. For more information, see your vSphere documentation.If the appliance or VM host is configured as an NTP client, ensure that the NTP server is working correctly. <p>NOTE:</p> <ul style="list-style-type: none">For HP-recommended best practices for managing the appliance VM, see “Best practices for managing a VM appliance” (page 153).

27.4.10 Reinstall the remote console

When running Firefox or Chrome on a Windows client, the first-time installation of the remote console prevents the installation dialog box from being displayed again. If you need to reinstall the console software, you must reset the installation dialog box.

Symptom	Possible cause and recommendation
Installation dialog box is not displayed	<p>If you installed the iLO remote console software using one browser (Firefox or Chrome), but are using another browser, the dialog box that prompts you to install the software is displayed, even if the software is already installed.</p> <p>To reinstall the console, press the Shift key and select Actions→Launch console.</p> <p>Reinstall the software</p> <ol style="list-style-type: none">Click Install software and close all of the dialog boxes for installing the application.Click My installation is complete — Launch console to launch the console after it is installed.

27.5 Troubleshooting enclosures and enclosure groups

27.5.1 Add or remove enclosure is unsuccessful

Symptom	Possible cause and recommendation						
Unable to add an enclosure	<p>If the enclosure add fails, a notification panel provides the reason the add action failed and provides a solution to the problem. Often, the resolution is to click the add link that is embedded in the message; the add action rediscovers all components and updates its knowledge of the enclosure.</p> <p>Enclosure is already being managed by some other management software and is claimed by that software</p> <ol style="list-style-type: none">1. If a first-time enclosure add fails, verify that the enclosures prerequisites listed in add an enclosure to manage its contents are met. Verify that the data you entered on the screen is corrects, and try the action again.2. Follow the guidance in the notification panel for the corrective action you need to take to successfully add the enclosure. <p>Failures can occur during the add action if all information about an enclosure, its server blades, or interconnect modules cannot be acquired. When this happens, an explanation of the problem and the component that caused the problem (the enclosure, a server blade, an interconnect) is provided in a notification panel.</p> <ol style="list-style-type: none">3. To re-add an enclosure, click the add link in the notification message panel (if there is one), or start the add action again from the Add Enclosure screen, supplying the address and credentials for the enclosure's Onboard Administrator. <p>To forcibly add the enclosure to the appliance, see the UI help for enclosures.</p>						
Unable to forcibly add an enclosure	<p>You forcibly added an enclosure but received an error message. This happens only in some cases where there is a VCMODE set and virtual connect is managing the enclosure.</p> <ol style="list-style-type: none">1. Manual clean-up of the configuration is needed, investigate the following items:<ul style="list-style-type: none">• The management URL might still point to the appliance. If so, it needs to be reset to point at the first interconnect in the enclosure. To fix this, use the following ssh commands to go into the Onboard Administrator (using administrator credentials) and change the management URL to point to the first active VC interconnect's IP address: <table><tr><td><code>clear vcmode</code></td><td>Disassociates the enclosures from the appliance.</td></tr><tr><td><code>restart interconnect <i>N</i></code></td><td>(where <i>N</i> is the bay number of a VC interconnect) Performing this step for every VC interconnect in the enclosure causes the interconnect to revert to a default configuration.</td></tr><tr><td><code>restart oa <i>N</i></code></td><td>(where <i>N</i> is the bay number of the active Onboard Administrator) This causes the OA to obtain the management URL from the first VC interconnect.</td></tr></table> <ol style="list-style-type: none">2. After manual configuration, Re-add an enclosure or refresh the enclosure.	<code>clear vcmode</code>	Disassociates the enclosures from the appliance.	<code>restart interconnect <i>N</i></code>	(where <i>N</i> is the bay number of a VC interconnect) Performing this step for every VC interconnect in the enclosure causes the interconnect to revert to a default configuration.	<code>restart oa <i>N</i></code>	(where <i>N</i> is the bay number of the active Onboard Administrator) This causes the OA to obtain the management URL from the first VC interconnect.
<code>clear vcmode</code>	Disassociates the enclosures from the appliance.						
<code>restart interconnect <i>N</i></code>	(where <i>N</i> is the bay number of a VC interconnect) Performing this step for every VC interconnect in the enclosure causes the interconnect to revert to a default configuration.						
<code>restart oa <i>N</i></code>	(where <i>N</i> is the bay number of the active Onboard Administrator) This causes the OA to obtain the management URL from the first VC interconnect.						
An existing enclosure is detected as being new after a midplane is replaced	<p>You replaced the enclosure midplane but did not follow the recommended procedure in the hardware documentation.</p> <p>Recommendation: Re-add an enclosure</p>						

Symptom	Possible cause and recommendation						
Unable to remove an enclosure	<p>You might be unable to remove an enclosure for the following reasons:</p> <ul style="list-style-type: none"> Lack of communication with the hardware during the remove action can prevent the appliance from being able to properly manage the interconnect, server hardware, and enclosure settings. To forcibly remove an enclosure from the appliance due to lack of communication, see the UI help for enclosures. The enclosure is not removed from the appliance. This is typically a problem on the appliance itself, and the best resolution is to follow instructions in the notification panels. The enclosure is removed but due to a communication failure, the configuration requires manual intervention to correct. <p>If manual clean-up of the configuration is needed, investigate the following items:</p> <ul style="list-style-type: none"> The management URL might still point to the appliance. If so, it needs to be reset to point at the first interconnect in the enclosure. To fix this, use the following ssh commands to go into the Onboard Administrator (using administrator credentials) and change the management URL to point to the first active VC interconnect's IP address: <table border="1"> <tr> <td><code>clear vcmode</code></td><td>Disassociates the enclosures from the appliance.</td></tr> <tr> <td><code>restart interconnect <i>N</i></code></td><td>(where <i>N</i> is the bay number of a VC interconnect) Performing this step for every VC interconnect in the enclosure causes the interconnect to revert to a default configuration.</td></tr> <tr> <td><code>restart oa <i>N</i></code></td><td>(where <i>N</i> is the bay number of the active Onboard Administrator) This causes the OA to obtain the management URL from the first VC interconnect.</td></tr> </table> <ul style="list-style-type: none"> The interconnects might still be claimed by the appliance. If this is the case, you have to remove the interconnects manually. 	<code>clear vcmode</code>	Disassociates the enclosures from the appliance.	<code>restart interconnect <i>N</i></code>	(where <i>N</i> is the bay number of a VC interconnect) Performing this step for every VC interconnect in the enclosure causes the interconnect to revert to a default configuration.	<code>restart oa <i>N</i></code>	(where <i>N</i> is the bay number of the active Onboard Administrator) This causes the OA to obtain the management URL from the first VC interconnect.
<code>clear vcmode</code>	Disassociates the enclosures from the appliance.						
<code>restart interconnect <i>N</i></code>	(where <i>N</i> is the bay number of a VC interconnect) Performing this step for every VC interconnect in the enclosure causes the interconnect to revert to a default configuration.						
<code>restart oa <i>N</i></code>	(where <i>N</i> is the bay number of the active Onboard Administrator) This causes the OA to obtain the management URL from the first VC interconnect.						
Unable to unconfigure single sign on (SSO) on the Onboard Administrator when adding or removing an enclosure	<p>Resolution: Remove all certificates and restart the OA (Onboard Administrator).</p> <ol style="list-style-type: none"> From the OA user interface, select Users/Authentication. Select HP SSO integration, in the right pane. Verify that Settings, Trust mode is set to Trust by Certificate. Select the Certification Information tab and remove all HP SSO Certificates. Reboot the OA. Re-add the enclosure. 						

27.5.2 Add server blade is unsuccessful

Symptom	Possible cause and recommendation
Add server blade failed	<p>If a server blade previously associated with this profile is re-inserted in a different place (different bay or enclosure), an error message is shown.</p> <p>The edit link within the expanded error message causes the new server blade location to be pre-populated in the edit profile dialog's location field when it is displayed.</p> <p>Same server blade, different bay error</p> <ol style="list-style-type: none">1. Manually move the server profile to a server blade in a different bay using the Edit Server Profile screen. If you come to this screen via the edit link the error message, it is auto-filled in for the server hardware value, with the appropriate change indications at the bottom of the dialog.2. Click OK. <p>Different server blade, same bay error</p> <p>Server profiles are associated by UUID to a specific server blade. If the wrong server blade is put back in the bay, an error is displayed, which can only be removed by resolving the conflict.</p> <p>Server Hardware hyperlink will point to the new server blade's Server Hardware screen. Connections will still show disabled status.</p> <p>The Server Hardware screen displays normally, since it doesn't recognize it was ever associated with a server profile.</p>

27.5.3 Certificate Error

Symptom	Possible cause and recommendation
Invalid certificate error message is displayed	<p>The OA single sign-on certificate can be corrupted when the OA firmware is downgraded to a lower version and then is upgraded to a higher version.</p> <p>Reset the OA:</p> <ol style="list-style-type: none">1. From the OA UI, select security+HPSIM SSO.2. Delete the corrupted certificate, which is shown in yellow.3. To re-install the original certificate, refresh the enclosure.

27.6 Troubleshooting firmware bundles

27.6.1 Incorrect credentials

Symptom	Possible cause and recommendation
The iLO user name or password is invalid	<p>Incorrect credentials for a server</p> <ul style="list-style-type: none">• The user name or password you supplied is not valid for a iLO management processor while attempting to update server firmware. Correct the credentials and then add the enclosure again..
Unable to get Onboard Administrator (OA) credentials	<p>OA credentials unavailable</p> <p>The appliance was unable to get Onboard Administrator (OA) credentials for the enclosure while attempting to update the firmware.</p> <ul style="list-style-type: none">• Add the enclosure again.

27.6.2 Lost iLO connectivity

Symptom	Possible cause and recommendation
Connection error	Reset the server to restore network connectivity to the server's management processor and update the firmware again.

27.6.3 HP SUM errors

Symptom	Possible cause and recommendation
Unable to remove the firmware upgrade log files	Restart the appliance and update the firmware again.
Unable to initiate the firmware update request	Update the firmware again.

27.7 Troubleshooting interconnects

27.7.1 Interconnect edit is unsuccessful

Symptom	Possible cause and recommendation
Notification that modifying an interconnect was unsuccessful	<p>If interconnect edit is unsuccessful:</p> <ol style="list-style-type: none">1. Verify that the prerequisites listed in the online help are met.2. Follow the instructions provided by any notification message. <p>When the interconnect has been edited successfully, a notification will display in the banner at the top of the screen, and the desired port setting and port status will be displayed.</p>

27.7.2 Interconnect modules are in Maintenance state

Symptom	Possible cause and recommendation
Interconnect modules are in the Maintenance state	<p>There is an OA credential caching issue if interconnect modules report their state as Maintenance.</p> <p>If interconnect modules are in the Maintenance state:</p> <p>You have to re-add the enclosure.</p> <ol style="list-style-type: none">1. From the main menu, select Enclosures→Add.2. Provide the enclosure information (IP/FQDN, Administrator account and password), and click the Add button. <p>This will initiate rediscovery of the enclosure and its components.</p>

27.8 Troubleshooting licensing

27.8.1 Restore a license key that has been erased from an enclosure OA

If you perform a factory reset on an enclosure, any license embedded on the OA is erased, and you must manually retrieve and re-add the license key.

NOTE: You need your entitlement certificate (physical or electronic document) to restore the license key.

Symptom	Possible cause and recommendation
The license key embedded on the OA is not discovered when you add the enclosure	The license key embedded on the OA has been erased <ol style="list-style-type: none">1. Go to the HP Licensing for Software Portal at https://www.hp.com/software/licensing to activate, register, and download your license key(s).2. Add the key(s) to the appliance from the Settings screen.

27.8.2 The license assigned does not match the type specified

Symptom	Possible cause and recommendation
Server hardware is assigned a license that is different from the one specified when it was added to the appliance	The server hardware has an embedded license <p>Embedded licenses override the license policy or type specified when the enclosure or rack server was added. Server hardware with an existing, permanent iLO Advanced license will be assigned an HP OneView w/o iLO license.</p> A server that was previously managed by the appliance and has been added again <p>If a server was previously managed by the appliance and had an HP OneView license applied, it will be assigned that same license when it is added, regardless of the license type specified.</p>

27.9 Troubleshooting logical interconnects

27.9.1 I/O bay occupancy errors

Symptom	Possible cause and recommendation
Change in interconnect state	Interconnect state errors due to: <ul style="list-style-type: none">• Interconnect missing from an IO bay (Interconnect state is Absent)• Unsupported interconnect model found in an IO bay (Interconnect state is Unsupported)• Unable to manage interconnect in IO bay due to unsupported firmware (Interconnect state is Unmanaged)

27.9.2 Uplink set warnings or errors

Symptom	Possible cause and recommendation
Uplink set not operational	Uplink set not operational due to: <ul style="list-style-type: none">• No uplinks, or at least one uplink, is not in an operational state• No networks assigned <ol style="list-style-type: none">1. Verify that the following prerequisites are met:<ul style="list-style-type: none">• At least one network is defined• You have Network administrator privileges or equivalent to manage networks.2. Verify that the data you entered on the Add Uplink Set screen is correct, and that the uplink set name is unique.3. Retry the operation.

27.9.3 Physical interconnect warnings and errors

Symptom	Possible cause and recommendation
Interconnect-level warnings or errors	Interconnect warnings or errors due to: <ul style="list-style-type: none">• Downlink with a deployed connection is not operational• Incorrect firmware version (different from firmware baseline version)• Configuration error• Hardware fault• Lost communication• Connection and redundancy status (no redundant paths)• Administratively disabled ports

27.10 Troubleshooting networks

27.10.1 Network create operation is unsuccessful

Symptom	Possible cause and recommendation
Network creation is unsuccessful	The prerequisites have not been met <ol style="list-style-type: none">1. Verify that the prerequisites listed in the online help have been met.2. Retry the create network operation. The network was configured incorrectly <ol style="list-style-type: none">1. Verify that:<ul style="list-style-type: none">• The VLAN ID is in the range of valid integers (2 through 4092).• The network name is unique.• The network bandwidth is within the range indicated by the UI. The preferred bandwidth must be less than the maximum bandwidth.2. Retry the create network operation.

27.11 Troubleshooting server hardware

27.11.1 Server add or remove is unsuccessful

If the add server action is not successful, a notification panel provides the reason why the add action failed and provides a solution to the problem. Often, the resolution is to click the **add** link

embedded in the message; the add action rediscovers all components and updates its knowledge of the server.

Symptom	Possible cause and recommendation
Cannot add a server	<p>Server is already being managed by some other management software and is claimed by that software</p> <ol style="list-style-type: none">1. Follow the instructions in the notification panel. Failures can occur during the add action if all information about a server cannot be acquired. When this happens, an explanation of the problem and the component that caused the problem is provided in a notification panel.2. To re-add a server, click the add retry or the refresh link in the notification message panel (if there is one), or start the add action again from the Add Server screen. If the server is in an unmanaged state and is claimed, the resolution is to refresh. If the server is not claimed, the resolution is to add.
Cannot remove a server	<p>Lack of connectivity with the server hardware can prevent the remove action from being successful</p> <p>The server is not removed from the appliance. The likely cause is an internal problem on the appliance and the best resolution is to follow the instructions in the notification panel.</p> <p>The server is removed but due to communication failure, the configuration requires manual intervention to correct.</p> <p>In the case where manual configuration is needed, investigate the following:</p> <ul style="list-style-type: none">• The management URL might still point to the appliance, leave it alone. Then later, use the Force option to add the server back under a new appliance manager.• Remove _HPOneViewAdmin administrative user, from the list of iLO users through the iLO.• Remove the SNMP trap destination, which is the IP address of the appliance, from the list of trap targets.

27.11.2 Cannot control power on server blade

Server hardware power control depends on both the HP Integrated Lights-Out (iLO) on the target server hardware, and in the case of ProLiant C-class servers, the Onboard Administrator module in the host enclosure.

If you have difficulty with server power control, examine recent configuration and security changes which might impact this feature. Often the iLO event log can be a useful starting point to see these changes.

Another area to examine for ProLiant C-class servers are the Power Management policies of the enclosure. Verify the Onboard Administrator to ensure sufficient power is available and the power operations policy is appropriate.

Hardware could have failed as well. Use the Integrated Management Log (IML) on the iLO for Power On Self Test (POST) errors to determine if a hardware failure has occurred.

If a power on or power off action fails, follow the instructions in the notification message.

27.11.3 Lost connectivity to server hardware after appliance restarts

When the appliance restarts after a crash, the server inventory is evaluated for any long-running activity that failed, such as applying server profile settings, that might have been in progress when the crash occurred. You can recover by performing the same action again, such as reapplying the server profile settings.

The appliance resynchronizes the servers. During resynchronization, each server hardware enters the `resyncPending` state. A full resynchronization of individual server hardware includes rediscovering the server hardware, verifying the server hardware power state and updating the



resource state accordingly, and updating the health status. The appliance creates a task queue for each task during a resynchronization operation.

Symptom	Possible cause and recommendation
Connectivity to server is lost	Open the Server Hardware activities panel to determine if any server hardware has a critical status, which might indicate a crash. For servers in that state, follow the troubleshooting recommendations in the alert.

27.12 Troubleshooting server profiles

27.12.1 Server profile is not created or updated correctly

When a server profile is not created or updated correctly, a notification appears at the top of the screen stating the profile operation was not successful; click the notification area to show more details. Also, the status icon next to the server profile name indicates it is in an `Error` condition

(). The profile remains on the appliance, but you must to correct it. When you correct the server profile, the profile status changes to OK ().

Symptom	Possible cause and recommendation
Server profile is not created or updated correctly	<p>Prerequisites and conditions have not been met</p> <ol style="list-style-type: none"> 1. Verify that the prerequisites listed in the online help have been met. 2. Verify that the following conditions are TRUE: <ul style="list-style-type: none"> • The profile name is unique • The selected server hardware is powered off • The server hardware is in the <code>No Profile Applied</code> state, has the correct firmware, and the ports are mapped to the correct interconnect • The server hardware is able to power cycle, and a user did not shut down the server hardware while the profile settings were being applied • You applied the correct iLO and ROM firmware levels • You are using supported server hardware • The environment has been configured • The iLO has an IP address and network connectivity • Communication exists with the server hardware iLO, including but not limited to whether the iLO is functioning, network cabling is connected and functional, and there are no problems with switches or interconnects in the management network • The add enclosure operation successfully completed • The OA has network connectivity • The add server hardware operation successfully completed • The specified network or network set is available on the server hardware port • The interconnects are in the <code>Configured</code> state, and have the correct firmware • The logical interconnect configuration matches its logical interconnect group definition • There are no duplicate networks on a physical port • If multiple adapters are installed, all adapters must have the same firmware version • User-specified addresses are unique and have correct format 3. When the issues have been addressed, either edit the profile or delete the profile and create another profile. <p>Server profile has duplicate networks on the same physical port</p> <ul style="list-style-type: none"> • Change the connection to a different port. • Change the connection to use a different VLAN.
Server profile fails to add connection	<p>The following conditions have not been met</p> <ul style="list-style-type: none"> • The interconnects are in the <code>Configured</code> state, and have the correct firmware • The servers are in <code>No Profile Applied</code> state, have the correct firmware, and the ports are mapped to the correct interconnect

Symptom	Possible cause and recommendation
A profile operation timeout when applying BIOS settings	<p>The server hardware or its iLO are powered-off or reset</p> <ul style="list-style-type: none"> In most cases, retrying the operation resolves the problem <p>The appliance cannot collect progress information from the iLO</p> <ul style="list-style-type: none"> In most cases, retrying the operation resolves the problem
Auto-assignment for FlexNIC fails while deploying connections	<p>Invalid configuration</p> <ul style="list-style-type: none"> Auto-assignment for FlexNIC connections does not validate the following: <ul style="list-style-type: none"> Bandwidth oversubscription on the physical port Maximum networks (VLANs) on the physical port Duplicate networks (VLANs) on the physical port Manual assignment is required

27.12.2 What to do when you cannot apply the server profile

Symptom	Possible cause and recommendation
Cannot apply the server profile	If you cannot apply the server profile because the PXE boot does not boot within the expected amount of time, reset the iLO.
Cannot verify the status of the server hardware	<p>Verify the operational status of the server hardware</p> <ol style="list-style-type: none"> Click Cancel to exit from the Create Server Profile screen. From the main menu, navigate to the Server Hardware screen. Find, and then select the server hardware.

27.12.3 Profile operations fail

Symptom	Possible cause and recommendation
Message indicates that the server is managed by another management system	<p>The enclosure is no longer managed by the appliance</p> <p>To prevent losing all allocated virtual IDs, perform the following steps before forcibly deleting the server profile.</p> <ol style="list-style-type: none">1. Use REST APIs to get the server profile. <code>GET /rest/server-profiles</code>2. Force delete the profile using the UI or REST APIs.3. Recreate the IDs using the User Specified option in the UI, or use REST APIs to create the server profile:<ol style="list-style-type: none">a. Get the server profile. <code>GET /rest/server-profiles</code>b. Edit the server profile.<ol style="list-style-type: none">1) Remove <code>uri</code>, <code>serverHardwareTypeUri</code>, <code>enclosureGroupUri</code>, <code>enclosureUri</code>, and <code>enclosureBay</code>.2) Change the <code>serverHardwareUri</code> value to the server the profile is going to be associated to.3) Change <code>serialNumberType</code> from <code>Virtual</code> to <code>UserDefined</code>.4) In the <code>connections</code> property, change <code>macType</code> from <code>Virtual</code> to <code>UserDefined</code>.5) In the <code>connections</code> property, change <code>wwpnType</code> from <code>Virtual</code> to <code>UserDefined</code>.6) In the <code>connections</code> property, if applicable change <code>networkUri</code> with the correct networks.c. Create the server profile. <code>POST /rest/server-profiles</code>

27.13 Troubleshooting user accounts

27.13.1 Incorrect privileges

Users must have view privileges (at minimum) on a managed object to see that object in the user interface.

Symptom	Possible cause and recommendation
Unable to see specific resource information or perform a resource task	<p>Your assigned role does not have the correct privileges</p> <ul style="list-style-type: none">• Request a different role or an additional role from the Infrastructure administrator in order to do your work

27.13.2 Unauthenticated user or group

Each user is authenticated on login to the appliance by the authentication service that confirms the user name and password. The **Edit Authentication** screen enables you to on the appliance; the default values are initially populated during first time setup of the appliance.

Symptom	Possible cause and recommendation
Unable to configure a directory user or group	<ol style="list-style-type: none">1. From the Users screen, click Add Directory User or Group.2. Click add a directory.3. From the Edit Authentication screen, click Add directory.4. Provide the requested information5. Click OK

27.13.3 User public key is not accepted

Symptom	Possible cause and recommendation
User public key does not work or is not accepted	Hidden characters introduced during a copy/paste operation change the key code <ul style="list-style-type: none">Enter the key again, taking care to prevent special characters from being injected into the key when pasting it into the public key field

27.13.4 Directory service not available

Symptom	Possible cause and recommendation
No connectivity	Directory service server is down <ol style="list-style-type: none">Locally run the <code>ping</code> command on the directory server's IP address or host name to determine if it is on-line.Verify that the appliance network is operating correctly.Contact the directory service administrator to determine if the server is down.

