Hewlett Packard Enterprise

HPE Workload Aware Security Version 1.3.0

Release Notes for Linux

Abstract

This document describes about HPE WASL 1.3.0, its features, known issues, and the installation requirements.

Part Number: P12138-002a
Published: November 2019
Edition: 2

Notices

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

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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

Acknowledgments

Intel®, Itanium®, Optane®, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

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

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

VMware vSphere® is a registered trademark of VMware, Inc. in the United States and/or other jurisdictions.

Linux® is a registered trademark of Linus Torvalds in the U.S. and other countries.

Red Hat® Enterprise Linux is a registered trademark of Red Hat, Inc. in the United States and other countries.

SUSE and the SUSE logo are registered trademarks of SUSE LLC in the United States and other countries.

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

CIS® is a registered trademark of Center for Internet Security, Inc.

SAP® and SAP HANA® are registered trademarks of SAP.

Intel® and Intel Xeon® are trademarks of Intel Corporation in the in the U.S. and other countries.

Revision history

Part Number	Published
P12138-002a	November 2019
P12138-002	June 2019

Table Continued

Part Number	Published
P12138-001	December 2018
P03765-001	April 2018

Contents

HPE WASL 1.3.0

Introduction

HPE Workload Aware Security for Linux (HPE WASL) offers a way to secure the operating system instance and the associated applications running on it from a centralized system (called Security Management Station- SMS). WASL can evaluate a workload (just operating system or operating system with an associated application) to assess the current security level; remediate- to increase the security level of the workload and provides rich actionable evaluation and remediation reports. WASL also offers a feature to roll back any remediation done and restores the workload configuration to a pre-remediation state. It uniquely provides a functionality to secure the workload along with the operating system.

Evaluation and Remediation is done using security profiles that are built based on XCCDF specification language, enabling extensibility of the profile set. It currently provides the standard profile set based on global benchmarking standards for Operating System; and SAP HANA profiles based on SAP HANA Security Guide and security best practices. The SAP HANA profiles are available only with Advance license version of the product.

What's new in HPE WASL 1.3.0

SAP HANA 2.0 security policy updates

An updated security policy for SAP HANA 2.0 is shipped. This security policy is based on the *SAP HANA Platform 2.0 SPS 03 Document Version: 1.1 of SAP HANA Security Guide, Security Checklists, and Recommendations*.

This policy can be used to secure SAP HANA 2.0 database on SLES for SAP Applications 12 (SP1, SP2, SP3, and SP4) and SLES for SAP Applications 15.

Hardened WASL SMS Appliance

HPE WASL SMS is hardened by default and a security policy that is based on CIS benchmark is delivered. This policy can be used to perform evaluation and remediation of the SMS on an ongoing basis.

Support for RHEL 7.6, SLES 12 SP4 and SLES 15 Operating Systems

This version additionally can secure RHEL 7.6 and SLES 12 SP4 operating system instances using the OS security policies. It also supports securing SLES 15 operating environments, using a draft OS policies.

NOTE: SLES 15 OS policies are draft version policies and will be obsoleted once the SLES 15 policy is created based on the SLES 15 CIS benchmark (which is yet to be published).

What's new in HPE WASL 1.2.0

WASL as a Virtual Appliance

WASL SMS is now shipped as a Virtual Appliance, it can be installed as a virtual machine on a VMware Hypervisor. WASL currently supports VMware vSphere 6.0, 6.5 and 6.7.

Migration support from WASL 1.1.0 to WASL 1.2.0

WASL supports a mechanism to migrate from WASL SMS 1.1.0 running on SLES 11SP4 to WASL 1.2 virtual appliance.

Backup and Restore features support for WASL

HPE WASL supports features to backup WASL SMS data and configuration from WASL 1.1 or WASL 1.2, and restores it on WASL 1.2 Virtual Appliance.

Simple Policy Update and Alerting

HPE WASL now allows a mechanism to update the policies (patch or new) and alert the administrator on new available policies.

Support for RHEL 7.5 and SAP HANA 2.0 SPS03

HPE WASL can now secure RHEL 7.5 operating system instances and SAP HANA 2.0 SPS03 running on SLES for SAP Applications 12.

WASL 1.2.0 defect fixes

WASL 1.2.0 includes the following defect fixes:

- **QXCR1001681412**: WASL node installation fails when OS user name has uppercase letters.
- **QXCR1001681413**: Evaluation fails with a message `Error Creating reports` for OS security policies under certain conditions.
- **QXCR1001681414**: The manual procedure documented for **Set Boot Loader Password** rule is incorrect.

HPE WASL features

The required security state of a workload is defined by a set of rules which constitutes a security policy. WASL automates the process of policy evaluation and enforcement on a workload. A single workload may have multiple applicable policies. HPE WASL provides the following features and benefits.

Evaluation

WASL assesses the compliance of a workload against a specific policy that is deployed on the workload. Assessment can either be done with a single policy or against all the deployed policies.

Remediation

WASL remediates or hardens the workload using a policy that is deployed on the workload. Remediation can either be done with a single policy or using all the deployed policies.

Rollback

WASL supports a mechanism to roll-back the security state of the workload to a state prior to the last remediation operation.

Security Policies

A default set of policies is made available with the product based on the type of license. The product also supports a methodology to customize the available policies and also allows the user to import new policies.

Default Policies

WASL 1.3.0 supports the following set of profiles for assessing and securing the workloads.

SLES Policies

- OS Security Level 1 for SLES 12
- OS Security Level 2 for SLES 12
- OS Security Level 1 for SLES for SAP Applications 12
- OS Security Level 2 for SLES for SAP Applications 12

- OS Security extras for SAP HANA**
- OS Security extras for SAP HANA - update 1*
- Draft OS Security Level 1 for SLES 15*
- Draft OS Security Level 2 for SLES 15*
- Draft OS Security Level 1 for SLES for SAP Applications 15*
- Draft OS Security Level 2 for SLES for SAP Applications 15*

RHEL Policies

- OS Security Level 1 for RHEL 7
- OS Security Level 2 for RHEL 7

SAP HANA Policies

- SAP HANA 1.0 DB Security Level 1
- SAP HANA 1.0 DB Security - Level 2
- SAP HANA 2.0 DB Security - Level 1**
- SAP HANA 2.0 DB Security - Level 1 - update 1*
- SAP HANA 2.0 DB Security - Level 2**
- SAP HANA 2.0 DB Security - Level 2 - update 1*

*Policies added in WASL version 1.3.0

**Deprecated from WASL version 1.3.0