27.13.5 Cannot add directory service

Symptom	Possible cause and recommendation
Connectivity	Lost connection with directory service host <ol style="list-style-type: none">Verify that the settings for the directory service host are accurate.Locally run the <code>ping</code> command on the directory server's IP address or host name to determine if it is on-line.Verify that the port for LDAP communication with the directory service is correct.Verify that the port you are using for communication is not blocked by any firewalls.Verify that the appliance network is operating correctly.Determine that the appliance virtual machine is functioning properly and that there are enough resources.
Cannot log in	Inaccurate credentials <ol style="list-style-type: none">Verify the login name and password are accurate.Verify the search context information is accurate; you might be trying to access a different account or group.Re-acquire and install the directory service host certificate.Contact the directory service provider to ensure that the credentials are accurate.

27.13.6 Cannot add server for a directory service

Symptom	Possible cause and recommendation
Connectivity	Lost connection with directory service host <ol style="list-style-type: none">1. Verify that the settings for the directory service host are accurate.2. Verify that the correct port is used for the directory service.3. Verify that the port you are using for communication is not blocked by any firewalls.4. Locally run the <code>ping</code> command on the directory service host's IP address or host name to determine if it is on-line.5. Verify that the appliance network is operating correctly.6. If the appliance is hosted on a virtual machine, determine that it is functioning properly and there are enough resources.
Cannot log in	Inaccurate credentials <ol style="list-style-type: none">1. Verify that the login name and password are accurate.2. Reacquire and install the directory service host certificate.3. Contact the directory service provider to ensure that the credentials are accurate.

27.13.7 Cannot add directory user or group

Symptom	Possible cause and recommendation
Cannot log in	Lost connection with directory service host <ol style="list-style-type: none">1. Verify that the settings for the directory service host are accurate.2. Verify that the correct port is used for the directory service.3. Verify that the port you are using for communication is not blocked by any firewalls.4. Locally run the <code>ping</code> command on the directory service host's IP address or host name to determine if it is on-line.5. Verify that the network the appliance is on and is operating correctly.6. If the appliance is hosted on a virtual machine, determine that it is functioning properly and there are enough resources. Inaccurate credentials <ol style="list-style-type: none">1. Verify that the login name and password are accurate.2. Reacquire and install the directory service host certificate.3. Contact the directory service provider to ensure that the credentials are accurate.
Cannot find user or group	User or group not configured in the directory service <ol style="list-style-type: none">1. Verify the name of the user or group.2. Contact the directory service administrator to verify that the user or group account is configured in the directory service.3. Verify that the user or group is within four hierarchical levels from the group specified by the DN.

28 Restoring an appliance from a backup file

This chapter describes how to use the UI, REST APIs, or a custom-written PowerShell script to restore a corrupted appliance from a backup file. A restore operation is required only to recover from catastrophic failures, not to fix minor problems that can be resolved in other ways.

UI screens and REST API resources

UI screen	REST API resource
Settings → Actions	restores

For more information about restoring an appliance, see the online help for the **Settings** screen.

- ❗ **IMPORTANT:** Do not use any hypervisor-provided capabilities or snapshots to restore an HP OneView appliance because doing so can cause synchronization errors and result in unpredictable and unwanted behavior.

28.1 Roles

Users with Infrastructure administrator or Backup administrator privileges can create and download backup files, however, only an Infrastructure administrator can restore an appliance from a backup file.

28.2 Restore operation overview

You can restore an appliance from a backup file that was created on the same appliance or, if an appliance fails and cannot be repaired, from a backup file from a different appliance.

During a restore operation, the appliance firmware reconciles the data in the backup file with the current state of the managed environment. There are some discrepancies that a restore operation cannot resolve automatically. After a restore operation is complete, the Infrastructure administrator must manually resolve any remaining inconsistencies, which are identified by activities.

See also [“Post-restoration tasks” \(page 224\)](#).

- ❗ **IMPORTANT:** After the restore operation, you need to upload the firmware baselines required by your server profiles, enclosures, and logical interconnects. Refer to each profile's **Firmware baseline** setting to determine the file name for the required baseline. You do not need to upload the default baseline, HP Service Pack for ProLiant - Base Firmware, which is included in the appliance image.

You should only use a restore operation to recover from catastrophic failures. Do not use it for minor problems that can be resolved in other ways.

Restoring a backup file replaces all management data and most configuration settings on the appliance.

The appliance is not operational during a restore operation.

It can take several hours to perform a restore operation.

A restore operation cannot be canceled or undone after it has started.

28.3 Preparing to restore an appliance

- Make sure that all users logged in to the appliance log out. Users who are logged in when the restore operation begins are automatically logged out, losing whatever work was in progress.
All users are blocked from logging in during a restore operation.
- Stop all automatically scheduled backups.
Restart the automatically scheduled backups after the appliance is restored.
- Make sure the appliance network settings are the ones you want the appliance to use after the restore operation.
- Ensure that the appliance being restored and the appliance on which the backup file was created are running compatible firmware versions.
The platform type, hardware model, major number, and minor number must match to restore a backup. The revision and build numbers do not need to match. The format of the appliance firmware version follows:
majornumber.minornumber.revisionnumber-buildnumber
If the backup file is incompatible with the firmware on the appliance, the upload returns an error and the restore operation stops. You will need to update the firmware or select a different backup file.
- Consider doing the following:
 - Maintain a list of the current user accounts on the appliance, and note the passwords you use.
The restore operation resets the user names and passwords to those that were in effect when the backup file was created.
 - Create a support dump.
Use the support dump to diagnose failures that occurred before the restore operation.
 - Download the existing audit logs, or store them for safekeeping.
The restore operation restores the audit logs from the backup file, overwriting the existing logs.
- If the backup file was created on an appliance that is different from the one you are restoring, do one of the following:
 - Decommission the original appliance.
 - Reconfigure the original appliance so that it no longer manages the devices it was managing when the backup file was created.
- Serious errors can occur if multiple appliances attempt to manage the same devices.
- Make the backup file accessible to the system from which you plan to issue the upload request. If you are using an enterprise backup/restore product to archive backup files, take any steps required by your backup/restore product to prepare for the restore operation.

28.4 Restore an appliance from a backup file

Before you restore an appliance from a backup file, note the following:

- A restore operation should only be used to recover from catastrophic failures. Do not use it for minor problems that can be resolved in other ways.
- The appliance is not operational during a restore operation.
- A restore operation cannot be canceled or undone after it has started.
- Use the latest backup file to restore the appliance. Changes made after the backup file is created cannot be saved.
- Restoring an appliance from a backup file replaces all management data and most configuration settings on the appliance. You are directed to re-enter unresolved data, if applicable.
- The appliance firmware referenced in the backup file must be identical to the firmware running on the appliance; otherwise, the restore operation fails.
- The appliance blocks login requests while a restore operation is in progress.
- It can take several hours to perform a restore operation; the more resources and devices to restore, the longer the process takes.
- Restoring the appliance validates the resource inventory (enclosures, servers, interconnects, and so on).
- During the restore operation, HP OneView refreshes each enclosure to validate its contents—especially to ensure that the appliance still claims them. Then, HP OneView refreshes each blade server and clears the virtual IDs of any servers added to an enclosure since the last time the backup file was created. HP OneView also refreshes all rack servers to ensure the appliance still claims them.

The appliance will also clear virtual IDs for servers that do not have a profile assigned but do have virtual IDs configured. These servers most likely had a profile assigned after the last backup was made.

- If you removed, and then re-added an enclosure after a backup file was created, and then perform a restore operation using that backup file, you must refresh the enclosure before the appliance can connect.
- If you added server hardware to the appliance after the backup file was created, that hardware is not in the appliance database when the restore operation completes. You must add that hardware to the appliance and then repeat any other configuration changes (such as assigning server profiles) that were made between the time the backup file was created and the restore operation completed.

HP recommends that you perform frequent backups, and especially after adding any hardware or changing the configuration.

After restoring the appliance, you must upload all the firmware bundles that were used by your existing server profiles, enclosures, and logical interconnects. Refer to each profile's *Firmware baseline* setting, which displays the file name of the required baseline.

You do not need to upload the default firmware bundle, *HP Service Pack for ProLiant - Base Firmware*. It is already included in the appliance image.

Prerequisites

- Minimum required privileges: Infrastructure administrator.
- Ensure that all tasks have been completed or stopped, and that all other users are logged off.

Restoring an appliance from a backup file

1. From the **Settings** screen, select **Actions**→**Restore from backup**.
2. Read the on-screen notification, then select the check box to confirm.
3. From the dialog box that opens, do one of the following:
 - Drag the backup file from a local folder or directory and drop it into the indicated field.
 - Click **Browse** and select the backup file to upload.

NOTE: Not all browsers and browser versions offer the same capabilities.

4. Click **Upload file**.
Wait until the file upload is complete.
A progress bar is displayed during the upload, and the file name, creation date, and version are displayed upon completion.
5. Select **Restore from backup** in the dialog box.
6. Select **Restore from backup** again.
7. Wait until the restore operation is complete. A status page indicates the progress.
8. Upon completion of the restore operation, you are returned to the login page where you can log in to the restored appliance.
9. Upload the firmware bundles used by your existing profiles, enclosures, and logical interconnects. These were not saved as part of the backup file.

28.5 Using REST APIs to restore an appliance from a backup file

Prerequisites

- Minimum required session ID privileges: Infrastructure administrator
- You have uploaded a backup file to the appliance.

Restoring the appliance from a backup file using REST APIs

1. Initiate the restore process.
`POST /rest/restores`
The `{restore URI}` is returned.
 2. List the status of the restore process.
`GET /rest/restores`
-

28.6 Creating a custom script to restore an appliance

If you prefer to write a script to restore an appliance from a backup file, see [“Sample restore script” \(page 282\)](#) for a sample PowerShell script that you can customize for your environment.

28.7 Post-restoration tasks

During a restore operation, the appliance reconciles the data in the backup file with the current state of the managed environment. There are some discrepancies that a restore operation cannot resolve automatically, for example, if servers were added after the backup file was created. The network configuration on these servers is unknown to the appliance after a restore and could result in duplicate MAC addresses and World Wide Names (WWNs), as a result.

After a restore operation completes, you must manually resolve any remaining alerts and add these servers back into the appliance to eliminate the risk of duplicate IDs. You must also perform manual

cleanup of hardware (servers, interconnects, and enclosures) if server profiles are forcibly unassigned or the hardware is forcibly removed without first being unconfigured.

Preventing duplicate IDs on the network after a restore

1. After a restore operation is complete, re-add any enclosure or server hardware added since the selected backup.

NOTE: For any enclosures added since the last backup that you decide *not* to re-add after the restore, avoid duplicate IDs by running the Onboard Administrator SSH command `clear vcmode` on these enclosures. Running this command ensures the virtual MACs and WWNs on the server blades in the enclosure have been cleared.

2. For any server profile alerts about the profile not matching the server hardware:
 - a. Identify all server profiles with a mismatch-type of error message. Make a list of these server profiles and the assigned server hardware.
 - b. Power off the server, and then unassign all of the server profiles individually. From the **Server Profiles** screen, select **Actions**→**Edit**, and then select **Unassign** from the server hardware drop down selector. Click **OK**.
 - c. Select **Actions**→**Edit** again, and then reassign all of the documented profiles to the documented server hardware.
3. For any alerts about ID ranges, the Network administrator should examine the address and identifier ranges and edit them, if needed.
4. Re-create any profiles for the servers in any enclosures that were added in step 1.

29 Support and other resources

To learn how to contact HP, obtain software updates, submit feedback on documentation, and locate links to HP OneView websites and other related HP products, see the following topics.

29.1 Gather information before contacting an authorized support representative

If you need to contact an authorized HP support representative, be sure to have the following information available:

- Your Service Agreement Identifier (SAID)
- Software product name — HP OneView
- Hypervisor virtualization platform and version
- Messages generated by the appliance
- Other HP or third-party software in use

29.2 How to contact HP

- See the Contact HP Worldwide website to obtain contact information for any country:
<http://www.hp.com/go/assistance>
- See the contact information provided on the HP Support Center website:
<http://www.hp.com/go/hpsc>
- In the United States, call +1 800 334 5144 to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored. Say *OneView* when prompted for the product name.

29.3 Get connected to the HP OneView online user forum

The HP OneView interactive online forum enables you to share your experiences and pose and answer questions related to using HP OneView.

This forum also hosts PowerShell and Python libraries that utilize the comprehensive HP OneView RESTful APIs to perform any operation.

See <http://www.hp.com/go/oneviewcommunity> to join the discussion.

29.4 Software technical support and software updates

HP OneView software products include three years of 24 x 7 software technical support and update services, which provides access to technical assistance to resolve software implementation or operations problems.

With this service, you benefit from expedited problem resolution as well as proactive notification and delivery of software updates.

See <http://www.hp.com/go/hpsc> for more information.

29.4.1 Registering for software technical support

When you order HP OneView, you receive a license entitlement certificate by physical shipment or email, which you must redeem online in order to obtain the license activation key.

After redeeming your license certificate activation key, you are prompted to register for software technical support and update services. Licenses that are embedded in the hardware are automatically registered.

See <http://www.hp.com/go/insightlicense> for more information.

29.4.2 Using your software technical support and update service

Once registered, you receive a service contract in the mail containing the customer service phone number and your Service Agreement Identifier (SAID). You need the SAID when you phone for technical support.

29.4.3 Obtaining HP OneView software and firmware updates

See <http://www.hp.com/go/oneviewupdates> to obtain HP OneView software updates and product-specific firmware bundles.

29.4.4 Obtaining software and drivers for HP ProLiant products

See <http://welcome.hp.com/country/us/en/support.htm> for the latest software and drivers for your HP ProLiant products.

29.4.5 Warranty

HP will replace defective delivery media for a period of 90 days from the date of purchase. This warranty applies to all products found on the delivery media.

29.5 Related information

Documentation

- HP OneView Information Library
<http://www.hp.com/go/oneview/docs>

Product websites

- HP OneView
 - Primary website: <http://www.hp.com/go/oneview>
 - Software and firmware updates: <http://www.hp.com/go/oneviewupdates>
 - User forum: <http://www.hp.com/go/oneviewcommunity>
 - Product demos: www.hp.com/go/oneviewdemos
 - Infrastructure management: www.hp.com/go/management-oneview
 - End-User license agreement: <http://www.hp.com/oneview/eula>
- HP Open Source Download Site
<http://www.hp.com/software/opensource>
- HP BladeSystem enclosures
<http://www.hp.com/go/bladesystem>
- HP ProLiant server hardware
<http://www.hp.com/go/proliant>

- HP ProLiant education
<http://www.hp.com/learn/proliant>
- HP Storage products
<http://www.hp.com/go/storage>
- HP Virtual Connect
<http://www.hp.com/go/virtualconnect>

29.6 Submit documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve our documentation, send errors, suggestions, and comments to:

docsfeedback@hp.com

For UI and REST API help

In your email message, include the product name, product version, help edition, and publication date located on the legal notices page.

For user guides and other manuals

In your email message, include the document title, edition, publication date, and document part number located on the front cover. Any other information you can provide, such as a section title or page number, is also helpful.

A Step by step: Configuring an example data center using HP OneView

This appendix contains an illustrated example of using the HP OneView appliance UI to configure and manage an example (fictional) data center. It demonstrates using the UI to:

1. Provision eight VMware vSphere ESXi host servers using the HP OneView appliance and vSphere Auto Deploy feature. This demonstration includes adding a firmware bundle to the appliance, establishing a firmware baseline for an enclosure, and creating networks and network sets that are used in the demonstrations that follow.
2. Configure a server blade to boot from SAN from an HP 3PAR Storage System that is directly attached to the enclosure that contains the server blade.
3. Bring an HP ProLiant DL360p Gen8 rack mount server under management. This scenario includes adding a license to the appliance and using the appliance **Map** view to display relationships between resources.



IMPORTANT:

- The information in this appendix, including all IP addresses, names, user names, passwords, and hardware and software configurations, is intended as an example for demonstration purposes only.
- The example in this appendix was created using HP OneView Version 1.0 and might not be valid for other versions of the software.

Video demonstrations of HP OneView are also available. See [“Support and other resources”](#) (page 227).

A.1 Tasks you can perform without data center hardware

You can perform the following tasks before you add any hardware to the appliance:

- Plan the data center configuration.
- Install the appliance.
- Add, edit, and delete networks, network sets, logical interconnect groups, and enclosure groups.
- Add, edit, and delete server profiles that are not assigned to hardware. Not all aspects of a server profile can be configured before the appropriate server hardware is added to the appliance.
- Upload firmware bundles to the appliance repository.
- Remove firmware bundles from the appliance repository.
- Add and delete users.
- Change settings.
- Create support dump files.
- Create backup files.

A.2 Information about the sample data center

A.2.1 Sample data center hardware

The sample data center hardware includes:

- One HP ProLiant DL360p Gen8 rack mount server
- One rack that contains the enclosures and rack mount servers

- Two HP BladeSystem c7000 Enclosures, each of which contain HP Virtual Connect FlexFabric modules and several different models of HP BladeServer server blades
- A pair of SAN switches that connect to data center storage devices
- A pair of Ethernet switches that connect to the data center networks
- An HP 3PAR Storage System that connects directly to one of the enclosures (a Flat SAN configuration)

All of the hardware is located in the same room.

Rack mount server

Attribute	Description
Model	HP ProLiant DL360p Gen8
Name	DL360pGen8-1796
iLO IP address	172.18.6.15
iLO administrator credentials	User name iLOAdmin Password S&leP@ssw0rd
Physical location	Rack 173, U26

Enclosure 1

Attribute	Description
Name	Enclosure-174
Primary Onboard Administrator IP address	172.18.1.11
Secondary Onboard Administrator IP address	172.18.1.12
Onboard Administrator credentials	User name OAAAdmin Password S&leP@ssw0rd
iLO administrator credentials (all servers)	User name iLOAdmin Password S&leP@ssw0rd
Physical location	Rack 173, U1 through U10

Interconnect hardware	I/O bay number
HP Virtual Connect FlexFabric 10Gb/24-Port Module	1, 2

Server hardware model	Server bay numbers
HP ProLiant BL660c Gen8	1, 2
HP ProLiant BL460c Gen8	3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16
None (bay is empty)	9, 10

Enclosure 2

Attribute	Description
Name	Enclosure-1904
Primary Onboard Administrator IP address	172.18.1.13
Secondary Onboard Administrator IP address	172.18.1.14
Onboard Administrator credentials	User name OAAAdmin Password S&leP@ssw0rd
iLO administrator credentials (all servers):	User name iLOAdmin Password S&leP@ssw0rd
Physical location	Rack 173, U11 through U20

Interconnect hardware	I/O bay number
HP Virtual Connect FlexFabric 10Gb/24-Port Module	1, 2

Server hardware models	Server bay numbers
HP ProLiant BL660c Gen8	1, 2
HP ProLiant BL460c Gen8	3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16
None (bay is empty)	9, 10

HP Virtual Connect FlexFabric 10Gb/24-Port Module port configurations

Ports	Permitted configurations
X1, X2, X3, X4	Either Fibre Channel or 10Gb Ethernet
X5, X6	Either 1GB or 10Gb Ethernet
X7, X8	Either internal stacking link or 1GB or 10Gb Ethernet. If a port is used for an internal stacking link, do not use it for an external Ethernet connection. For this data center, use X7 for the internal stacking link.

A.2.2 Data center networks

All data center switch ports that connect to the VC (Virtual Connect) interconnect modules are configured as described in [“Data center switch port requirements” \(page 115\)](#).

A.2.2.1 Fibre Channel networks

Fibre Channel networks for the SAN fabrics

The sample data center has two Fibre Channel SAN switches. To see a graphical representation of the configuration, see [Figure 17 \(page 235\)](#).

The names for the Fabric attach Fibre Channel networks are:

- SAN A
- SAN B

Table 11 SAN A and SAN B Fibre Channel network configurations

Configuration attribute	Value	Notes
Type	Fibre Channel	
Fabric type	Fabric attach	Choose Fabric attach for Fibre Channel networks that connect to SAN switches in the data center.
Preferred bandwidth	2.5 Gb/s	This is the default value displayed on the Create network screen.
Maximum bandwidth	8 Gb/s	This is the default value displayed on the Create network screen.
Uplink speed	Auto	This is the default value displayed on the Create network screen.
Login redistribution	Auto	This is the default value displayed on the Create network screen.
Link stability time	30 seconds	This is the default value displayed on the Create network screen.

Fibre Channel networks directly attached to the 3PAR Storage System (Flat SAN)

The sample data center has a 3PAR Storage System that is connected directly to an enclosure. This is called a Flat SAN or Direct attach network configuration. To see a graphical representation of the configuration, see [Figure 17 \(page 235\)](#).

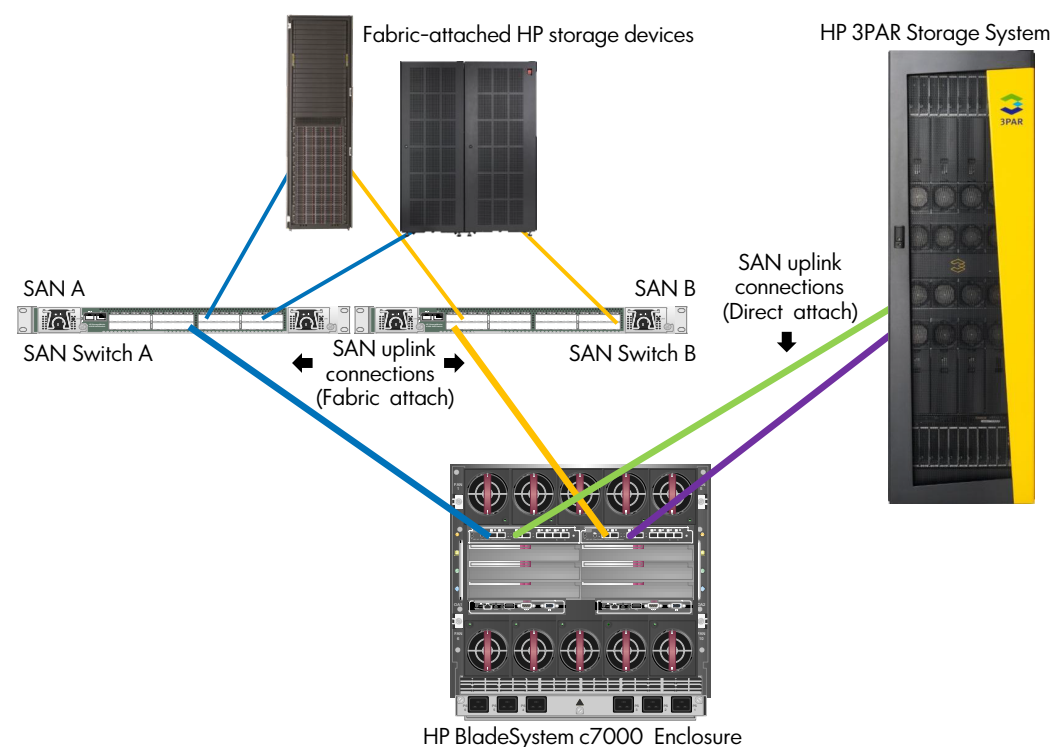
The names of the Direct attach Fibre Channel networks follow:

- FlatSAN A
- FlatSAN B

Table 12 FlatSAN A and FlatSAN B Fibre Channel network configurations

Configuration attribute	Value	Notes
Type	Fibre Channel	
Fabric type	Direct attach	Choose Direct attach for Fibre Channel networks that connect to the 3PAR storage system.
Preferred bandwidth	2.5 Gb/s	This is the default value displayed on the Create network screen.
Maximum bandwidth	8 Gb/s	This is the default value displayed on the Create network screen.
Uplink speed	Auto	This is the default value displayed on the Create network screen.
Login redistribution	Auto	This is the default value displayed on the Create network screen.
Link stability time	30 seconds	This is the default value displayed on the Create network screen.

Figure 17 Sample data center: Fibre Channel network connections



A.2.2.2 Ethernet Networks

You will configure all of the networks described in this section with the attributes listed in [Table 17 \(page 236\)](#).

For each Ethernet network:

- The network name indicates the purpose of the network and enables users to search and filter by networks with similar names and purposes.
- The VLAN ID in the network name enables users to determine the VLAN ID of the network without having to look it up.

Table 13 Networks for vMotion and virtual machine management

Name	VLAN ID	Notes
esxi mgmt 1131	1131	This is the boot network that includes the PXE server.
esxi vmotion 1132	1132	This is the network used for live migration of VMs (virtual machines).

Table 14 Production networks

Name	VLAN ID
prod 1101	1101
prod 1102	1102
prod 1103	1103
prod 1104	1104

Table 15 Development networks

Name	VLAN ID
dev 1105	1105
dev 1106	1106
dev 1107	1107
dev 1108	1108

Table 16 Test networks

Name	VLAN ID
test 1111	1111
test 1112	1112
test 1113	1113
test 1114	1114

Table 17 Ethernet network configuration values

Configuration attribute	Value	Notes
Type	Ethernet	
Preferred bandwidth	2.5 Gb/s	This is the default value displayed on the Create network screen.
Maximum bandwidth	10 Gb/s	This is the default value displayed on the Create network screen.
Smart link	Selected	This is the default value displayed on the Create network screen.
Private network	Not selected	This is the default value displayed on the Create network screen.

A.3 Planning the configuration

A.3.1 Planning for installation of the appliance

For the sample data center, assume that you make the following choices before and during installation:

- You follow the recommendations in the *HP OneView Installation Guide*, including:
 - Choosing a physical host for the appliance virtual machine (VM) that is not targeted to be managed by this appliance
 - Choosing a static IP address
 - Ensuring that the ports required by the appliance are available
- You allow support personnel to access the appliance.
- You synchronize the appliance time with the VM host time.
- When prompted to change the Administrator password, you use the password SDC14u\$.
- You specify the following for the appliance networking settings:

Configuration attribute	Value
Appliance host name	myhostname.example.com
IPv4 address assignment	Manual
Subnet mask	255.255.240.0

Configuration attribute	Value
Gateway address	172.18.0.0
Preferred DNS server	172.18.0.0
Alternate DNS server	172.18.0.1
IPv6 address assignment	Unassigned (do not use IPv6 addresses)

A.3.2 Planning for network sets

To enable servers to connect any Ethernet production network or test network without having to specify an individual network name, and to provision additional networks of these types without being required to change the configuration for every server, this data center requires network sets for these networks:

- Production networks
- Development networks
- Test networks

A.3.3 Planning for users and roles

The Administrator user ID, which has full access and privileges on the appliance, can perform all configuration steps.

The appliance provides RBAC (role-based access control), which enables an administrator to quickly establish authentication and authorization for users based on their responsibilities for specific resources. Users can view only the resources for which they are authorized, and they can initiate actions only for the resources for which they are authorized.

The appliance also provides SSO (single sign-on) for the server iLO and the enclosure Onboard Administrator. The appliance roles are mapped to the appropriate role for the iLO or Onboard Administrator.

[“Understanding the security features of the appliance” \(page 45\)](#) describes controlling access for authorized users. The online help lists the minimum required privileges for each task and resource.

For the sample data center, assume that all tasks are performed by a user with Infrastructure administrator privileges, such as the Administrator user.

A.3.4 Planning resource names

Searching and filtering in the appliance is based on a smart search model. By embedding information about the resource in the resource name, you can take advantage of the search and filter capability. In this example:

- All uplink set names include the text `US`.
Example: `testUS`
- The names of Direct attach Fibre Channel networks include the text `FlatSAN`.
Example: `FlatSAN A`
- The names of networks, network sets, and uplink sets include text that indicates the purpose of the network:

Network category	Text used in names	Examples
production networks	<code>prod</code>	<code>prod 1101</code> , <code>prod networks</code> , <code>prodUS</code>
development networks	<code>dev</code>	<code>dev 1105</code> , <code>dev networks</code> , <code>devUS</code>
test networks	<code>test</code>	<code>test 1111</code> , <code>test networks</code> , <code>testUS</code>

For information about what to consider when choosing resource names, see [“Planning resource names” \(page 238\)](#).

A.4 Installing the appliance

For installation instructions, see the *HP OneView Installation Guide*.

A.5 Provisioning eight host servers for VMware vSphere Auto Deploy

This example demonstrates using the appliance to provision and prepare eight server blades for use by VMware vSphere Auto Deploy to create a host cluster.

Assumptions

- The appliance has been installed and the appliance networking settings have been configured, but no other configuration has been completed.
- You are adding Enclosure 1 of the sample data center.
- The enclosure has embedded licenses.
- You will add the Ethernet networks and Fabric attach SAN networks described in [“Data center networks” \(page 233\)](#).

A.5.1 Workflow

1. [“Downloading the latest firmware bundle and adding it to the appliance” \(page 239\)](#).
2. [“Configuring the networks and network sets for a typical vSphere Auto Deploy environment” \(page 239\)](#).
3. Configuring an enclosure group that captures the VC uplink configuration in its logical interconnect group:
 - a. [“Creating the logical interconnect group” \(page 244\)](#).
 - b. [“Creating an enclosure group for vSphere \(ESXi\) hosts” \(page 248\)](#).
4. [“Adding the enclosure” \(page 249\)](#).
5. [“Viewing the server hardware types” \(page 249\)](#).

6. “Create an unassigned server profile for use as a template for ESXi servers” (page 250).
This server profile includes a firmware baseline, the BIOS settings for the profile, and the network connections required for vSphere host servers in the sample data center.
7. “Copying the template server profile to eight servers” (page 255).

A.5.2 Downloading the latest firmware bundle and adding it to the appliance

You use the latest firmware bundles in your firmware baselines to ensure that managed resources have the latest firmware and to enable you take advantage of all available management features.

1. Download SPPs from the HP website www.hp.com/go/spp to your local system.
2. From the [main menu](#), select **Firmware Bundles**, and then click **Add Firmware Bundle** in the [master pane](#).
3. Do one of the following:
 - Drag and drop the firmware bundle file onto the shaded portion of the screen.
 - Click **Choose File** to select the `.iso` file that contains the firmware bundle.
4. Click **Start upload** to upload the firmware bundle (the `.iso` files) to the firmware bundle repository.

NOTE: Wait for the SPP upload to complete before you start firmware updates or set firmware baselines. Keep this browser window open until the upload is complete and details about the SPP are displayed in the **Firmware Bundles** screen.



TIP: You can perform other tasks while the firmware bundle is uploading.

Uploading a firmware bundle can take several minutes. If the browser window closes before the upload completes, the upload fails. HP recommends starting the firmware upload in a separate browser window to prevent you from accidentally interrupting the upload as you perform other tasks.

A.5.3 Configuring the networks and network sets

A.5.3.1 Configuring the Fibre Channel SAN networks

In this procedure, you will create the Fibre Channel networks that connect to the Fibre Channel SAN switches in the data center. Fibre Channel networks that connect to Fibre Channel SAN switches are Fabric attach Fibre Channel networks.

Create the Fibre Channel SAN networks:

1. From the [main menu](#), select **Networks**, and then click + **Create network** in the [master pane](#).
The **Create network** dialog box opens.
2. For **Name**, enter **SAN A**.
3. For **Type**, select **Fibre Channel**.
4. For **Fabric type**, select **Fabric attach**.
5. For this data center, use the default values for the other configuration attributes.
6. Click **Create +**.

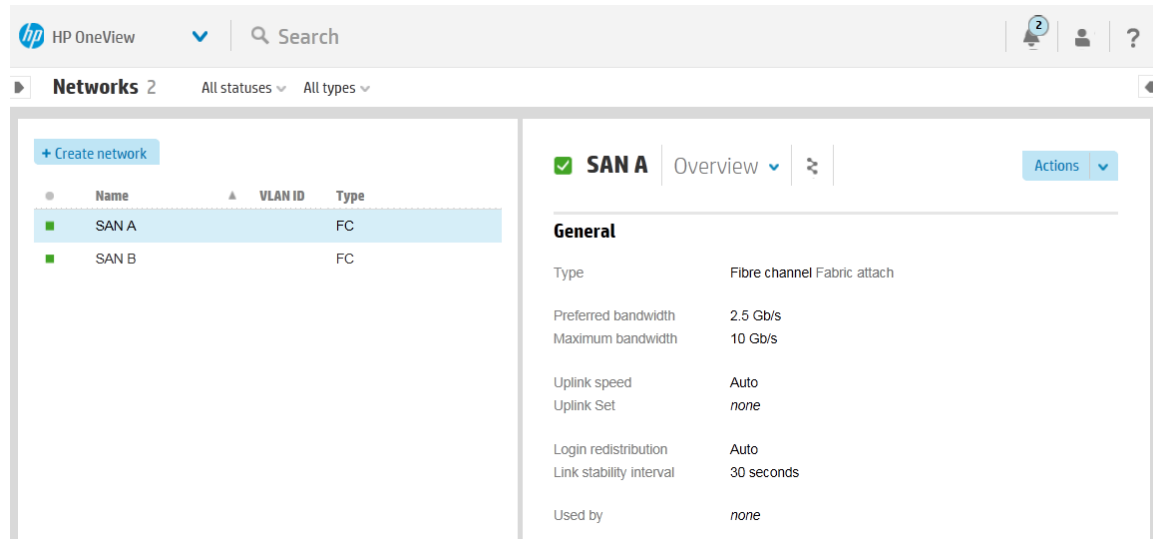
The appliance creates the network and opens the **Create network** dialog box. This dialog box uses the configuration values you selected in the preceding steps, except for the name.

7. For **Name**, enter **SAN B** and click **Create**.
The **Networks** screen opens.

After the networks are added, when you select a network in the [master pane](#), you can see details about that network in the details pane. For each of the networks you created:

- The value for **Uplink Set** is *none* because you have not yet defined an uplink set that uses this network. You will define the logical interconnect and its uplink sets in [“Creating a logical interconnect group and its uplink sets”](#) (page 244).
- The value for **Used by** is *none* because there are no server profiles using this network. You will define a server profile in [“Creating a server profile to use as a template”](#) (page 250).

The following figure shows the **Networks** screen after you add the Fibre Channel networks.



A.5.3.2 Configuring the Ethernet networks

1. From the [main menu](#), select **Networks**, and then click **+ Create network** in the [master pane](#). The **Create network** dialog box opens.

2. Create the ESXi management and vMotion networks:

- a. For **Type**, select **Ethernet**.
- b. For **Preferred bandwidth** and **Maximum bandwidth**, use the default values.
- c. Select **Smart link**, but do not select **Private network**.

Smart link specifies that if all of the uplinks to this network within an uplink set fail, server connections that specify this network report an error. This feature enables the server software to detect and respond to an uplink failure. It can be helpful when using certain server network teaming (bonding) configurations.

- d. For **Name**, enter **esxi mgmt 1131**.
- e. For **VLAN ID**, enter **1131**.
- f. For **Purpose**, select **Management**.
- g. Click **Create +** to create another network.

The appliance creates the network and opens the **Create network** dialog box. This dialog box uses the configuration values you selected in the preceding steps, except for the name and VLAN ID.

Behind the **Create network** dialog box, you might see the networks you create listed in the [master pane](#) of the **Networks** screen as those networks are added.

- h. For **Name**, enter **esxi vmotion 1132**.
- i. For **VLAN ID**, enter **1132**.
- j. For **Purpose**, select **VM Migration**.

- k. Click **Create +** to create another network.

The appliance creates the network and opens the **Create network** dialog box. This dialog box uses the configuration values you selected in the preceding steps, except for the name and VLAN ID.

3. Create the production networks.

For this procedure, you use the default values displayed on the **Create network** dialog box. Because all of the configuration values for production networks are the same except for the name and VLAN ID, you follow the same procedure for each network.

- a. For **Name**, enter the name of the network.
- b. For **VLAN ID**, enter the VLAN ID of the network.
- c. For **Purpose**, select **General**.
- d. Click **Create +** to create another network.

Use the following names and VLAN IDs for the production networks:

Name	VLAN ID
prod 1101	1101
prod 1102	1102
prod 1103	1103
prod 1104	1104

Behind the **Create network** screen, you also might see the networks you create listed in the [master pane](#) of the **Networks** screen as those networks are added.

4. Create the development networks and test networks.

For this procedure, you continue to use the default values displayed on the **Create network** dialog box. Because all of the configuration values for production networks are the same except for the name and VLAN ID, you follow the same procedure for each network:

- a. For **Name**, enter the name of the network.
- b. For **VLAN ID**, enter the VLAN ID of the network.
- c. Click **Create +** to create another network.

When you finish entering the values for the last Ethernet network you want to create, click **Create** instead of **Create +**. The **Networks** screen opens.

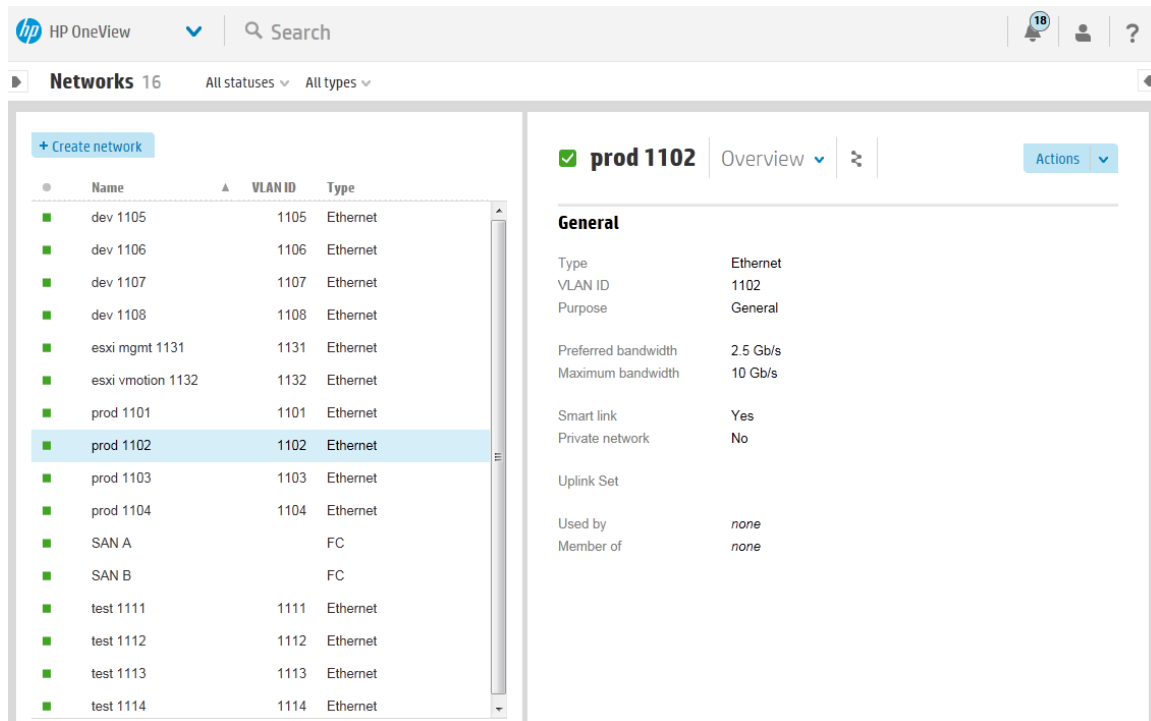
Use the following names and VLAN IDs for the development networks:

Name	VLAN ID
dev 1105	1105
dev 1106	1106
dev 1107	1107
dev 1108	1108

Use the following names and VLAN IDs for the test networks:

Name	VLAN ID
test 1111	1111
test 1112	1112
test 1113	1113
test 1114	1114

The following illustration shows the **Networks** screen after you add the Ethernet networks.



A.5.3.3 Configuring the network sets

You use network sets to create multiple networks per connection. During this task, you will use the smart search features of the appliance to quickly narrow down the list of networks to those networks you will add to the network set.

1. From the [main menu](#), select **Network Sets**, and then click **+ Create network set** in the [master pane](#).

The **Create network set** dialog box opens.

2. For all of the network sets in this data center, use the defaults displayed on the screen for **Type**, **Preferred Bandwidth**, and **Maximum Bandwidth**.
3. Create the network set for the production networks:

- a. For **Name**, enter **prod networks** and click **Add networks**.

The **Add Networks to prod networks** dialog box opens. All Ethernet networks that have been configured on this appliance are listed in alphabetical order.

- b. In the search box, enter **prod**.

The **Add Networks to prod networks** dialog box displays only the networks with names beginning with **prod**.

To learn more about searching and filtering, which is available throughout the appliance, see ["Search resources"](#) (page 67).

- c. Select all of the **prod** networks listed and click **Add** (see the following illustration).



TIP: You can use the **Ctrl** key to select multiple networks at once.

Add Networks to prod networks
?

prod

4 matches

Name	VLAN ID
prod 1101	1101
prod 1102	1102
prod 1103	1103
prod 1104	1104

4 selected
Add
Add +
Cancel

The **Create network set** dialog box shows the networks that you added to the network set.

- d. Select a network in the network set to receive untagged traffic.
 - i. On the **Create network set** dialog box, under **Networks**, locate the first network.
 - ii. Select the check box under **Untagged**.


The network you select as untagged receives untagged traffic in addition to traffic tagged with the VLAN ID for the network. For example, if you select `prod 1101` to receive untagged traffic, `prod 1101` receives traffic that is tagged with VLAN ID 1101 and traffic that is not tagged with any VLAN ID.

If you do not select a network to receive untagged traffic, untagged traffic is rejected.

The following illustration shows the **Networks** panel of the **Create network set** dialog box after you add the production networks and select the untagged network.

Networks

Name	VLAN ID	Untagged	
prod 1101	1101	<input checked="" type="checkbox"/>	×
prod 1102	1102	<input type="checkbox"/>	×
prod 1103	1103	<input type="checkbox"/>	×


Changed: Name to "prod networks"
Create
Create +
Cancel

- e. Click **Create +**.

The appliance creates the `prod networks` network set and opens the **Create network set** dialog box.

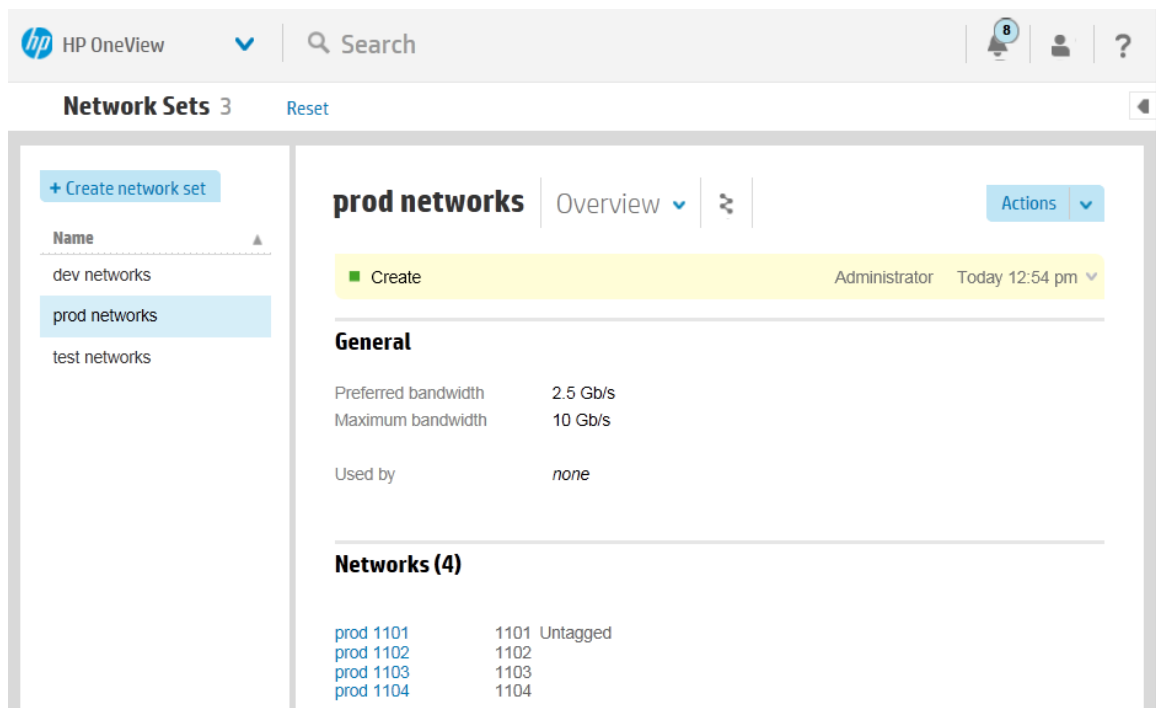
Behind the **Create network sets** dialog box, you might see the networks you create listed in the [master pane](#) of the **Network Sets** screen as those networks are added.

4. Create the network set for the development networks:
 - a. For **Name**, enter `dev networks` and click **Add networks**.

The **Add Networks to dev networks** dialog box opens.

- b. In the search box, enter **dev** to filter the list of networks.
 - c. Select all of the **dev** networks listed and click **Add**.
 - d. Select **Untagged** for the first network in the list of networks.
 - e. Click **Create +**.
5. Create the network set for the test networks:
 - a. For **Name**, enter **test networks** and click **Add networks**.
The **Add Networks to dev networks** dialog box opens.
 - b. In the search box, enter **test** to filter the list of networks.
 - c. Select all of the **test** networks listed and click **Add**.
 - d. Select **Untagged** for the first network in the list of networks.
 - e. Click **Create**.

The **Network Sets** screen opens. As shown in the following illustration, if you select a network set in the **master pane**, the appliance displays details about that network set in the details pane.



A.5.4 Creating a logical interconnect group and its uplink sets

You can create logical interconnect groups, including their uplink sets, and their associated enclosure groups in different ways:

- You can create them before you add enclosures to the appliance.
- You can create them during the enclosure add operation.

In this procedure, you will define the groups before you add any enclosures.

Creating the logical interconnect group

1. From the **main menu**, select **Logical Interconnect Groups** and click **+ Create logical interconnect group**.

The **Create logical interconnect group** dialog box opens. The large boxes on the screen represent enclosure interconnect bays, with bays 1 and 2 in the top row, bays 3 and 4 in the next row, and so forth. Only interconnects of the same model can be installed in horizontally adjacent bays.

2. For **Name**, enter **EsxFlexFabricLIG**.

3. In the top left box, click **Add interconnect** and select **HP Virtual Connect FlexFabric 10Gb/24-Port Module**.
4. In the top right box, click **Add interconnect** and select **HP Virtual Connect FlexFabric 10Gb/24-Port Module**.
5. Leave the dialog box open so that you can create the uplink sets.

Creating the uplink sets for the Fibre Channel networks

The uplink sets assign data center networks to physical interconnect ports.

1. Click **Add uplink set**.
The **Add uplink set** dialog box opens.
2. Configure the uplink set for the SAN A Fibre Channel network:
 - a. For **Name**, enter **SAN A**.
 - b. For **Type**, select **Fibre Channel**.
The dialog box expands to include additional configuration items.
 - c. For **Network**, select **SAN A**.
3. Configure the uplink ports:
 - a. For **Interconnect** under **Uplink Ports**, select **Interconnect: 1**.
The appliance displays the ports that you can use for Fibre Channel networks.
 - b. Select ports **X3** and **X4**.

Add uplink set ?

General

Name: SAN A

Type: ☐ Ethernet ☒ Fibre channel

Networks

Network: SAN A

Uplink Ports

Interconnect: interconnect: 1

☐ X1 ☐ X2 ☒ X3 ☒ X4

Create **Create +** **Cancel**

4. Click **Create +** to add the SAN A uplink set to the EsxFlexFabricLIG logical interconnect group and reopen the **Add uplink set** screen.

5. Add the uplink set for the SAN B:
 - a. For **Name**, enter **SAN B**.
 - b. For **Type**, select **Fibre Channel**.
 - c. For **Network**, select **SAN B**.
 - d. Configure the uplink ports. For **Interconnect** under **Uplink Ports**, select **Interconnect: 2** and then select ports **X3** and **X4**.
 - e. Click **Create**.

The **Create logical interconnect group** dialog box opens.

See the following illustration for an example.

Create logical interconnect group General ?

General

Name: EsxFlexFabricLIG

Logical Interconnect Group

SAN A (1 network, 2 uplink ports) is connected to ports X3 and X4 of the first HP VC FlexFabric 10Gb/24-Port Module.

SAN B (1 network, 2 uplink ports) is connected to ports X3 and X4 of the second HP VC FlexFabric 10Gb/24-Port Module.

Buttons: Add uplink set

Creating the uplink sets for the Ethernet networks

The uplink sets assign data center networks to physical interconnect ports.



TIP: If you click **Cancel** on the **Create Logical Interconnect Group** dialog box, all changes are discarded.

Instead of adding all of the uplink sets in one session, you can click **Create** to create the logical interconnect group, and then edit the logical interconnect group to add additional uplink sets.

1. Click **Add uplink set**.
The **Add uplink set** screen opens.
2. Configure the uplink set for the ESXi networks:
 - a. For **Name**, enter **esxiUS**.
 - b. For **Type**, select **Ethernet**.
The dialog box expands to include additional configuration items.
 - c. For **Connection Mode**, select **automatic**.
The default value, *automatic*, instructs the system to determine the best load-balancing scheme by creating as many LAGs (link aggregation groups) as possible in a physical interconnect, enabling multiple links to behave as a single link.
 - d. Click **Add networks** to open the **Add Networks to esxiUS** dialog box.

- e. Add the ESXi networks:
 - i. In the search box, enter **esx** to display only the ESXi networks.
 - ii. Select all of the EXSi networks listed.

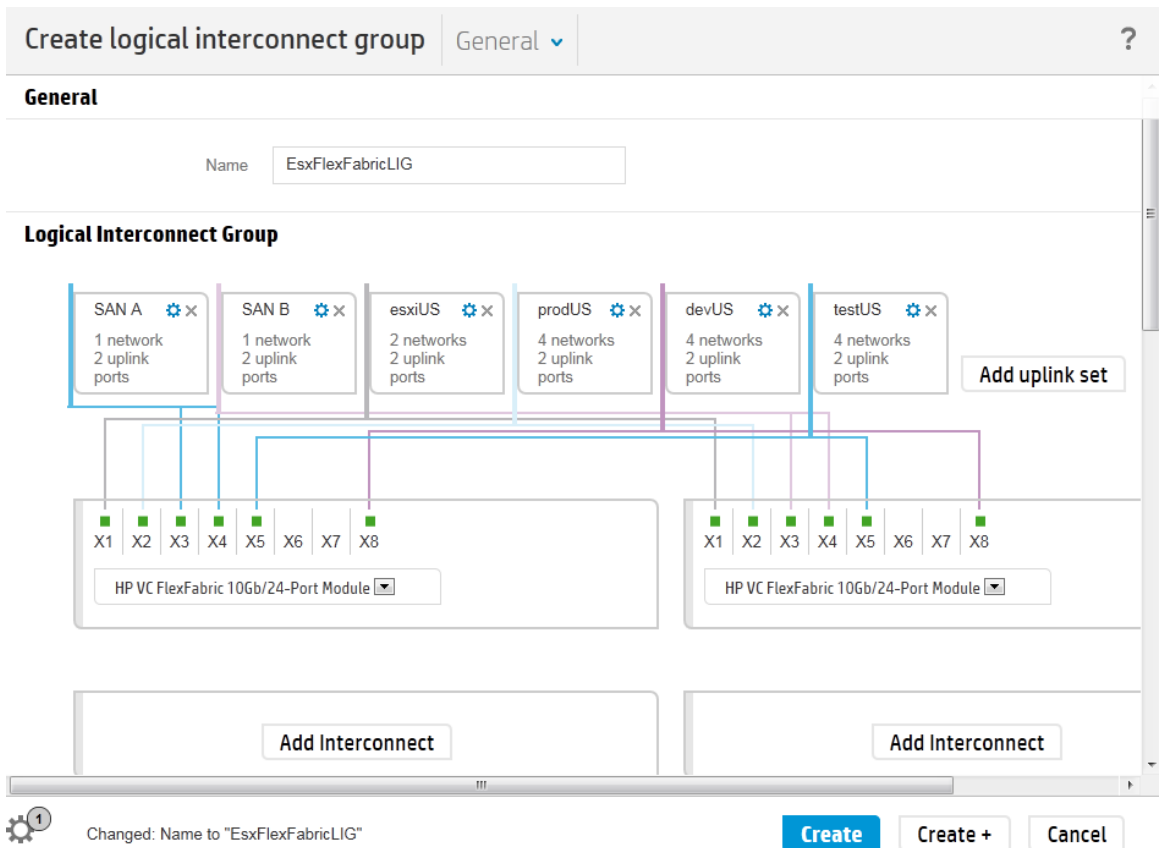


TIP: Select all networks listed by pressing and holding either **Shift** or **Ctrl** and then left-clicking the networks. Alternatively, select one of the networks and then use **Ctrl+A** to select all of the networks listed.

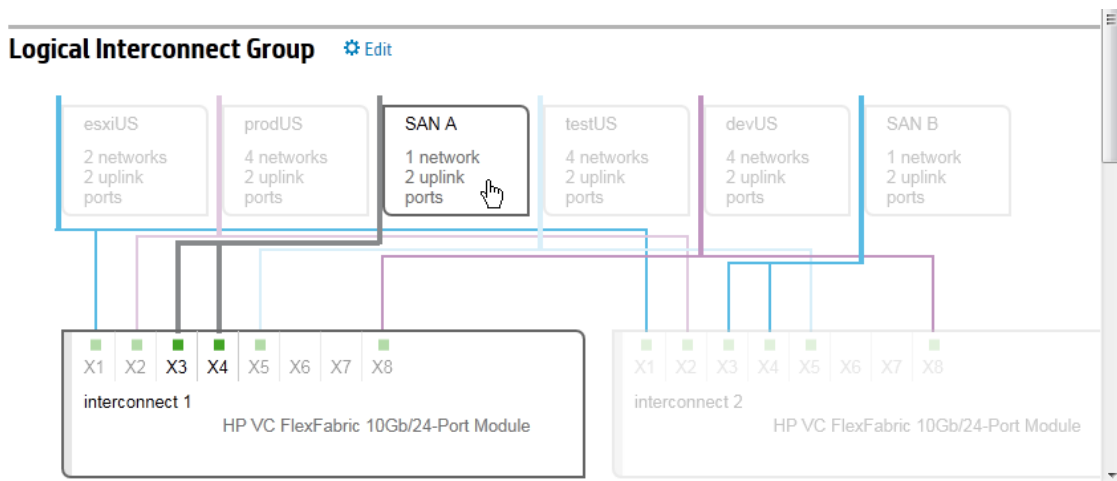
- iii. Click **Add**.
 - f. Add the uplink ports:
 - i. Click **Add uplink ports** to open the **Add Uplink Ports to esxUS** dialog box.
 - ii. In the search box, enter **x1** to display only the interconnects that have X1 ports available.
 - iii. Select the two interconnects displayed and click **Add**.
 - iv. Do not select a preferred port.
 - g. Click **Create +** to add the **esxUS** uplink set to the **EsxFlexFabricLIG** logical interconnect group and reopen the **Add uplink set** screen.
3. Add the uplink sets for the production networks, development networks, and test networks. As you add networks to uplink sets for the logical interconnect group, note that the networks that have already been added to an uplink set are not listed.

Networks	Uplink set	Interconnect port
production networks	prodUS	X2
development networks	devUS	X8
test networks	testUS	X5

When you finish entering the values for the last uplink set you want to create, click **Create** to add the uplink set and close the dialog box. The **Create logical interconnect group** screen opens (see the following illustration).



4. Click **Create** to create the logical interconnect group.
5. In the details pane of the **Logical Interconnect Groups** screen, you can use your pointing device to hover over an uplink set in the diagram to highlight the connections for that uplink set.



A.5.5 Creating an enclosure group for vSphere (ESXi) hosts

An enclosure group defines a set of enclosures that use the same configuration for network connectivity. The network connectivity for an enclosure group is defined by the logical interconnect group associated with the enclosure group.

Create an enclosure group that captures the logical interconnect group and its uplink configuration:

1. From the [main menu](#), select **Enclosure Groups**, and click **Create enclosure group**.
The **Create enclosure group** dialog box appears.
2. For **Name**, enter **EsxFlexFabricGroup**.

3. For **Logical interconnect group**, select **EsxFlexFabricLIG**.
4. Click **Create**.

A.5.6 Adding the enclosure

Adding an enclosure brings the rack, the enclosure, and the enclosure's contents—server hardware and interconnects—under managed control. You add an enclosure by providing its IP address or host name, along with the enclosure's Onboard Administrator credentials. In this procedure, you will also establish a firmware baseline for the enclosure.

NOTE: The name associated with the enclosure is the enclosure name, which is set in the Onboard Administrator, and is not the name of the Onboard Administrator.

In this procedure you will add one enclosure:

Attribute	Description
Enclosure 1 primary Onboard Administrator IP address	172.18.1.11
Enclosure 1 secondary Onboard Administrator IP address	172.18.1.12
Onboard Administrator credentials (same for both enclosures)	User name OAAAdmin Password S&leP@ssw0rd

1. From the [main menu](#), select **Enclosures** and click **Add enclosure**.
The **Add Enclosure** dialog box opens.
2. Enter the following information:
 - For **OA IP address or host name**, enter the primary Onboard Administrator IP address for Enclosure 1.
 - For **User name** and **Password**, enter the Onboard Administrator credentials in the preceding table. These credentials establish a trust relationship between the appliance and the Onboard Administrator.
 - For **Enclosure group**, select **EsxFlexFabricGroup**.
 - For **Licensing**, select **OneView** to apply both a OneView and a permanent iLO Advanced license to the servers in the enclosure. The appliance applies this licensing policy only to enclosures and servers that do not have factory-embedded licenses.
 - For **Firmware baseline**, select the firmware bundle that you added in [“Downloading the latest firmware bundle and adding it to the appliance”](#) (page 239).

When you add an enclosure, the appliance:

- Detects the server blades installed in the enclosure and adds them to the appliance. For each unique server blade hardware configuration, the appliance automatically adds a server hardware type.
- Detects and adds the interconnect modules installed in the enclosure. Because you selected an existing enclosure group, the appliance does the following:
 1. Compares the interconnect hardware configuration to the interconnect configuration specified by the logical interconnect group associated with the enclosure group.
 2. Notifies you if the two configurations do not match.

A.5.7 Viewing the server hardware types

After you add the enclosure, you can view the server hardware and server hardware types that the appliance added automatically.

Viewing server hardware types

From the [main menu](#), select **Server Hardware Types**.

The **Server Hardware Types** screen lists server hardware types for each unique server hardware configuration added to the appliance.

The default name assigned to each server hardware type starts with an abbreviated form of the server model name and ends with an enumerator. For example, BL460c Gen8 1 is an HP ProLiant BL460c server with a Flexible LOM and an HP FlexFabric 10Gb 2-port 554FLB Adapter. If you add an HP ProLiant BL460c server that has a different adapter, the default name for that server hardware type is:

BL460c Gen8 2

Editing server hardware types

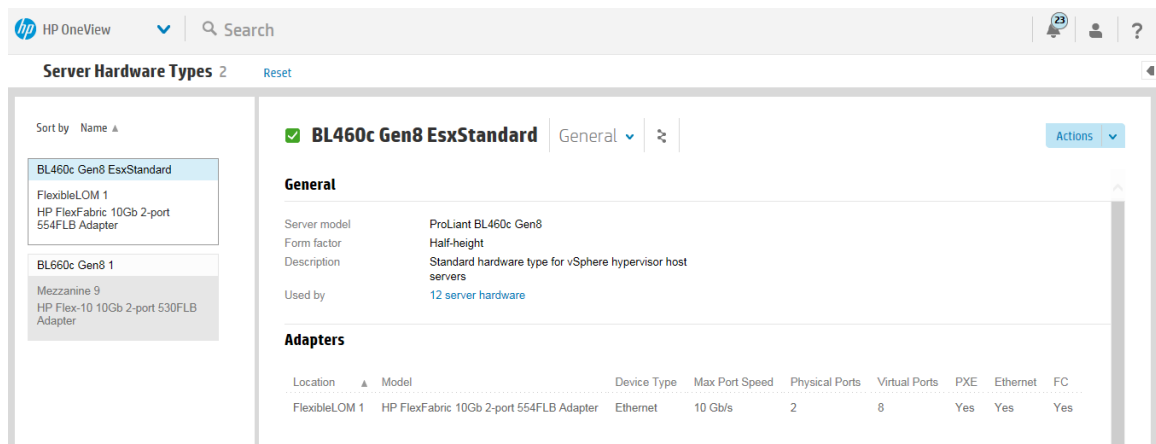
You can change the name of a server hardware type and add a description:

1. In the [master pane](#) of the **Server Hardware Types** screen, select the **BL460c Gen8 1** server hardware type.
2. Select **Actions**→**Edit**.

The **Edit BL460c Gen8 1** dialog box opens.

3. For **Name**, enter **BL460c Gen8 EsxStandard**.
4. For **Description**, enter **Standard hardware type for vSphere hypervisor host servers**.
5. Click **OK**.

The **Server Hardware Types** screen is updated with your changes.



View information about the server hardware

From the [main menu](#), select **Server Hardware**.

The [master pane](#) of the **Server Hardware** screen displays a list of all the servers in the appliance. The details pane displays detailed information about the selected server. The online help for the **Server Hardware** screen describes the information shown on the screen.

A.5.8 Creating a server profile to use as a template

Now that you have defined the server hardware types and the enclosure groups, you can start creating the server profile to use as a template for servers to be provisioned as hosts by VMware vSphere Auto Deploy.

1. From the [main menu](#), select **Server Profiles** and then click + **Create profile**. The **Create Server Profile** dialog box opens.

Create server profile | General ▾ ?

General

Name

Description

Server hardware 🔍

Server hardware type

Enclosure group

Firmware baseline ▾

Connections

To define network connections, you must first select server hardware or select unassigned server hardware and specify the server hardware type and enclosure group.

Boot Order

To define boot order, you must first select server hardware or select unassigned server hardware and specify the server hardware type and enclosure group.

BIOS

To define BIOS settings, you must first select server hardware or select unassigned server hardware and specify the server hardware type and enclosure group.

Advanced

To define advanced settings, you must first select server hardware or select unassigned server hardware and specify the server hardware type and enclosure group.

Create **Create +** **Cancel**

2. Under **General**, enter the following information:
 - For **Name**, enter **ESX TEMPLATE**.
 - For **Description**, enter **Standard server profile for stateless autodeploy**.
 - For **Server hardware**, select **unassigned**.
 - For **Server hardware type**, select **BL460c Gen8 EsxStandard**.
 - For **Enclosure group**, select **EsxFlexFabricGroup**.
 - For **Firmware baseline**, you can select **manage manually** or one of the other firmware bundles in the repository. For this example, select **manage manually**. You will change the firmware baseline when you copy the profile in [“Copying the template server profile to eight servers”](#) (page 255).
3. Add the connections for this server profile. Click **Add Connection** to open the **Add Connection** dialog box:

- a. Add two connections to the `esxi mgmt 1131` network. When you finish entering the information for a connection, click **Add +** to add this connection and reopen the dialog box so that you can add the connections in the next step.

Attribute	Value
Device type	Ethernet
Network	esxi mgmt 1131
Requested bandwidth	2.5 (the default value)
FlexNIC	Auto (the default value)
Boot	For the first connection, select Primary . For the second connection, select Secondary .

- b. Add two connections to the `esxi vmotion 1132` network. Because the configuration is the same for both connections, you can enter the information, and then click **Add +** twice to add both connections and reopen the dialog box for the next step.

Attribute	Value
Device type	Ethernet
Network	esxi vmotion 1132
Requested bandwidth	2.5 (the default value)
FlexNIC	Auto (the default value)
Boot	For both connections, select Not bootable

- c. Add two connections to the `esxi vmotion 1132` network. Because the configuration is the same for both connections, you can enter the information, and then click **Add +** twice to add both connections and reopen the dialog box for the next step.

Attribute	Value
Device type	Ethernet
Network	esxi vmotion 1132
Requested bandwidth	2.5 (the default value)
FlexNIC	Auto (the default value)
Boot	For both connections, select Not bootable

- d. Add two connections to the `prod networks` network set. Because the configuration is the same for both connections, you can enter the information, and then click **Add +** twice to add both connections and reopen the dialog box for the next step.

Attribute	Value
Device type	Ethernet
Network	prod networks
Requested bandwidth	2.5 (the default value)
FlexNIC	Auto (the default value)
Boot	For both connections, select Not bootable

- e. Add one connection to the SAN A network. Enter the information shown in the following table, and then click **Add +** to add the connection and reopen the dialog box for the next step.

Attribute	Value
Device type	Fibre Channel
Network	SAN A
Requested bandwidth	2.5 (the default value)
FlexNIC	Auto (the default value)
Boot	Not bootable

- f. Add one connection to the SAN B network. Enter the information shown in the following table, and then click **Add** to add the connection and close the dialog box.

Attribute	Value
Device type	Fibre Channel
Network	SAN B
Requested bandwidth	2.5 (the default value)
FlexNIC	Auto (the default value)
Boot	Not bootable

The following illustration shows the **Create Server Profile** dialog box with all the connections added.

Create server profile

General

?

General

Name

ESX TEMPLATE

Description

Standard server profile for stateless autodeploy

Server hardware

unassigned

✕

🔍

Server hardware type

BL460c Gen8 EsxStandards

✕

🔍

Enclosure group

EsxFlexFabricGroup

✕

🔍

Firmware baseline

managed manually

▼

Connections

ID	Type	Network	Network IDs	Requested bandwidth (Gb/s)	Port	Boot		
1	Ethernet	esxi mgmt 1131	Auto	2.5	Auto	Primary	⚙️	✕
2	Ethernet	esxi mgmt 1131	Auto	2.5	Auto	Secondary	⚙️	✕
3	Ethernet	esxi vmotion 1132	Auto	2.5	Auto	Not bootable	⚙️	✕
4	Ethernet	esxi vmotion 1132	Auto	2.5	Auto	Not bootable	⚙️	✕
5	Ethernet	prod networks	Auto	2.5	Auto	Not bootable	⚙️	✕
6	Ethernet	prod networks	Auto	2.5	Auto	Not bootable	⚙️	✕
9	Fibre Channel	SAN A	Auto	2.5	Auto	Not bootable	⚙️	✕
11	Fibre Channel	SAN B	Auto	2.5	Auto	Not bootable	⚙️	✕

Add Connection

⚙️ 11

Add Connection: SAN B

Create

Create +

Cancel

4. Scroll down to see other items in the dialog box.
5. Configure the boot order for this server profile. **Manage boot order** is selected by default. Drag and drop the items so that they are in this order:

1. PXE
2. HardDisk
3. CD
4. Floppy
5. USB

Notice that the number next to each item is adjusted automatically when you use the drag-and-drop method to change the order.

6. Edit the BIOS settings:
 - a. Select **Manage BIOS**.
 - b. Click **Edit BIOS Settings**.
The **Edit BIOS Settings** dialog box opens. The server hardware type that you selected for this profile determines the default values for the BIOS settings.
 - c. Scroll to **Administrator Info Text** and make the following edits:
 - For **Admin Name**, enter the name of the server administrator responsible for all servers that will use this server profile (for example **Sanjay Bharata**).
 - For **Other Text**, enter **See company directory**.

- d. Click **OK** to save the edits and close the dialog box.
The **Create Server Profile** dialog box displays the BIOS settings whose values differ from the default values.
7. Under **Advanced**, ensure that **Virtual** is selected for **Serial Number/UUID**, **MAC addresses**, and **WWN addresses**.
Selecting **Virtual** for these settings provides flexibility because the appliance assigns these numbers and addresses. For example, when you assign this server profile to a server bay in an enclosure, any server hardware inserted in that server bay uses the same serial number, MAC address, and WWN address. Therefore, you can replace the server hardware without affecting other resources (such as interconnects).
8. Click **Create** to create the server profile and close the dialog box.
The **master pane** of the **Server Profiles** screen lists the profile you created. If you select a server profile in the master pane, the appliance displays information about that server profile in the details pane.

A.5.9 Copying the template server profile to eight servers

In this procedure, you will copy the server profile you created to use as a template and assign the profile to eight servers.

1. In the **master pane** of the **Server Profiles** screen, select **ESX TEMPLATE**.
2. Copy the **ESX TEMPLATE** server profile and assign the profile to a specific instance of server hardware:
 - a. Select **Actions**→**Copy**.
The **Copy ESX TEMPLATE** dialog box opens. All of the configuration information for this profile, except for **Name**, is obtained from the profile you are copying.
 - b. For **Name**, enter **ESX01**.
 - c. For **Server hardware**, select **Search for another**, and then select **Encl1, bay 11**.
 - d. For **Firmware baseline**, select the firmware bundle that was included with the appliance.
 - e. Click **Create**.
The appliance validates the parameters and the server hardware is booted using the HP Intelligent Provisioning environment embedded in the iLO management processor of HP ProLiant Gen8 servers.
3. Copy the **ESX TEMPLATE** server profile and assign it to the other seven servers:

Name	Server hardware
esx02	Encl1, bay 12
esx03	Encl1, bay 13
esx04	Encl1, bay 14
esx05	Encl1, bay 15
esx06	Encl1, bay 16
esx07	Encl1, bay 3
esx08	Encl1, bay 4

4. (Optional) View the progress of the create profile action from the **Server Profiles** screen. Optionally, launch the iLO remote console to view the progress of the boot and firmware load operations for the server:
 - a. From the [main menu](#), select **Server Hardware**.
 - b. In the [master pane](#), select an instance of server hardware.
 - c. Select **Actions**→**Launch console**.The appliance launches the remote console for the selected server.

A.6 Configuring a server blade to boot from the attached HP 3PAR Storage System

This example demonstrates configuring a server blade to boot from SAN from an HP 3PAR Storage System that is directly attached to the enclosure that contains the server blade.

Assumptions

- The appliance is installed.
- You have created the production networks and network set as described in [“Provisioning eight host servers for VMware vSphere Auto Deploy” \(page 238\)](#).
- The enclosure you will add, Enclosure 2, has embedded licenses.
- The HP 3PAR Storage System is installed and configured, and the cables are attached to the enclosure you want to use.

A.6.1 Workflow

1. [“Creating the Flat SAN networks” \(page 256\)](#).
2. [“Adding the enclosure that is connected to the HP 3PAR Storage System” \(page 257\)](#). During this procedure, you will create the enclosure group and logical interconnect group during the add enclosure operation.
3. [“Creating the server profile” \(page 260\)](#).
4. [“Collecting the WWPNs to use when configuring the HP 3PAR Storage System” \(page 263\)](#).

A.6.2 Creating the Flat SAN networks

The sample data center has an HP 3PAR Storage System and an enclosure that are connected directly together instead of through the data center SAN switches. This configuration is called a Flat SAN or Direct attach network configuration. To see a graphical representation of the configuration, see [Figure 17 \(page 235\)](#).

When you create the Flat SAN networks, you do not need to know what physical connections are used or which enclosure is connected to the storage system. The physical connections are specified in the uplink set, which you will add later. For this procedure, you must supply the names of the networks, and decide if you want to change the default values the appliance provides for configuration attributes like preferred bandwidth, maximum bandwidth, and uplink speed.

To create the Flat SAN networks:

1. From the [main menu](#), select **Networks**.
2. Click **Create Network**.
3. For **Name**, enter **FlatSAN A**.
4. For **Type**, select **Fibre Channel**.
5. For **Fabric type**, select **Direct attach**.
6. For this data center, use the default values for the other configuration attributes.
7. Click **Create +**.

The appliance creates the network and opens the **Create network** dialog box. This dialog box uses the configuration values you selected in the preceding steps, except for the name.

8. In **Name**, enter **FlatSAN B** and click **Create**.

The **Networks** screen opens.

After the networks are added, when you select a network in the **master pane**, you can see the details about that network in the details pane. For each of the networks you created:

- The value for **Uplink Set** is **none** because you have not yet defined a logical interconnect and uplink set that uses this network.
- The value for **Used by** is **none** because there are no server profiles using this network. You will define a server profile in “[Creating the server profile](#)” (page 260).

A.6.3 Adding the enclosure that is connected to the HP 3PAR Storage System

Adding an enclosure brings the rack, the enclosure, and the enclosure's contents under managed control. You add an enclosure by providing its IP address or host name, along with the enclosure's Onboard Administrator credentials.

NOTE: The name associated with the enclosure is the enclosure name, which is set in the Onboard Administrator, and is not the name of the Onboard Administrator.

In this procedure, you add the enclosure before you define the enclosure group and the logical interconnect group. By adding the enclosure first, you can use the enclosure group and logical interconnect group that the appliance creates based on the enclosure interconnect hardware it detects in the enclosure.

In this procedure, you will add Enclosure 2 of the sample data center.

Attribute	Description
Enclosure 2 primary Onboard Administrator IP address	172.18.1.13
Enclosure 2 secondary Onboard Administrator IP address	172.18.1.14
Onboard Administrator credentials (same for both enclosures)	User name OAdmin Password S&leP@ssw0rd

1. From the **main menu**, select **Enclosures**, and then click **Add enclosure**.

The **Add Enclosure** dialog box opens.

2. Enter the following information:

- For **OA IP address or host name**, enter the primary Onboard Administrator IP address for Enclosure 2.
- For **User name** and **Password**, enter the Onboard Administrator credentials in the preceding table. These credentials establish a trust relationship between the appliance and the Onboard Administrator.
- For **Enclosure group**, select **Create new enclosure group**.
- For **Enclosure group name**, enter **DirectAttachGroup**.
- For **Logical interconnect group**, select **Create new logical interconnect group**.
- For **Licensing**, select **OneView** to apply both a OneView and a permanent iLO Advanced license to the servers in the enclosure. The appliance applies this licensing policy only to enclosures and servers that do not have factory-embedded licenses.
- For **Firmware baseline**, select **manage manually**.

3. Click **Add** to add the enclosure.

The appliance discovers the interconnects in the enclosure, creates a logical interconnect group, and opens the **Edit DirectAttachGroup logical interconnect group** screen (see the following illustration).

4. Add the uplink sets for the Flat SAN networks:
 - a. Click **Add uplink set**.
The **Add uplink set** screen opens.
 - b. Configure the uplink set for the FlatSAN A Fibre Channel network.
 - For **Name**, enter **FlatSAN A**.
 - For **Type**, select **Fibre Channel**.
When you select **Fibre Channel**, the screen expands to include additional configuration items.
 - For **Network**, select **FlatSAN A**.
 - c. Configure the uplink ports:
 - i. For **Interconnect** under **Uplink Ports**, select **Interconnect: 1**.
The ports that can be used for Fibre Channel networks are displayed.
 - ii. Select ports **X3** and **X4**.
 - d. Click **Create +** to add the FlatSAN A uplink set to the logical interconnect group and reopen the **Add uplink set** screen.
5. Add the uplink set for the FlatSAN B Fibre Channel network:
 - a. For **Name**, enter **FlatSAN B**.
 - b. For **Type**, select **Fibre Channel**.

- c. For **Network**, select **FlatSAN B**.
 - d. Configure the uplink ports. For **Interconnect** under **Uplink Ports**, select **Interconnect : 2** and then select ports **X3** and **X4**.
 - e. Click **Create +** to add the **FlatSAN B** uplink set to the logical interconnect group and reopen the **Add uplink set** screen.
6. Add the uplink set for the Ethernet production networks:
- a. For **Name**, enter **prodUS**.
 - b. For **Type**, select **Ethernet**.
The dialog box expands to include additional configuration items.
 - c. For **Connection Mode**, select **automatic**.
The default value, **automatic**, instructs the system to determine the best load-balancing scheme by creating as many LAGs (link aggregation groups) as possible in a physical interconnect, enabling multiple links to behave as a single link.
 - d. Click **Add networks** to open the **Add Networks to prodUS** dialog box.
 - e. Add the production networks:
 - i. In the search box, enter **prod** to display only the production networks.
 - ii. Select all of the production networks listed.



TIP: Select all networks listed by pressing and holding either **Shift** or **Ctrl** and then left-clicking the networks. Alternatively, select one of the networks and then use **Ctrl+A** to select all of the networks listed.

- iii. Click **Add**.
- f. Add the uplink ports:
- i. Click **Add uplink ports** to open the **Add Uplink Ports to prodUS** dialog box.
 - ii. In the search box, enter **x5** to display only the interconnects that have X5 ports available.
 - iii. Select the two interconnects displayed and click **Add**.
 - iv. Do not select a preferred port.
- g. Click **Create** to add the **prodUS** uplink set.

The logical interconnect group now includes three uplink sets, as shown in the following illustration:

Add Enclosure
Edit DirectAttachGroup logical interconnect group

A logical interconnect group is required in order to be able to add an enclosure.

This group has been pre-populated with the supported interconnects found in the enclosure. You should create uplink sets to enable connectivity to external networks via the interconnects. You only need to do this once and can re-use this group for other similarly configured enclosures.

FlatSAN A
1 network
2 uplink ports

FlatSAN B
1 network
2 uplink ports

prodUS
4 networks
2 uplink ports

Add uplink set

X1
X2
X3
X4
X5
X6
X7
X8

interconnect 1

HP VC FlexFabric 10Gb/24-Port Module

X1
X2
X3
X4
X5
X6
X7
X8

interconnect 2

HP VC FlexFabric 10Gb/24-Port Module

Add Interconnect

Add Interconnect

Add Interconnect

Add Interconnect

OK and add enclosure

Cancel

- Click **OK and add enclosure**.

The appliance adds the enclosure, the enclosure group, the logical interconnect group, and the uplink sets:

Enclosure name	Encl2
Enclosure group name	DirectAttachGroup
Logical interconnect group name	DirectAttachGroup interconnect group

A.6.4 Creating the server profile

- From the [main menu](#), select **Server Profiles** and then click **+ Create profile**. The **Create Server Profile** screen opens.
- Enter the general information:
 - For **Name**, enter **win2k12 boot from 3PAR**.
 - For **Description**, enter **Windows 2012 boot from 3PAR direct attach**.
 - For **Server hardware**, select **Encl2, bay 12**.

- For **Server hardware type**, select **BL460c Gen8 Standard**.
 - For **Enclosure Group**, select **DirectAttachGroup**.
 - For **Firmware Baseline**, select **Manage manually**.
3. Click **Add Connection** to open the **Add Connection** dialog box.
 4. Add two connections to the `prod networks` network set. Because the configuration is the same for both network sets, you can enter the information, and then click **Add +** twice to add both connections and reopen the dialog box for the next step.

Attribute	Value
Device type	Ethernet
Network	prod networks
Requested bandwidth	2.5 (the default value)
FlexNIC	Auto (the default value)
Boot	For both connections, select Not bootable .

Add Connection

Device type

Ethernet

Network

prod 1101

vlan 1101

Requested bandwidth (Gb/s)

prod 1102

vlan 1102

Port

prod 1103

vlan 1103

Boot

prod 1104

vlan 1104

prod networks (network set)

test 1111

vlan 1111

test 1112

vlan 1112

Add

Add +

Cancel

5. Add one connection to the `FlatSAN A` network. Enter the information shown in the following table, and then click **Add +** to add the connection and reopen the dialog box for the next step.

Device type	Fibre Channel
Network	FlatSAN A
Requested bandwidth	2.5 (the default value)
FlexNIC	Auto (the default value)
Boot	Not bootable

6. Add one connection to the FlatSAN B network. Enter the information shown in the following table, and then click **Add** to add the connection and close the dialog box.

Attribute	Value
Device type	Fibre Channel
Network	FlatSAN B
Requested bandwidth	2.5 (the default value)
FlexNIC	Auto (the default value)
Boot	Not bootable

The following illustration shows the **Connections** panel for the server profile after you add the connections.

✓ win2k12 boot from 3PAR
Connections ▾
⌵
Actions ▾

Create Completed 9m13s
Administrator Sep 16 7:24 pm ▾

Connections

ID	Type	Address	Network	Allocated bandwidth (Gb/s)	Interconnect	Port	Boot
1	Ethernet	MAC (v)	prod networks (network set)	2.5	Encl2, interconnect 1	FlexibleLOM 1:1-a	Not bootable
2	Ethernet	MAC (v)	prod networks (network set)	2.5	Encl2, interconnect 2	FlexibleLOM 1:2-a	Not bootable
3	Fibre Channel	WWPN (v) WWNN (v) MAC (v)	FlatSAN A	2.5	Encl2, interconnect 1	FlexibleLOM 1:1-b	Not bootable
4	Fibre Channel	WWPN (v) WWNN (v) MAC (v)	FlatSAN B	2.5	Encl2, interconnect 2	FlexibleLOM 1:2-b	Not bootable

7. Scroll down to display the lower half of the **Create server profile** dialog box.
8. Configure the boot order for this server profile. Ensure that **Manage boot order** is selected. Drag and drop the items so that they are in this order:
 1. CD
 2. HardDisk
 3. Floppy
 4. USB
 5. PXE

Notice that the number next to each item is adjusted automatically when you use the drag-and-drop method to change the order.

9. Edit the BIOS settings. For example:
 - a. Select **Manage BIOS**.

- b. Click **Edit BIOS Settings**.

The **Edit BIOS Settings** dialog box opens. The server hardware type that you selected for this profile determines the default values for the BIOS settings.

- c. Scroll to **Power Management Options** and for **HP Power Profile**, select **Maximum Performance**.

Changing this setting results automatic changes to several other BIOS settings.

- d. Click **OK** to save the edits and close the dialog box.

The **Create Server Profile** dialog box displays the BIOS settings whose values differ from the default values.

BIOS

☒ Manage BIOS

Modified Settings

HP Power Profile	Maximum Performance
HP Power Regulator	HP Static High Performance Mode
Intel QPI Link Power Management	Disabled
Minimum Processor Idle Power Core State	No C-states
Minimum Processor Idle Power Package State	No Package State
Energy/Performance Bias	Maximum Performance
DIMM Voltage Preference	Optimized for Performance

Edit BIOS settings

Advanced

MAC addresses ☒ Virtual ☐ Physical

WWN addresses ☒ Virtual ☐ Physical

Checked: Manage BIOS

Create Create + Cancel

10. Under **Advanced**, ensure that **Virtual** is selected for **Serial Number/UUID**, **MAC addresses**, and **WWN addresses**.

Selecting **Virtual** for these settings provides flexibility because the appliance assigns these numbers and addresses. For example, when you assign this server profile to a server bay in an enclosure, any server hardware inserted in that server bay uses the same serial number, MAC address, and WWN address. Therefore, you can replace the server hardware without affecting other resources (such as interconnects).

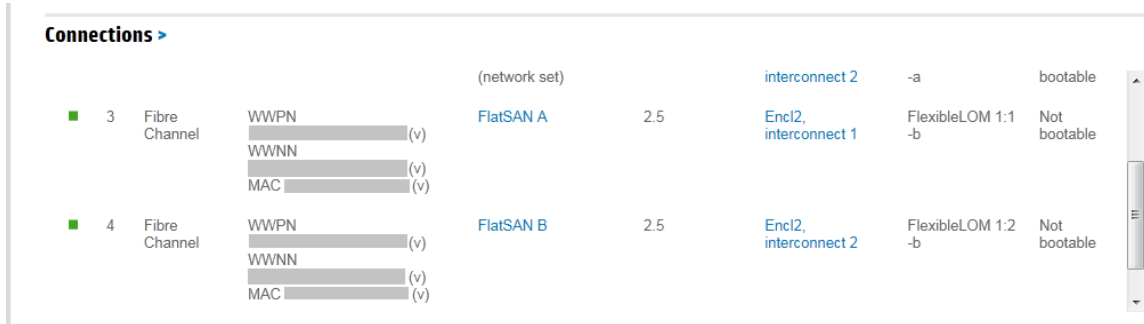
11. Click **Create** to create the server profile and close the dialog box.

The **master pane** of the **Server Profiles** screen lists the profile you created. If you select a server profile in the master pane, the appliance displays information about that server profile in the details pane.

A.6.5 Collecting the WWPNs to use when configuring the HP 3PAR Storage System

When you configure the HP 3PAR Storage System, you use the WWPNs for each of the Direct attach Fibre Channel connection. To collect the WWPNs:

1. In the [master pane](#) of the **Server Profiles** screen, select **win2k12 boot from 3PAR**.
The appliance displays the details about the server profile in the details pane.
2. In the **Connections** panel, scroll so that the two Fibre Channel connections are visible.
3. Record the WWPN information for **FlatSAN A** and **FlatSAN B**.



A.7 Bringing an HP ProLiant DL360p Gen8 rack mount server under management

This example demonstrates bringing the following HP ProLiant DL360p Gen8 rack mount server under management.

Attribute	Description
Model	HP ProLiant DL360p Gen8
Name	DL360pGen8-1796
iLO IP address	172.18.6.15
iLO administrator credential:	User name iLOAdmin Password S&leP@ssw0rd
Physical location	Rack 173, U26

Assumptions

- The appliance is installed.
- The iLO management processor for the server is configured with the IP address and administrator credentials listed in the preceding table.
- The server is connected to a live power source.
- You do not have an embedded license for this server, but all of the other servers managed by the appliance have licenses.

Because this is an HP ProLiant DL rack mount server:

- You cannot use this appliance to provision any networks for the server.
- You cannot assign a server profile to the server.

A.7.1 Workflow

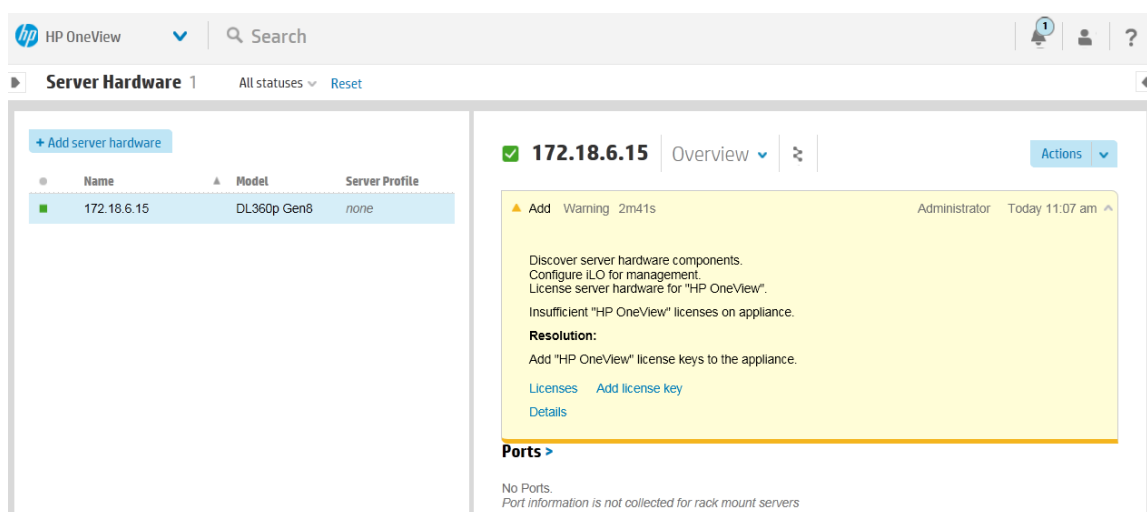
1. "Adding the server hardware" (page 265).
2. "Powering on the server" (page 265).
3. "Viewing information about the server" (page 265).
4. "Adding a license for the server" (page 267).

A.7.2 Adding the server hardware

1. From the [main menu](#), select **Server Hardware**, and then click + **Add server hardware**.
2. Enter the following information:
 - For **iLO IP address**, enter 172.18.6.15.
 - Enter the credentials for the iLO administrator account: User name iLOAdmin and password S&leP@ssw0rd.
 - For **Licensing**, select the default, **OneView**. By selecting **OneView**, you specify that, if this server does not have an embedded license, the appliance applies the **OneView** license, which licenses both HP OneView and the iLO for that server.
3. Click **Add**.

The server is added to the appliance. In this case, the server does not have an embedded license, so the appliance adds the server, but displays an alert.
4. Click the alert to display details.

For information about adding a license, see [“Adding a license for the server”](#) (page 267).



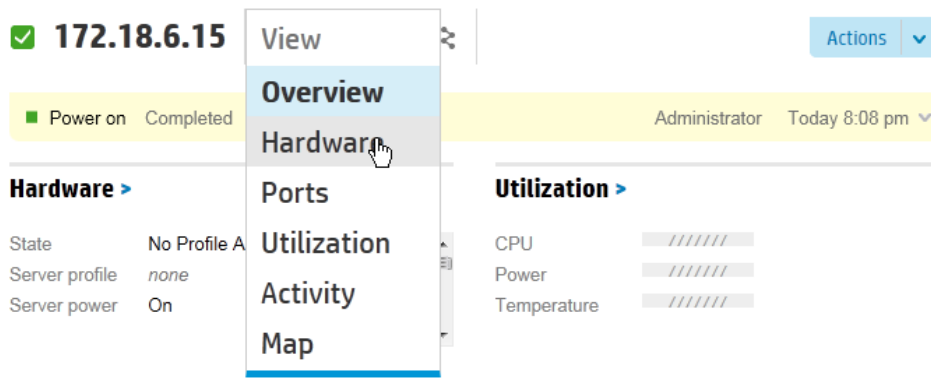
A.7.3 Powering on the server

1. From the **Server Hardware** screen, select the server you added 172.18.6.15.
2. Select **Actions**→**Power on**.

A.7.4 Viewing information about the server

1. On the **Server Hardware** screen, select the server you added 172.18.6.15.

The details pane displays information about the server.
2. To display only the **Hardware**, either click the **Hardware** panel or use the view selector to select **Hardware**.



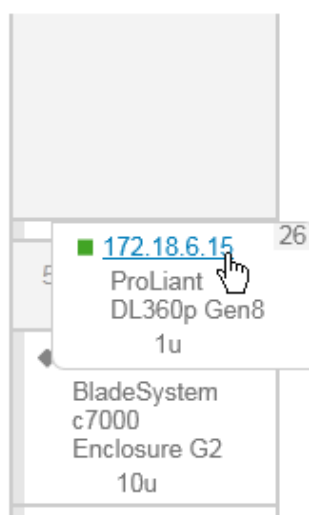
NOTE: To view utilization data or connect to the remote console, the server must have the appropriate licenses. See [“Adding a license for the server”](#) (page 267).

3. Explore the links to additional information.

Some items in the **Hardware** panel are links. The cursor changes when you use your pointing device to hover over a link. In this example:

- If you click the IP address shown for **iLO** under **Host name** or **IPv4**, you launch the iLO remote console for the server.
- If you click the value for **Server hardware type**, **DL360p Gen8 1**, the appliance displays the **Server Hardware Types** screen with details about the DL360p Gen8 1 server hardware type in the details pane.
- If you click the value for **Location**, **Rack-173**, the appliance displays the **Racks** screen with details about Rack-173 in the details pane. To return to the **Server Hardware** screen, click the link for the server **172.18.6.15** in the **Layout** panel.

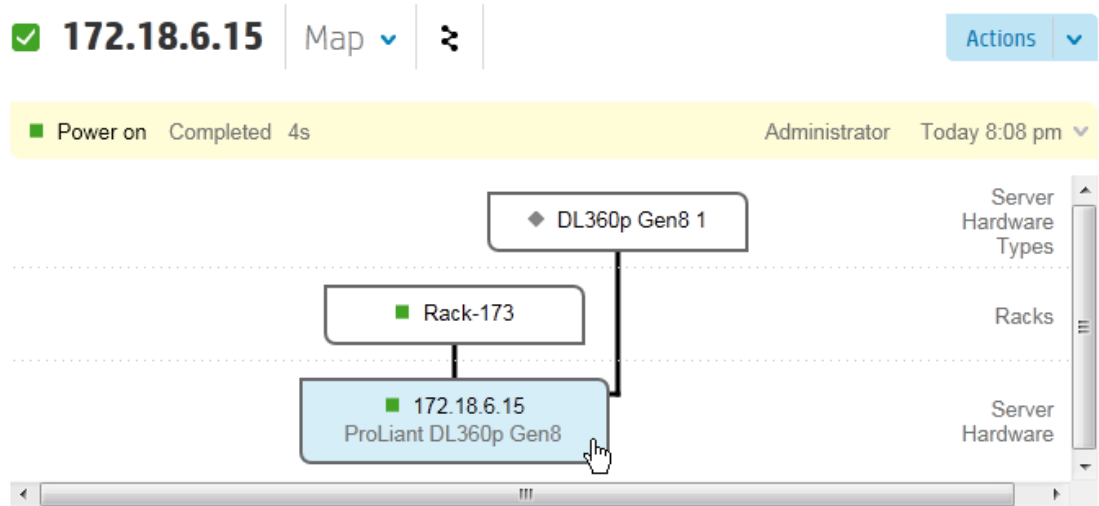
Layout > **Edit**



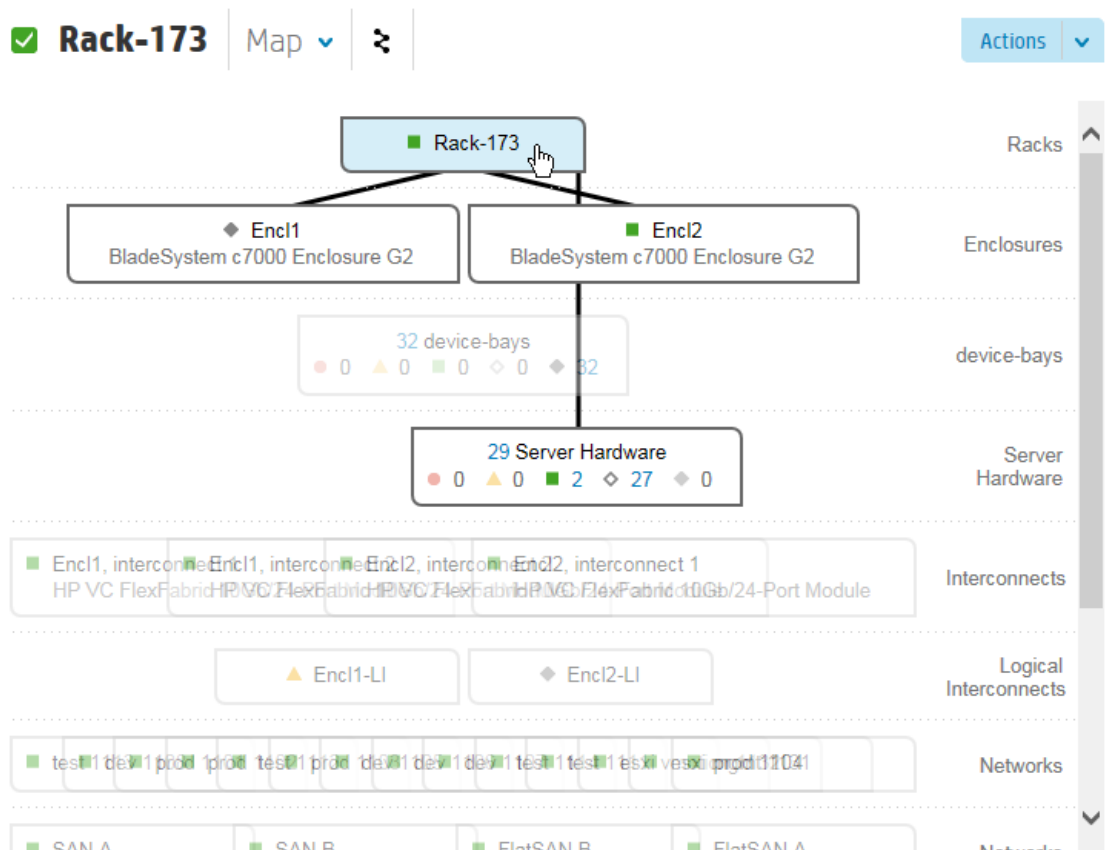
4. In the view selector, select **Map**.

The **Map** view shows the relationships between this resource and other resources. Use your pointing device to hover over any resource to see its direct relationships to other resources. A connecting line between boxes indicates a direct relationship.

In this example, the server is related to Rack-173 and the DL360p Gen 8 1 server hardware type.



- Click **Rack-173** to display the **Map** view for the rack.



- To return to the **Server Hardware** screen, click the **Server Hardware** box.

A.7.5 Adding a license for the server

If you do not purchase licenses that are embedded in the enclosure or server hardware, you must add licenses to the appliance. The online help provides detailed information about licensing and how the appliance manages licenses.

To add an HP OneView license for the server you added in [“Adding the server hardware”](#) (page 265):

1. Do one of the following:
 - From the warning message for the server you just added, click the **Add license key** link.
 - From the [main menu](#), select **Settings**, and then select **Actions**→**Add license**.

The **Add license** dialog box opens.

2. Enter or paste your license key into the **License Key** box, and then click **Add**.

The appliance adds the license to the license pool.

3. On the **Server Hardware** screen, select **172.18.6.15**.

4. Select **Actions**→**Refresh**.

The **Server Hardware** screen displays the utilization data for the server.

B Using the virtual appliance console

B.1 Using the virtual appliance console

The virtual appliance console has a restricted browser interface that supports the following:

- Appliance networking configuration in non-DHCP environments
- Password reset requests for the Administrator account
- Advanced diagnostics for authorized support representatives

Use the virtual appliance console to access the appliance and configure the appliance network for the first time. The virtual appliance console enables you to bootstrap an appliance onto the network in non-DHCP environments. The virtual appliance console is not intended to be a full-featured replacement for your browser.

The virtual appliance console starts a browser session; The browser takes up the full screen; you cannot add tabs. You cannot perform any operation that requires you to select a file from a dialog box, including uploading software updates and firmware bundles (SPPs). Only basic browsing, including forward and backward navigation, are enabled.

Table 18 Key combinations for the virtual appliance console

Key combination	Function
Alt-← (Alt and left arrow)	Browse backward
Alt-→ (Alt and right arrow)	Browse forward
Ctrl++ (Ctrl and plus sign)	Zoom in
Ctrl-- (Ctrl and hyphen)	Zoom out
Ctrl-0 (Ctrl and zero)	Reset zoom
Ctrl-F	Search
Ctrl-R or F5	Reload/Refresh
Ctrl-Alt-Backspace	Restart the browser interface

C Backup and restore script examples

C.1 Sample backup script

As an alternative to using **Settings**→**Actions**→**Create backup** from the appliance UI, you can write and run a script to automatically create and download an appliance backup file.

Example 8 “Sample backup.ps1 script” provides a sample PowerShell script that uses REST calls to create and download an appliance backup file. Cut and paste this sample script into a file on a Windows system that runs PowerShell version 3.0, and edit the script to customize it for your environment.

You can schedule the backup script to run automatically in interactive or batch mode on a regular basis (HP recommends daily backups). Only a user with Backup administrator or Infrastructure administrator privileges can run the script interactively.

- To run the script interactively, do not include any parameters. The script prompts you to enter the appliance host name, appliance user name and password, and the name of a file to store these parameters for batch mode executions. Enter the name and password of a user with the Backup administrator or Infrastructure administrator role. The user name and password are stored encrypted.

HP recommends that you run the script interactively the first time. Then, you can schedule the script to run automatically in the background using the parameter file created by the first run.

- To run the script in batch mode, specify the name of the file containing the parameters on the command line.

HP recommends that you install cURL with the SSL option to improve performance. The sample script works without cURL, but it might take several hours to download a large backup file. To download cURL, see:

<http://curl.haxx.se/download.html>

NOTE: You might also need to install Microsoft Visual C++ Redistributable, the `MSVCR100.dll` file, available here:

- 64 bit: <http://www.microsoft.com/download/en/details.aspx?id=14632>
- 32 bit: <http://www.microsoft.com/download/en/details.aspx?id=5555>

Make sure the path environment variable includes the path for cURL.

Sample script

The **sample script** makes the following calls to create and download a backup file:

1. Calls `queryfor-credentials()` to get the appliance host name, user name, and password by either prompting the user or reading the values from a file.
2. Calls `login-appliance()` to issue a REST request to obtain a session ID used to authorize backup REST calls.
3. Calls `backup-appliance()` to issue a REST request to start a backup.
4. Calls `waitFor-completion()` to issue REST requests to poll for backup status until the backup completes.
5. Calls `get-backupResource()` to issue a REST request to get the download URI.
6. Calls `download-backup()` to issue a REST request to download the backup.

Example 8 Sample backup.ps1 script

```
# (C) Copyright 2013 Hewlett-Packard Development Company, L.P.
#####
# Name:      backup.ps1
# Usage:     {directory}\backup.ps1 or {directory}\backup.ps1 filepath
# Parameter: $filepath: optional, uses the file in that path as the login credentials. ie: host address,
#            username, password
# Purpose:   Runs the backup function on the appliance and downloads it onto your machine's drive
#            in current user's home directory
# Notes:     To improve performance, this script uses the curl command if it is installed. The curl command
#            must be installed with the SSL option.
#            Windows PowerShell 3.0 must be installed to run the script
#####

#Notifies the computer that this is a trusted source that we are connecting to (brute force, could be refined)
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = { $true }

$global:interactiveMode = 0

# The scriptApiVersion is the default Api version (if the appliance supports this level
# or higher). This variable may be changed if the appliance is at a lower Api level.
$global:scriptApiVersion = 3
# Using this Api version or greater requires a different interaction when creating a backup.
Set-Variable taskResourceV2ApiVersion -option Constant -value 3

try {
    #this log must be added if not already on your computer
    New-EventLog -LogName Application -Source backup.ps1 -ErrorAction stop
}
catch [System.Exception]
{
    #this is just to keep the error "already a script" from showing up on the screen if it is already created
}

##### Querying user for login info #####
function queryfor-credentials ()
{
    <#
        .DESCRIPTION
            Gathers information from User if in manual entry mode (script ran with zero arguments) or
            runs silently and gathers info from specified path (script ran with 1 argument)

        .INPUTS
            None, this function does not take inputs.

        .OUTPUTS
            Returns an object that contains the login name, password, and host name to connect to.

        .EXAMPLE
            $variable = queryfor-credentials #runs function, saves json object to variable.
    #>

    if ($args[0] -eq $null)
    {
        Write-Host "Enter Appliance name (https://ipaddress)"
        $appliance = Read-Host
        # Correct some common errors
        $appliance = $appliance.Trim().ToLower()
        if (!$appliance.StartsWith("https://"))
        {
            if ($appliance.StartsWith("http://"))
            {
                $appliance = $appliance.Replace("http","https")
            } else {
                $appliance = "https://" + $appliance
            }
        }

        Write-Host "Enter user name"
        $username = Read-Host -AsSecureString | ConvertFrom-SecureString

        Write-Host "Enter password"
        $SecurePassword = Read-Host -AsSecureString | ConvertFrom-SecureString

        Write-Host "Would you like to save these credentials to a file? (username and password encrypted)"
        $saveQuery = Read-Host

        $loginVals = [pscustomobject]@{ userName = $username; password = $SecurePassword; hostname = $appliance }
        $loginJson = $loginVals | convertTo-json

        $global:interactiveMode = 1

        if ($saveQuery[0] -eq "y") #enters into the mode to save the credentials
        {
            Write-Host "Enter file path and file name to save credentials (example: C:\users\bob\machine1.txt)"
            $storagepath = Read-Host

            try
            {
                $loginJson | Out-File $storagepath -NoClobber -ErrorAction stop
            }
        }
    }
}
```



```

    }
    catch [System.Exception]
    {
        Write-Host $_.Exception.message
        if ($_.Exception.GetType() -eq [System.IO.IOException]) # file already exists throws an IO exception
        {
            do
            {
                Write-Host "Overwrite existing credentials for this machine?"
                [string]$overwriteQuery = Read-Host
                if ($overwriteQuery[0] -eq 'y')
                {
                    $loginJson | Out-File $storagepath -ErrorAction stop
                    $exitquery = 1
                }
                elseif ($overwriteQuery[0] -eq 'n')
                {
                    $exitquery = 1
                }
                else
                {
                    Write-Host "Please respond with a y or n"
                    $exitquery = 0
                }
            } while ($exitquery -eq 0)
        }
        else
        {
            Write-Host "improper filepath or no permission to write to given directory"
            Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Improper filepath,
            $storagepath " $_.Exception.message
            return
        }
    }

    $savedLoginJson = Get-Content $storagepath

    Write-Host "Run backup?"

    $continue = 0
    do
    {
        $earlyExit = Read-Host
        if ($earlyExit[0] -eq 'n')
        {
            return
        }
        elseif ($earlyExit[0] -ne 'y')
        {
            Write-Host "please respond with a y or n"
        }
        else
        {
            $continue = 1
        }
    } while ($continue -eq 0)

    }
    else
    {
        return $loginJson
    }
}
elseif ($args.count -ne 1)
{
    Write-Host "Incorrect number of arguments, use either filepath parameter or no parameters."
    return
}
else
{
    foreach ($arg in $args)
    {
        $storagepath = $arg
    }
    try
    {
        $savedLoginJson = Get-Content $storagepath -ErrorAction stop
    }
    catch [System.Exception]
    {
        Write-Host "Login credential file not found. Please run script without arguments to access manual entry
        mode."
        Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Login credential file not
        found. Please run script without arguments to access manual entry mode."
        return
    }
}
return $savedloginJson
}

```

```

##### getApiVersion: Get X API Version #####
function getApiVersion ([int32] $currentApiVersion,[string]$hostname)
{
    <#
        .DESCRIPTION
            Sends a web request to the appliance to obtain the current Api version.
            Returns the lower of: Api version supported by the script and Api version
            supported by the appliance.

        .PARAMETER currentApiVersion
            Api version that the script is currently using

        .PARAMETER hostname
            The appliance address to send the request to (in https://{ipaddress} format)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs the new active Api version

        .EXAMPLE
            $global:scriptApiVersion = getApiVersion()
    #>

    # the particular Uri on the Appliance to request the Api Version
    $versionUri = "/rest/version"

    # append the Uri to the end of the IP address to obtain a full Uri
    $fullVersionUri = $hostname + $versionUri

    # use setup-request to issue the REST request api version and get the response
    try
    {
        $applianceVersionJson = setup-request -Uri $fullVersionUri -method "GET" -accept "application/json"
    -contentType "application/json"
        if ($applianceVersionJson -ne $null)
        {
            $applianceVersion = $applianceVersionJson | convertFrom-Json
            $currentApplianceVersion = $applianceVersion.currentVersion
            if ($currentApplianceVersion -lt $currentApiVersion)
            {
                return $currentApplianceVersion
            }
            return $currentApiVersion
        }
    }
    catch [System.Exception]
    {
        if ($global:interactiveMode -eq 1)
        {
            Write-Host $error[0].Exception.Message
        }
        else
        {
            Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $error[0].Exception.Message
        }
    }
}

##### Sending login info #####
function login-appliance ([string]$username,[string]$password,[string]$hostname)
{
    <#
        .DESCRIPTION
            Attempts to send a web request to the appliance and obtain an authorized sessionID.

        .PARAMETER username
            The username to log into the remote appliance

        .PARAMETER password
            The correct password associated with username

        .PARAMETER hostname
            The appliance address to send the request to (in https://{ipaddress} format)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs the response body containing the needed session ID.

        .EXAMPLE
            $authToken = login-appliance $username $password $hostname
    #>

    # the particular Uri on the Appliance to request an "auth token"
    $loginUri = "/rest/login-sessions"

    # append the Uri to the end of the IP address to obtain a full Uri
    $fullLoginUri = $hostname + $loginUri

```

```

# create the request body as a hash table, then convert it to json format
$body = @{ userName = $username; password = $password } | convertTo-json

# use setup-request to issue the REST request to login and get the response
try
{
    $loginResponse = setup-request -Uri $fullLoginUri -method "POST" -accept "application/json" -contentType
"application/json" -Body $body
    if ($loginResponse -ne $null)
    {
        $loginResponse | convertFrom-Json
    }
}
catch [System.Exception]
{
    if ($global:interactiveMode -eq 1)
    {
        Write-Host $error[0].Exception.Message
    }
    else
    {
        Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $error[0].Exception.Message
    }
}
}

##### Executing backup #####
function backup-Appliance ([string]$authValue,[string]$hostname)
{
    <#
        .DESCRIPTION
            Gives the appliance the command to start creating a backup

        .PARAMETER authValue
            The authorized sessionID given by login-appliance

        .PARAMETER hostname
            The location of the appliance to connect to (in https://{ipaddress} format)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The task Resource returned by the appliance, converted to a hashtable object

        .EXAMPLE
            $taskResource = backup-Appliance $sessionID $hostname
    #>

    # append the REST Uri for backup to the IP address of the Appliance
    $bkupUri = "/rest/backups/"
    $fullBackupUri = $hostname + $bkupUri

    # create a new webrequest and add the proper headers (new header, auth, is needed for authorization
    # in all functions from this point on)
    try
    {
        if ($global:scriptApiVersion -lt $taskResourceV2ApiVersion)
        {
            $taskResourceJson = setup-request -Uri $fullBackupUri -method "POST" -accept "application/json" -contentType
"application/json" -authValue $authValue
        }
        else
        {
            $taskUri = setup-request -Uri $fullBackupUri -method "POST" -accept "application/json" -contentType
"application/json" -authValue $authValue -returnLocation $true
            if ($taskUri -ne $null)
            {
                $taskResourceJson = setup-request -Uri $taskUri -method "GET" -accept "application/json" -contentType
"application/json" -authValue $authValue
            }
        }
        if ($taskResourceJson -ne $null)
        {
            return $taskResourceJson | ConvertFrom-Json
        }
    }
    catch [System.Exception]
    {
        if ($global:interactiveMode -eq 1)
        {
            Write-Host $error[0].Exception.Message
        }
        else
        {
            Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $error[0].Exception.Message
        }
    }
}

##### Polling to see if backup is finished #####

```

```

function waitFor-completion ([object]$taskResource,[string]$authValue,[string]$hostname)
{
    <#
        .DESCRIPTION
            Checks the status of the backup every twenty seconds, stops when status changes from running to a
different status

        .PARAMETER taskResource
            The response object from the backup-appliance method

        .PARAMETER authValue
            The authorized session ID

        .PARAMETER hostname
            The appliance to connect to (in https://{ipaddress} format)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The new task resource object, which contains the Uri to get the backup resource in the next function

        .EXAMPLE
            $taskResource = waitFor-Completion $taskResource $sessionID $hostname
    #>

    # extracts the Uri of the task Resource from itself, to poll repeatedly
    $taskResourceUri = $taskResource.uri
    if ($taskResourceUri -eq $null)
    {
        # Caller will provide the error message
        return
    }

    # appends the Uri to the hostname to create a fully-qualified Uri
    $fullTaskUri = $hostname + $taskResourceUri

    # retries if unable to get backup progress information
    $errorCount = 0
    $errorMessage = ""

    if ($global:interactiveMode -eq 1)
    {
        Write-Host "Backup initiated."
        Write-Host "Checking for backup completion, this may take a while."
    }

    # a while loop to determine when the backup process is finished
    do
    {
        try
        {
            # creates a new webrequest with appropriate headers
            $taskResourceJson = setup-request -Uri $fullTaskUri -method "GET" -accept "application/json" -authValue
$authValue -isSilent $true
            # converts the response from the Appliance into a hash table
            $taskResource = $taskResourceJson | convertFrom-Json
            # checks the status of the task manager
            $status = $taskResource.taskState
        }
        catch
        {
            $errorMessage = $error[0].Exception.Message
            $errorCount = $errorCount + 1
            $status = "RequestFailed"
            Start-Sleep -s 15
            continue
        }

        # Update progress bar
        if ($global:interactiveMode -eq 1)
        {
            $trimmedPercent = ($taskResource.completedSteps) / 5
            $progressBar = "[" + "=" * $trimmedPercent + " " * (20 - $trimmedPercent) + "]"
            Write-Host "`r Backup progress: $progressBar " $taskResource.completedSteps "%" -NoNewline
        }

        # Reset the error count since progress information was successfully retrieved
        $errorCount = 0

        # If the backup is still running, wait a bit, and then check again
        if ($status -eq "Running")
        {
            Start-Sleep -s 20
        }
    } while (($status -eq "Running" -or $status -eq "RequestFailed") -and $errorCount -lt 20);

    # if the backup reported an abnormal state, report the state and exit function
    if ($status -ne "Completed")
    {

```

```

        if ($global:interactiveMode -eq 1)
        {
            Write-Host "`n"
            Write-Host "Backup stopped abnormally"
            Write-Host $errorMessage
        }
        else
        {
            #log error message
            Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Backup stopped abnormally"

            Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $errorMessage
        }
        return $null
    }

    # upon successful completion of task, outputs a hash table which contains task resource
    else
    {
        Write-Host "`n"
        $taskResource
        return
    }
}

##### Gets the backup resource #####
function get-backupResource ([object]$taskResource, [string]$authValue, [string]$hostname)
{
    <#
        .DESCRIPTION
            Gets the Uri for the backup resource from the task resource and gets the backup resource

        .PARAMETER taskResource
            The task resource object that we use to get the Uri for the backup resource

        .PARAMETER authValue
            The authorized sessionID

        .PARAMETER hostname
            the appliance to connect to (in https://{ipaddress} format)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The backup resource object

        .EXAMPLE
            $backupResource = get-BackupResource $taskResource $sessionID $applianceName
    #>

    # the backup Resource Uri is extracted from the task resource
    if ($global:scriptApiVersion -lt $taskResourceV2ApiVersion)
    {
        $backupUri = $taskResource.associatedResourceUri
    }
    else
    {
        $backupUri = $taskResource.associatedResource.resourceUri
    }
    if ($backupUri -eq $null)
    {
        # Caller will provide the error message
        return
    }
    # construct the full backup Resource Uri from the hostname and the backup resource uri
    $fullBackupUri = $hostname + $backupUri

    # get the backup resource that contains the Uri for downloading
    try
    {
        # creates a new webrequest with appropriate headers
        $backupResourceJson = setup-request -Uri $fullBackupUri -method "GET" -accept "application/json" -auth
$authValue
        if ($backupResourceJson -ne $null)
        {
            $resource = $backupResourceJson | convertFrom-Json
            if ($global:interactiveMode -eq 1)
            {
                Write-Host "Obtained backup resource. Now downloading. This may take a while ..."
            }
            $resource
            return
        }
    }
    catch [System.Exception]
    {
        if ($global:interactiveMode -eq 1)
        {
            Write-Host $error[0].Exception.Message
        }
        else
        {

```

```

        Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $error[0].Exception.Message
    }
}
}

##### Function to download the backup file #####
function download-Backup ([PSCustomObject]$backupResource, [string]$authValue, [string]$hostname)
{
    <#
        .DESCRIPTION
            Downloads the backup file from the appliance to the local system. Tries to use the
            curl command. The curl command has significantly better performance especially for
            large backups. If curl isn't installed, invokes download-Backup-without-curl to
            download the backup.

        .PARAMETER backupResource
            Backup resource containing Uri for downloading

        .PARAMETER authValue
            The authorized sessionID

        .PARAMETER hostname
            The IP address of the appliance

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The absolute path of the download file

        .EXAMPLE
            download-backup $backupResource $sessionID https://11.111.11.111
    #>

    $downloadUri = $hostname + $backupResource.downloadUri
    $fileDir = [environment]::GetFolderPath("Personal")
    $filePath = $fileDir + "\" + $backupResource.id + ".bkp"
    $curlDownloadCommand = "curl -o " + $filePath + " -s -f -L -k -X GET " +
        "-H 'accept: application/octet-stream' " +
        "-H 'auth: " + $authValue + "' " +
        "-H 'X-API-Version: $global:scriptApiVersion' " +
        $downloadUri
    $curlGetDownloadErrorCommand = "curl -s -k -X GET " +
        "-H 'accept: application/json' " +
        "-H 'auth: " + $authValue + "' " +
        "-H 'X-API-Version: $global:scriptApiVersion' " +
        $downloadUri

    try
    {
        $testCurlSslOption = curl -V
        if ($testCurlSslOption -match "SSL")
        {
            invoke-expression $curlDownloadCommand
        }
        else
        {
            if ($global:interactiveMode -eq 1)
            {
                Write-Host "Version of curl must support SSL to get improved download performance."
            }
            else
            {
                Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Version of curl must
support SSL to get improved download performance"
            }

            return download-Backup-without-curl $backupResource $authValue $hostname
        }
    }

    if ($LASTEXITCODE -ne 0)
    {
        $errorResponse = invoke-expression $curlGetDownloadErrorCommand
        if ($global:interactiveMode -eq 1)
        {
            Write-Host "Download using curl error: $errorResponse"
        }
        else
        {
            Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Download error:
$errorResponse"
        }

        if (Test-Path $filePath)
        {
            Remove-Item $filePath
        }
        return
    }

    if ($global:interactiveMode -eq 1)
    {

```

```

        Write-Host "Backup download complete!"
    }
}
catch [System.Management.Automation.CommandNotFoundException]
{
    return download-Backup-without-curl $backupResource $authValue $hostname
}
catch [System.Exception]
{
    Write-Host "Not able to download backup"
    Write-Host $error[0].Exception
    return
}

return $filePath
}

##### Function to download the Backup file without using the curl command #####
function download-Backup-without-curl ([PSCustomObject]$backupResource, [string]$authValue, [string]$hostname)
{
    <#
        .DESCRIPTION
            Downloads the backup file from the appliance to the local system (without using curl)

        .PARAMETER backupResource
            Backup resource containing Uri for downloading

        .PARAMETER authValue
            The authorized sessionID

        .PARAMETER hostname
            The IP address of the appliance

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The absolute path of the download file

        .EXAMPLE
            download-backup-without-curl $backupResource $sessionID https://11.111.11.111
    #>

    # appends Uri ( obtained from previous function) to IP address
    $downloadUri = $hostname + $backupResource.downloadUri
    $downloadTimeout = 43200000 # 12 hours
    $bufferSize = 65536 # bytes

    # creates a new webrequest with appropriate headers
    [net.webRequest]$downloadRequest = [net.webRequest]::create($downloadUri)
    $downloadRequest.method = "GET"
    $downloadRequest.AllowAutoRedirect = $TRUE
    $downloadRequest.Timeout = $downloadTimeout
    $downloadRequest.ReadWriteTimeout = $downloadTimeout
    $downloadRequest.Headers.Add("auth", $authValue)
    $downloadRequest.Headers.Add("X-API-Version", $global:scriptApiVersion)
    # accept either octet-stream or json to allow the response body to contain either the backup or an exception

    $downloadRequest.accept = "application/octet-stream;q=0.8,application/json"

    # creates a variable that stores the path to the file location. Note: users may change this to other file
    paths.
    $fileDir = [environment]::GetFolderPath("Personal")

    try
    {
        # connects to the Appliance, creates a new file with the content of the response
        [net.webResponse]$response = $downloadRequest.getResponse()
        $responseStream = $response.GetResponseStream()
        $responseStream.ReadTimeout = $downloadTimeout

        #saves file as the name given by the backup ID
        $filePath = $fileDir + "\" + $backupResource.id + ".bkp"
        $srr = New-Object System.IO.FileStream ($filePath, [System.IO.FileMode]::create)
        $responseStream.CopyTo($srr, $bufferSize)
        $response.close()
        $srr.close()
        if ($global:interactiveMode -eq 1)
        {
            Write-Host "Backup download complete!"
        }
    }
    catch [Net.WebException]
    {
        $errorMessage = $error[0].Exception.message

        #Try to get more information about the error
        try {
            $errorResponse = $error[0].Exception.InnerException.Response.GetResponseStream()
            $srr = New-Object IO.StreamReader ($errorResponse)
            $rawErrorStream = $srr.readtoend()
            $error[0].Exception.InnerException.Response.close()
            $errorObject = $rawErrorStream | convertFrom-Json
        }
    }
}

```

```

        if (($errorObject.message.length -gt 0) -and
            ($errorObject.recommendedActions.length -gt 0))
        {
            $errorMessage = $errorObject.message + " " + $errorObject.recommendedActions
        }
    }
catch [System.Exception]
{
    #Use exception message
}

if ($global:interactiveMode -eq 1)
{
    Write-Host $errorMessage
}
else
{
    Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $errorMessage
}
return
}

return $filePath
}

function setup-request ([string]$uri,[string]$method,[string]$accept,[string]$contentType = "",[string]$authValue
= "",[object]$body = $null,[bool]$isSilent=$false, [bool]$returnLocation=$false)
{
    try
    {
        [net.httpWebRequest]$request = [net.webRequest]::create($uri)
        $request.method = $method
        $request.accept = $accept

        $request.Headers.Add("Accept-Language: en-US")
        if ($contentType -ne "")
        {
            $request.ContentType = $contentType
        }
        if ($authValue -ne "")
        {
            $request.Headers.Item("auth") = $authValue
        }
        $request.Headers.Item("X-API-Version") = $global:scriptApiVersion
        if ($body -ne $null)
        {
            $requestBodyStream = New-Object IO.StreamWriter $request.getRequestStream()
            $requestBodyStream.WriteLine($body)
            $requestBodyStream.Flush()
            $requestBodyStream.Close()
        }

        # attempt to connect to the Appliance and get a response
        [net.httpWebResponse]$response = $request.GetResponse()

        if ($returnLocation)
        {
            $taskUri = $response.GetResponseHeader("Location")

            $response.Close()
            return $taskUri
        }
        else
        {
            # response stored in a stream
            $responseStream = $response.GetResponseStream()
            $sr = New-Object IO.StreamReader ($responseStream)

            #the stream, which contains a json object, is read into the storage variable
            $rawResponseContent = $sr.ReadToEnd()
            $response.Close()
            return $rawResponseContent
        }
    }
catch [Net.WebException]
{
    $errorMessage = $error[0].Exception.message

    #Try to get more information about the error
    try {
        $errorResponse = $error[0].Exception.InnerException.Response.GetResponseStream()
        $sr = New-Object IO.StreamReader ($errorResponse)
        $rawErrorStream = $sr.ReadToEnd()
        $error[0].Exception.InnerException.Response.Close()
        $errorObject = $rawErrorStream | ConvertFrom-Json
        if (($errorObject.message.length -gt 0) -and
            ($errorObject.recommendedActions.length -gt 0))
        {
            $errorMessage = $errorObject.message + " " + $errorObject.recommendedActions
        }
    }
catch [System.Exception]
{

```



```

        #Use exception message
    }

    if ($isSilent) {
        throw $errorMessage
    }
    elseif ($global:interactiveMode -eq 1)
    {
        Write-Host $errorMessage
    }
    else
    {
        Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $errorMessage
    }

    #No need to rethrow since already recorded error
    return
}
}

##### Start of function calls #####

#gets the credentials from user, either manual entry or from file
$savedLoginJson = queryfor-credentials $args[0]
if ($savedLoginJson -eq $null)
{
    #if an error occurs, it has already been logged in the queryfor-credentials function
    return
}

#extracts needed information from the credential json
try
{
    $savedLoginJson = "[" + $savedLoginJson + "]"
    $savedloginVals = $savedLoginJson | convertFrom-Json
    $SecStrLoginname = $savedloginVals.userName | ConvertTo-SecureString -ErrorAction stop
    $loginname =

[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($SecStrLoginName))

    $hostname = $savedloginVals.hostname
    $SecStrPassword = $savedloginVals.password | ConvertTo-SecureString -ErrorAction stop
    $password =

[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($SecStrpassword))
}
catch [System.Exception]
{
    if ($global:interactiveMode -eq 1)
    {
        Write-Host "Failed to get credentials: " + $error[0].Exception.Message
    }
    else
    {
        Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Failed to get credentials: "
+ $error[0].Exception.Message
    }
}

#determines the active Api version
$global:scriptApiVersion = getApiVersion $global:scriptApiVersion $hostname
if ($global:scriptApiVersion -eq $null)
{
    if ($global:interactiveMode -eq 1)
    {
        Write-Host "Could not determine appliance Api version"
    }

    Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Could not determine appliance
Api version"
    return
}

#sends the login request to the machine, gets an authorized session ID if successful
$authValue = login-appliance $loginname $password $hostname
if ($authValue -eq $null)
{
    if ($global:interactiveMode -eq 1)
    {
        Write-Host "Failed to receive login session ID."
    }
    Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Failed to receive login session
ID."
    return
}

#sends the request to start the backup process, returns the taskResource object
$taskResource = backup-Appliance $authValue.sessionID $hostname
if ($taskResource -eq $null)
{
    if ($global:interactiveMode -eq 1)
    {

```

```

        Write-Host "Could not initialize backup"
    }

    Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Could not initialize backup"
    return
}

#loops to keep checking how far the backup has gone
$taskResource = waitfor-completion $taskResource $authValue.sessionID $hostname
if ($taskResource -eq $null)
{
    if ($global:interactiveMode -eq 1)
    {
        Write-Host "Could not fetch backup status"
    }

    Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Could not fetch backup status"

    return
}

#gets the backup resource
$backupResource = get-backupResource $taskResource $authValue.sessionID $hostname
if ($backupResource -eq $null)
{
    if ($global:interactiveMode -eq 1)
    {
        Write-Host "Could not get the Backup Resource"
    }
    Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Could not get the Backup Resource"

    return
}

#downloads the backup file to the local drive
$filePath = download-Backup $backupResource $authValue.sessionID $hostname
if ($filePath -eq $null)
{
    if ($global:interactiveMode -eq 1)
    {
        Write-Host "Could not download the backup"
    }
    Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message "Could not download the backup"

    return
}

if ($global:interactiveMode -eq 1)
{
    Write-Host "Backup can be found at $filePath"
    Write-Host "If you wish to automate this script in the future and re-use login settings currently entered,"
    Write-Host "then provide the file path to the saved credentials file when running the script."
    Write-Host "ie: " $MyInvocation.MyCommand.Definition " filepath"
}
else
{
    Write-Host "Backup completed successfully."
    Write-Host "The backup can be found at $filePath."
}
Write-EventLog -EventId 0 -LogName Application -Source backup.ps1 -Message "script completed successfully"

```

C.2 Sample restore script

As an alternative to using **Settings**→**Actions**→**Restore from backup** from the appliance UI, you can write and run a script to automatically restore the appliance from a backup file.

NOTE: Only a user with Infrastructure administrator privileges can restore an appliance.

Example 9 “Sample restore.ps1 script” provides a sample script that restores the appliance from a backup file or obtains progress about an ongoing restore process.

Sample script

If you do not pass parameters to the script, the script uploads and restores a backup file.

1. Calls `query-user()` to get the appliance host name, user name and password, and backup file path.
2. Calls `login-appliance()` to issue a REST request to get a session ID used to authorize restore REST calls.
3. Calls `uploadTo-appliance()` to upload the backup to the appliance.

4. Calls `start-restore()` to start the restore.
 5. Calls `restore-status()` to periodically check the restore status until the restore completes.
- If you pass the `-status` option to the script, the script verifies and reports the status of the last or an ongoing restore until the restore process is complete:
1. Calls `recover-restoreID()` to get the URI to verify the status of the last or an ongoing restore.
 2. Calls `restore-status()` to periodically verify the restore status until the restore completes.

Example 9 Sample restore.ps1 script

```
#(C) Copyright 2013 Hewlett-Packard Development Company, L.P.
#####
# Name:      restore.ps1
# Usage:     {directory}\restore.ps1 or {directory}\restore.ps1 -status https://{ipaddress}
# Purpose:   Uploads a backup file to the appliance and then restores the appliance using the backup data
# Notes:     To improve performance, this script uses the curl command if it is installed. The curl command
#            must be installed with the SSL option.
#            Windows PowerShell 3.0 must be installed to run the script
#####

#Notifies the computer that this is a trusted source we are connecting to (brute force, could be refined)
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = { $true }

# The scriptApiVersion is the default Api version (if the appliance supports this level
# or higher). This variable may be changed if the appliance is at a lower Api level.
$global:scriptApiVersion = 3

#### Obtain information from user ####
function query-user ()
{
    <#
        .DESCRIPTION
            Obtains information needed to run the script by prompting the user for input.

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs an object containing the obtained information.

        .EXAMPLE
            $userVals = query-user
    #>
    Write-Host "Restoring from backup is a destructive process, continue anyway?"

    $continue = 0
    do
    {
        $earlyExit = Read-Host
        if ($earlyExit[0] -eq 'n')
        {
            return
        }
        elseif ($earlyExit[0] -ne 'y')
        {
            Write-Host "please respond with a y or n"
        }
        else
        {
            $continue = 1
        }
    } while ($continue -eq 0)

    do
    {
        Write-Host "Enter directory backup is located in (ie: C:\users\joe\)"
        $backupDirectory = Read-Host
        # Add trailing slash if needed
        if (!$backupDirectory.EndsWith("\"))
        {
            $backupDirectory = $backupDirectory + "\"
        }

        Write-Host "Enter name of backup (ie: appliance_vml_backup_2012-07-07_555555.bkp)"
        $backupFile = Read-Host

        # Check if file exists
        $fullFilePath = $backupDirectory + $backupFile
        if (!(Test-Path $fullFilePath))
        {
            Write-Host "Sorry the backup file $fullFilePath doesn't exist."
        }
    } while (!(Test-Path $fullFilePath))

    Write-Host "Enter appliance IP address (ie: https://10.10.10.10)"
    $hostname = Read-Host
    # Correct some common errors
    $hostname = $hostname.Trim().ToLower()
    if (!$hostname.StartsWith("https://"))
    {
        if ($hostname.StartsWith("http://"))
        {
            $hostname = $hostname.Replace("http", "https")
        }
        else {
            $hostname = "https://" + $hostname
        }
    }
}
```

```

Write-Host "Enter user name"
$secUsername = Read-Host -AsSecureString
$username =

[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($secUsername))

Write-Host "Enter password"
$secPassword = Read-Host -AsSecureString
$password =

[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($secPassword))

$absolutePath = $backupDirectory + $backupFile

$loginVals = @{ hostname = $hostname; userName = $username; password = $password; backupPath = $absolutePath;
backupFile = $backupFile; }

return $loginVals
}

##### getApiVersion: Get X_API Version #####
function getApiVersion ([int32] $currentApiVersion, [string] $hostname)
{
    <#
        .DESCRIPTION
            Sends a web request to the appliance to obtain the current Api version.
            Returns the lower of: Api version supported by the script and Api version
            supported by the appliance.

        .PARAMETER currentApiVersion
            Api version that the script is currently using

        .PARAMETER hostname
            The appliance address to send the request to (in https://{ipaddress} format)

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs the new active Api version

        .EXAMPLE
            $global:scriptApiVersion = getApiVersion()
    #>

    # the particular Uri on the Appliance to request the Api Version
    $versionUri = "/rest/version"

    # append the Uri to the end of the IP address to obtain a full Uri
    $fullVersionUri = $hostname + $versionUri

    # use setup-request to issue the REST request api version and get the response
    try
    {
        $applianceVersionJson = setup-request -Uri $fullVersionUri -method "GET" -accept "application/json"
        -contentType "application/json"
        if ($applianceVersionJson -ne $null)
        {
            $applianceVersion = $applianceVersionJson | convertFrom-Json
            $currentApplianceVersion = $applianceVersion.currentVersion
            if ($currentApplianceVersion -lt $currentApiVersion)
            {
                return $currentApplianceVersion
            }
            return $currentApiVersion
        }
    }
    catch [System.Exception]
    {
        if ($global:interactiveMode -eq 1)
        {
            Write-Host $error[0].Exception.Message
        }
        else
        {
            Write-EventLog -EventId 100 -LogName Application -Source backup.ps1 -Message $error[0].Exception.Message
        }
    }
}

##### Send the login request to the appliance #####
function login-appliance ([string] $username, [string] $password, [string] $hostname)
{
    <#
        .DESCRIPTION
            Attempts to send a web request to the appliance and obtain a authorized sessionId.

        .PARAMETER username
            The username to log into the remote appliance

        .PARAMETER password

```

```

        The correct password associated with username

.PARAMETER hostname
    The appliance address to send the request to (in https://{ipaddress} format)

.INPUTS
    None, does not accept piping

.OUTPUTS
    Outputs the response body containing the needed session ID.

.EXAMPLE
    $authToken = login-appliance $username $password $hostname
#>

# the particular URI on the Appliance to request an "auth token"
$loginURI = "/rest/login-sessions"

# append the URI to the end of the IP address to obtain a full URI
$fullLoginURI = $hostname + $loginURI
# create the request body as a hash table, then convert it to json format
$body = @{ userName = $username; password = $password } | convertTo-json

try
{
    # create a new webrequest object and give it the header values that will be accepted by the Appliance, get
    response
    $loginRequest = setup-request -Uri $fullLoginURI -method "POST" -accept "application/json" -contentType
"application/json" -Body $body
    Write-Host "Login completed successfully."
}
catch [System.Exception]
{
    Write-Host $_.Exception.message
    Write-Host $error[0].Exception
    return
}

#the output for the function, a hash table which contains a single value, "sessionID"
$loginRequest | convertFrom-Json
return
}

##### Upload the backup file to the appliance #####
function uploadTo-appliance ([string]$filepath, [string]$authinfo, [string]$hostname, [string]$backupFile)
{
    <#

    .DESCRIPTION
        Attempts to upload a backup file to the appliance. Tries to use the curl command.
        The curl command has significantly better performance especially for large backups.
        If curl isn't installed, invokes uploadTo_appliance-without-curl to upload the file.

    .PARAMETER filepath
        The absolute filepath to the backup file.

    .PARAMETER authinfo
        The authorized session ID returned by the login request

    .PARAMETER hostname
        The appliance to connect to

    .PARAMETER backupFile
        The name of the file to upload. Only used to tell the server what file is contained in the post
request.

    .INPUTS
        None, does not accept piping

    .OUTPUTS
        The response body to the upload post request.

    .EXAMPLE
        $uploadResponse = uploadTo-appliance $filePath $sessionID $hostname $fileName
#>

$uploadUri = "/rest/backups/archive"
$fullUploadUri = $hostname + $uploadUri
$curlUploadCommand = "curl -s -k -X POST " +
    "-H 'content-type: multipart/form-data' " +
    "-H 'accept: application/json' " +
    "-H 'auth: " + $authinfo + "' " +
    "-H 'X-API-Version: $global:scriptApiVersion' " +
    "-F file=@" + $filepath + " " +
    $fullUploadUri

Write-Host "Uploading backup file to appliance, this may take a few minutes..."
try
{
    $testCurlSslOption = curl -V
    if ($testCurlSslOption -match "SSL")
    {
        $rawUploadResponse = invoke-expression $curlUploadCommand
        if ($rawUploadResponse -eq $null)

```

```

    {
        return
    }
    $uploadResponse = $rawUploadResponse | convertFrom-Json

    if ($uploadResponse.status -eq "SUCCEEDED")
    {
        Write-Host "Upload complete."
        return $uploadResponse
    }
    else
    {
        Write-Host $uploadResponse
        return
    }
}
else
{
    Write-Host "Version of curl must support SSL to get improved upload performance."
    return uploadTo-appliance-without-curl $filepath $authinfo $hostname $backupFile
}
}
catch [System.Management.Automation.CommandNotFoundException]
{
    return uploadTo-appliance-without-curl $filepath $authinfo $hostname $backupFile
}
catch [System.Exception]
{
    Write-Host "Not able to upload backup"
    Write-Host $error[0].Exception
    return
}
}

##### Upload the backup file to the appliance without using the curl command #####
function uploadTo-appliance-without-curl
([string]$filepath, [string]$authinfo, [string]$hostname, [string]$backupFile)
{
    <#
        .DESCRIPTION
            Attempts to upload a backup to the appliance without using curl.

        .PARAMETER filepath
            The absolute filepath to the backup file.

        .PARAMETER authinfo
            The authorized session ID returned by the login request

        .PARAMETER hostname
            The appliance to connect to

        .PARAMETER backupFile
            The name of the file to upload. Only used to tell the server what file is contained in the post
request.

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The response body to the upload post request.

        .EXAMPLE
            $uploadResponse = uploadTo-appliance $filePath $sessionID $hostname $fileName
    #>

    $uploadUri = "/rest/backups/archive"
    $fullUploadUri = $hostname + $uploadUri
    $uploadTimeout = 43200000 # 12 hours
    $bufferSize = 65536 # bytes

    try
    {
        [net.webRequest]$uploadRequest = [net.webRequest]::create($fullUploadUri)
        $uploadRequest.method = "POST"
        $uploadRequest.Timeout = $uploadTimeout
        $uploadRequest.ReadWriteTimeout = $uploadTimeout
        $uploadRequest.SendChunked = 1
        $uploadRequest.AllowWriteStreamBuffering = 0
        $uploadRequest.accept = "application/json"
        $boundary = "-----bac8d687982e"
        $uploadRequest.ContentType = "multipart/form-data; boundary=-----bac8d687982e"
        $uploadRequest.Headers.Add("auth", $authinfo)
        $uploadRequest.Headers.Add("X-API-Version", $global:scriptApiVersion)
        $fs = New-Object IO.FileStream ($filepath, [System.IO.FileMode]::Open)
        $rs = $uploadRequest.getRequestStream()
        $rs.WriteTimeout = $uploadTimeout
        $disposition = "Content-Disposition: form-data; name=""file""; filename=""encryptedBackup""
        $contentType = "Content-Type: application/octet-stream"

        [byte[]]$BoundaryBytes = [System.Text.Encoding]::UTF8.GetBytes("--" + $boundary + "`r`n");
        $rs.write($BoundaryBytes, 0, $BoundaryBytes.Length);

        [byte[]]$contentDisp = [System.Text.Encoding]::UTF8.GetBytes($disposition + "`r`n");

```

```

$rs.write($contentDisp,0,$contentDisp.Length);

[byte[]]$contentType = [System.Text.Encoding]::UTF8.GetBytes($contentType + "`r`n`r`n");
$rs.write($contentType,0,$contentType.Length);

$fs.CopyTo($rs,$bufferSize)
$fs.close()

[byte[]]$endBoundaryBytes = [System.Text.Encoding]::UTF8.GetBytes("`n`r`n--" + $boundary + "--`r`n");
$rs.write($endBoundaryBytes,0,$endBoundaryBytes.Length);
$rs.close()
}
catch [System.Exception]
{
    Write-Host "Not able to send backup"
    Write-Host $error[0].Exception
}
try
{
    [net.httpWebResponse]$response = $uploadRequest.getResponse()
    $responseStream = $response.getResponseStream()
    $responseStream.ReadTimeout = $uploadTimeout
    $streamReader = New-Object IO.StreamReader ($responseStream)
    $rawUploadResponse = $streamReader.readtoend()
    $response.close()

    if ($rawUploadResponse -eq $null)
    {
        return
    }

    $uploadResponse = $rawUploadResponse | convertFrom-Json

    if ($uploadResponse.status -eq "SUCCEEDED")
    {
        Write-Host "Upload complete."
        return $uploadResponse
    }
    else
    {
        Write-Host $rawUploadResponse
        Write-Host $uploadResponse
        return
    }
}
catch [Net.WebException]
{
    Write-Host $error[0]
    $errorResponse = $error[0].Exception.InnerException.Response.getResponseStream()
    $srr = New-Object IO.StreamReader ($errorResponse)

    $rawErrorStream = $srr.readtoend()
    $error[0].Exception.InnerException.Response.close()
    $errorObject = $rawErrorStream | convertFrom-Json

    Write-Host $errorObject.errorcode $errorObject.message $errorObject.resolution
    return
}
}

##### Initiate the restore process #####
function start-restore ([string]$authinfo, [string]$hostname, [object]$uploadResponse)
{
    <#
        .DESCRIPTION
            Sends a POST request to the restore resource to initiate a restore.

        .PARAMETER authinfo
            The authorized sessionID obtained from login.

        .PARAMETER hostname
            The appliance to connect to.

        .PARAMETER uploadResponse
            The response body from the upload request. Contains the backup URI needed for restore call.

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            Outputs the response body from the POST restore call.

        .EXAMPLE
            $restoreResponse = start-restore $sessionID $hostname $uploadResponse
    #>
    # append the appropriate URI to the IP address of the Appliance
    $backupUri = $uploadResponse.uri
    $restoreUri = "/rest/restores"
    $fullRestoreUri = $hostname + $restoreUri
    $body = @{ type = "RESTORE"; uriOfBackupToRestore = $backupUri } | convertTo-json
    # create a new webrequest and add the proper headers
    try
    {

```



```

    $rawRestoreResponse = setup-request -uri $fullRestoreUri -method "POST" -accept "application/json" -contentType
"application/json" -authValue $authinfo -Body $body

    $restoreResponse = $rawRestoreResponse | convertFrom-Json
    return $restoreResponse
}

catch [Net.WebException]
{
    Write-Host $_.Exception.message
}
}

##### Check for the status of ongoing restore #####
function restore-status ([string]$authinfo = "foo", [string]$hostname, [object]$restoreResponse, [string]$recoveredUri
= "")
{
    <#
        .DESCRIPTION
            Uses GET requests to check the status of the restore process.

        .PARAMETER authinfo
            **to be removed once no longer a required header**

        .PARAMETER hostname
            The appliance to connect to

        .PARAMETER restoreResponse
            The response body from the restore initiation request.

        .PARAMETER recoveredUri
            In case of a interruption in the script or connection, the Uri for status is instead obtained through
this parameter.

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            None, end of script upon completion or fail.

        .EXAMPLE
            restore-status *$authinfo* -hostname $hostname -restoreResponse $restoreResponse

            or

            restore-status -hostname $hostname -recoveredUri $recoveredUri
    #>
    # append the appropriate URI to the IP address of the Appliance

    if ($recoveredUri -ne "")
    {
        $fullStatusUri = $hostname + $recoveredUri
        write-host $fullStatusUri
    }
    else
    {
        $fullStatusUri = $hostname + $restoreResponse.uri
    }
    do
    {
        try
        {
            # create a new webrequest and add the proper headers (new header, auth is needed for authorization
            $rawStatusResp = setup-request -uri $fullStatusUri -method "GET" -accept "application/json" -contentType
"application/json" -authValue $authinfo
            $statusResponse = $rawStatusResp | convertFrom-Json
            $trimmedPercent = ($statusResponse.percentComplete) / 5
            $progressBar = "[" + "=" * $trimmedPercent + " " * (20 - $trimmedPercent) + "]"
            Write-Host "`rRestore progress: $progressBar " $statusResponse.percentComplete "%" -NoNewline
        }
        catch [Net.WebException]
        {
            try
            {
                $errorResponse = $error[0].Exception.InnerException.Response.GetResponseStream()
                $sr = New-Object IO.StreamReader ($errorResponse)

                $rawErrorStream = $sr.readtoend()
                $error[0].Exception.InnerException.Response.close()
                $errorObject = $rawErrorStream | convertFrom-Json

                Write-Host $errorObject.message $errorObject.recommendedActions
            }
            catch [System.Exception]
            {
                Write-Host "`r`n" $error[1].Exception
            }
            return
        }
    }
    if ($statusResponse.status -eq "SUCCEEDED")
    {
        Write-Host "`r`nRestore complete!"
        return
    }
}

```

```

    }
    if ($statusResponse.status -eq "FAILED")
    {
        Write-Host "`r`nRestore failed! System should now undergo a reset to factory defaults."
    }
    Start-Sleep 10
} while ($statusResponse.status -eq "IN_PROGRESS")

return
}

##### Recovers Uri to the restore resource if connection lost #####
function recover-restoreID ([string]$hostname)
{
    <#
        .DESCRIPTION
            Uses GET requests to check the status of the restore process.

        .PARAMETER hostname
            The appliance to end the request to.

        .INPUTS
            None, does not accept piping

        .OUTPUTS
            The Uri of the restore task in string form.

        .EXAMPLE
            $reacquiredUri = recover-restoredID $hostname
    #>

    $idUri = "/rest/restores/"
    $fullIdUri = $hostname + $idUri
    try
    {
        $rawIdResp = setup-request -uri $fullIdUri -method "GET" -contentType "application/json" -accept
"application/json" -authValue "foo"
        $idResponse = $rawIdResp | convertFrom-Json
    }
    catch [Net.WebException]
    {
        $_.Exception.message
        return
    }
    return $idResponse.members[0].uri
}

function setup-request ([string]$uri,[string]$method,[string]$accept,[string]$contentType =
"",[string]$authValue="0", [object]$body = $null)
{
    <#
        .DESCRIPTION
            A function to handle the more generic web requests to avoid repeated code in every function.

        .PARAMETER uri
            The full address to send the request to (required)

        .PARAMETER method
            The type of request, namely POST and GET (required)

        .PARAMETER accept
            The type of response the request accepts (required)

        .PARAMETER contentType
            The type of the request body

        .PARAMETER authValue
            The session ID used to authenticate the request

        .PARAMETER body
            The message to put in the request body

        .INPUTS
            None

        .OUTPUTS
            The response from the appliance, typically in Json form.

        .EXAMPLE
            $responseBody = setup-request -uri https://10.10.10.10/rest/doThis -method "GET" -accept "application/json"
    #>
    try
    {
        [net.httpsWebRequest]$request = [net.webRequest]::create($uri)
        $request.method = $method
        $request.accept = $accept

        $request.Headers.Add("Accept-Language: en-US")
        if ($contentType -ne "")
        {
            $request.ContentType = $contentType
        }
    }

```

```

        if ($authValue -ne "0")
        {
            $request.Headers.Item("auth") = $authValue
        }
        $request.Headers.Add("X-API-Version: $global:scriptApiVersion")
        if ($body -ne $null)
        {
            #write-host $body
            $requestBodyStream = New-Object IO.StreamWriter $request.getRequestStream()
            $requestBodyStream.WriteLine($body)

            $requestBodyStream.flush()
            $requestBodyStream.close()
        }

        # attempt to connect to the Appliance and get a response
        [net.HttpWebResponse]$response = $request.GetResponse()

        # response stored in a stream
        $responseStream = $response.GetResponseStream()
        $sr = New-Object IO.StreamReader ($responseStream)

        #the stream, which contains a json object is read into the storage variable
        $rawResponseContent = $sr.readtoend()
        $response.close()
        return $rawResponseContent
    }
    catch [Net.WebException]
    {
        try
        {
            $errorResponse = $error[0].Exception.InnerException.Response.GetResponseStream()
            $sr = New-Object IO.StreamReader ($errorResponse)
            $rawErrorStream = $sr.readtoend()
            $error[0].Exception.InnerException.Response.close()
            $errorObject = $rawErrorStream | convertFrom-Json
            Write-Host $errorObject.message $errorObject.recommendedActions
        }
        catch [System.Exception]
        {
            Write-Host $error[1].Exception.Message
        }
        throw
        return
    }
}

##### Begin main #####

#this checks to see if the user wants to just check a status of an existing restore
if ($args.count -eq 2)
{
    foreach ($item in $args)
    {
        if ($item -eq "-status")
        {
            [void]$foreach.movenext()
            $hostname = $foreach.current
            # Correct some common errors in hostname
            $hostname = $hostname.Trim().ToLower()
            if (!$hostname.StartsWith("https://"))
            {
                if ($hostname.StartsWith("http://"))
                {
                    $hostname = $hostname.Replace("http","https")
                } else {
                    $hostname = "https://" + $hostname
                }
            }
        }
    }
    else
    {
        Write-Host "Invalid arguments."
        return
    }
}

$reacquiredUri = recover-restoreID -hostname $hostname
if ($reacquiredUri -eq $null)
{
    Write-Host "Error occurred when fetching active restore ID. No restore found."
    return
}
restore-status -recoveredUri $reacquiredUri -hostname $hostname

return
}
elseif ($args.count -eq 0)
{

```

```

$loginVals = query-user
if ($loginVals -eq $null)
{
    Write-Host "Error passing user login vals from function query-host, closing program."
    return
}

#determines the active Api version
$global:scriptApiVersion = getApiVersion $global:scriptApiVersion $loginVals.hostname
if ($global:scriptApiVersion -eq $null)
{
    Write-Host "Could not determine appliance Api version"
    return
}

$authinfo = login-appliance $loginVals.userName $loginVals.password $loginVals.hostname
if ($authinfo -eq $null)
{
    Write-Host "Error getting authorized session from appliance, closing program."
    return
}

$uploadResponse = uploadTo-appliance $loginVals.backupPath $authinfo.sessionID $loginVals.hostname
$loginVals.backupFile
if ($uploadResponse -eq $null)
{
    Write-Host "Error attempting to upload, closing program."
    return
}

$restoreResponse = start-restore $authinfo.sessionID $loginVals.hostname $uploadResponse
if ($restoreResponse -eq $null)
{
    Write-Host "Error obtaining response from Restore request, closing program."
    return
}
restore-status -hostname $loginVals.hostname -restoreResponse $restoreResponse -authinfo $authinfo.sessionID

return
}
else
{
    Write-Host "Usage: restore.ps1"
    Write-Host "or"
    Write-Host "restore.ps1 -status https://{ipaddress}"
    return
}
}

```

Index

A

- Actions menu, 59
- activity, 173
 - see also alert
 - see also task
 - states, 175
 - statuses, 175
 - types, 174
- administrator password
 - resetting, 148
- agentless management, 21
- aggregation switch see data center switch
- alert, 173, 174
 - auto-cleanup, 174
- appliance
 - backup and restore features, 23
 - backup file best practices, 149
 - backup script, 271
 - crash recovery, automated features, 154
 - crash recovery, data protection, 153
 - crash recovery, manual, 154
 - creating support dump file, 201
 - describing icons, 62
 - downloads from, 55
 - host location, 83
 - host, security access, 80
 - initial configuration, 91
 - IP address requirements, 83
 - logging out, 66
 - management LAN, 83
 - NTP configuration, 83
 - online help, 75
 - restart behavior, 154
 - restore script, 282
 - restoring from backup file, 223
 - searching, 67
 - unexpected shutdown, automated recovery features, 154
 - unexpected shutdown, data protection, 153
 - unexpected shutdown, manual recovery, 154
 - VM management best practices, 153
- audit log, 48
 - policy for, 80
- authentication, 47
- authorization, 48
- availability
 - virtual appliance, 24

B

- backup file
 - best practices, 149
 - creating, 150
 - downloading, 150
 - restoring appliance from , 223
 - troubleshooting, 205

- backup policy, 80
- backup script, 80, 271
- best practices
 - appliance backups, 149
 - browser, 52
 - firmware, 137
 - health monitoring, 170, 171
 - VM appliance management, 153
- BladeSystem enclosure, 228
- browser
 - best practices, 52
 - required plugins and settings, 57
 - supported features and settings, 57
 - supported types and version, 57

C

- certificate, 50
 - policy, choosing, 80
 - troubleshooting, 204
- compliance checking, 128
- configuration change
 - planning for, 85
- console access, 53
 - restrict, 54
- contact HP, 227
- copyright, 1
- crashes
 - appliance, automated recovery features, 154
 - appliance, data protection, 153
 - appliance, manual recovery, 154
- credentials, 48

D

- Dashboard, 176
- data center
 - configuring rack placement, 141
 - monitoring temperature, 179
 - planning considerations, 79
 - resource names, 79
 - visualizing temperature, 179
- data center switch
 - matching VLAN IDs to uplink set VLAN IDs, 115
 - port configuration for uplink sets, 115
 - spanning tree edge, 115
 - trunk ports, 115
- details pane, 59
- directory server
 - troubleshooting, 220
- directory service
 - configuring, 143
 - troubleshooting, 219
- discovery, hardware, 19
- documentation
 - download and serve HTML UI help files, 76
 - download and serve REST API documentation, 76
 - enabling off-appliance browsing, 76

- Information Library, [76](#)
 - online help, [75](#)
 - submit feedback to HP, [229](#)
 - website, [76](#)
- downlink, [123](#)

E

- enclosure
 - adding, affected resources, [87](#)
 - HP BladeSystem website, [228](#)
 - managing, [132](#)
- environment
 - initial configuration, [91](#)
- environmental management, [22](#)
- Ethernet networks
 - VLAN range, [119](#)
- EULA
 - how to view, [59](#)

F

- Fibre Channel
 - Direct attach, [117](#)
 - Fabric attach, [117](#)
 - flat SAN, [117](#)
 - uplink set, [124](#)
- Fibre Channel Direct attach, [117](#)
- Fibre Channel Fabric attach, [117](#)
- Fibre Channel over Ethernet (FCoE)
 - downlink from enclosure interconnect to server, [119](#)
- filters sidebar, [61](#)
- firmware
 - appliance shutdown during update, [154](#)
 - best practices, [137](#)
 - compliance checking, [20](#)
 - repository, [20](#)
- flat SAN, [117](#)
- forum
 - user community, [227](#)
- full access role, [144](#)

G

- group
 - compliance checking, [20](#)

H

- hardening, [45](#)
- hardware
 - discovery of, [19](#)
 - inventory management features, [23](#)
- health icon, [62](#)
- health monitoring, [22](#), [170](#)
 - see also activity and SCMB, [21](#)
 - best practices, [170](#), [171](#)
 - REST APIs, [171](#)
- health status, [68](#)
- help
 - searching, [66](#)
- help sidebar, [61](#)

HP

- contacting, [227](#)
- HP iPDU
 - device detection, [19](#)
- HP OneView
 - availability features, [24](#)
 - backup and restore features, [23](#)
 - change management features, [20](#)
 - configuration, automated, [21](#)
 - device detection, [19](#)
 - discovery, [19](#)
 - enclosures, automatic configuration, [19](#)
 - environmental management features, [22](#)
 - firmware baseline compliance checking, [20](#)
 - firmware management features, [20](#)
 - group compliance checking, [20](#)
 - groups, overview, [17](#)
 - hardware inventory, [23](#)
 - hardware provisioning, [16](#)
 - health monitoring, [21](#)
 - health monitoring features, [22](#)
 - Information Library, [76](#)
 - integration with Onboard Administrator, [26](#)
 - integration with other software, [19](#), [26](#)
 - monitoring from other platforms, [21](#)
 - networking features, [27](#)
 - online help, [75](#)
 - operating system deployment, [19](#)
 - overview, [15](#)
 - port-level statistics, [22](#)
 - power and cooling management features, [22](#)
 - provisioning features, [16](#)
 - resource utilization monitoring, [22](#)
 - REST APIs, [25](#)
 - SCMB, [26](#)
 - server profile, overview, [17](#)
 - sets, overview, [17](#)
 - SNMP trap configuration, [21](#)
 - user interface, [25](#)
- HP OneView Information Library, [76](#), [228](#)
- hypervisor client
 - security access, [80](#)

I

- icon description, [62](#)
- iLO management processor
 - accessing using HP OneView, [113](#)
 - configuration by HP OneView, [113](#)
 - HP OneView user roles, [26](#)
 - integration with HP OneView, [26](#), [113](#)
 - licensing, [182](#)
 - licensing with HP OneView, [159](#)
- Information Library, [76](#)
- initial configuration, [91](#)
- interconnect
 - about, [121](#)
 - and staged firmware, [85](#)
 - module in Maintenance state, troubleshooting, [211](#)
 - outage during firmware activation, [85](#)

- staged firmware and reboot actions, 85
- unsupported hardware, 122
- interconnect modification failure
 - troubleshooting, 211

K

- key combinations
 - virtual appliance console, 269

L

- LACP, 115

- LAG, 115

- license

- about, 159
 - compliance, 160
 - delivery, 159
 - enclosures, 161
 - hardware, 160
 - iLO Advanced license, 159
 - rack mount servers, 162
 - reporting, 159
 - servers, 160
 - utilization, 162
 - view, 160

- Link Aggregation Control Protocol *see* LACP

- Link Aggregation Group *see* LAG

- log files, 201

- logical interconnect

- adding, 125
 - compliance checking, 128
 - deleting, 126
 - naming convention, 125
 - outage during firmware activation, 85
 - preventing loss of network connectivity during firmware update, 85
 - removing, 126
 - stacking health, defined, 125
 - stacking mode, enclosure, 125

M

- main menu, 59

- Map view, 59, 64

- master pane, 59

- metric units of measure, 58

N

- naming convention

- data center, 82
 - default names, 82
 - network, 81
 - network set, 81
 - resource, 81
 - typical abbreviations for resources, 82
 - uplink set, 81

- network

- adding, affected resources, 86
 - deleting, affected resources, 85
 - health monitoring, 171
 - naming conventions, 81

- network access
 - troubleshooting, 203

- network set

- deleting, affected resources, 86
 - naming conventions, 81

- networking

- overview, 27

- notifications area

- viewing, 65

O

- Onboard Administrator

- integration with HP OneView, 26

- OneView Forum

- how to access, 59

- online user forum, 227

- Open integration, 26

- open source code

- how to view written offer, 59

P

- password

- resetting administrator, 148

- planning considerations

- data center, 79
 - data center resources, 79
 - security, 79

- ProLiant server hardware, 228

- public key

- troubleshooting, 219

R

- RBAC

- effect on UI, 24

- requirements

- VM host, 82

- resetting administrator password, 148

- resource

- naming conventions, 81
 - relationships, 64

- resource model, 29

- REST API

- online help, 75

- REST API documentation

- enabling off-appliance browsing , 76
 - online help, 75

- restart failure

- troubleshooting, 206

- restore script, 282

- role, 48

S

- SCMB *see* State-Change Message Bus

- screen component

- icons, 67

- screen description, 58

- script

- backup appliance, 271
 - restore appliance, 282

- search, 66, 67
- security
 - Administrator password, 79
 - allowing access by support personnel, 79
 - and DoS attacks, 24
 - and RBAC (role-based access control), 24, 80
 - appliance, 24
 - audit log policy, 80
 - audit logging, 24
 - best practices, 46
 - certificate, 50, 80
 - certificates, 24
 - data download restrictions, 24
 - directory service support, 24
 - firewall, 81
 - hypervisor client access policy, 80
 - management LAN, 24, 79
 - open ports, 81
 - overview of features, 24
 - passwords, 48
 - separation of data and management, 24
 - SNMP read community string, 80
 - SSO (single sign-on), 24
 - UI features, 24
 - user roles, 80
- server blade
 - troubleshooting, 210
- server hardware
 - health monitoring, 171
 - model features, 111
- server profile
 - and network deletion, 85
 - and network set deletion, 86
 - and uplink set deletion, 85
 - and uplink set name changes, 85
 - configuration changes requiring powered off hardware, 86
 - effect of changes to other resources, 86
 - overview, 17
 - previously deleted network set, adding, 86
 - previously deleted network, adding, 86
- services access, 54
- session security, 47
- shutdown failure
 - troubleshooting, 206
- Smart Search toolbar, 67
- SNMP settings, 127
- specialized access role, 144
- SSL cipher suites, 54
- SSL protocol, 50
- stacking health, 125
- stacking links, 123
- stacking mode
 - enclosure, 125
 - logical interconnect, 125
- State-Change Message Bus
 - .NET C# code example, 188
 - connect to the SCMB, 185
 - Java code example, 191
 - JSON structure of message, 187
 - Python code example, 192
 - re-create the AMQP client certificate, 195
 - set up a queue, 186
- status icon, 62
- storage system
 - website, 229
- support dump file
 - creating, 201
 - troubleshooting creation of, 204
- switch, data center see data center switch

T

- tagging, network see VLAN ID
- task, 22, 173, 174
 - see also activity
- thermal hot spots, 179
- top of rack switch see data center switch
- ToR switch see data center switch
- troubleshoot
 - adding enclosure, 208
 - adding server blade, 210
 - adding server hardware, 213
 - creating network, 213
 - network access, 203
 - powering off a server, 214
 - powering on a server, 214
 - removing enclosure, 208
 - removing server hardware, 213
 - support dump file creation, 204

U

- UI help
 - enable off-appliance browsing, 76
 - submit feedback to HP, 229
 - zip file, 76
- unmanaged device
 - about, 42, 165
- unsupported hardware
 - about, 165
- uplink, 123
- uplink set
 - Ethernet networks, 124
 - Fibre Channel networks, 124
 - matching VLAN IDs to switch port VLAN IDs, 115
 - multiple uplinks from same interconnect to same switch, 115
 - naming conventions, 81
 - native network in, 115
 - relationship to data center switches, 115
 - relationship to logical interconnect, 124
 - relationship to logical interconnect group, 124
 - VLAN tags, 115
- US units of measure, 58
- user accounts, 48
- user community
 - online forum, 227
- user interface
 - navigating, 60

- navigating screens, [58](#)
- screen topography, [58](#)
- user role, [80](#), [144](#)
- utilization
 - iLO Advanced license requirement, [182](#)
 - meters, [181](#)
 - overview, [181](#)
 - panel, [181](#)
 - setting US or metric units of measure, [58](#)

V

- view selector, [59](#)
- virtual appliance console, [269](#)
- Virtual Connect
 - website, [229](#)
- VLAN ID
 - matching uplink set to data center switch ports, [115](#)
- VM host
 - requirements for, [82](#)
- vSphere client
 - security access, [80](#)

W

- web browser
 - required plugins and settings, [57](#)
 - supported features and settings, [57](#)
 - supported types and version, [57](#)
- website
 - HP BladeSystem enclosures, [228](#)
 - HP OneView, [228](#)
 - HP OneView community forum, [227](#)
 - HP OneView documentation, [228](#)
 - HP ProLiant server hardware, [228](#)
 - HP Storage, [229](#)
 - HP Virtual Connect, [229](#)
- wizard
 - quick start, [91](#)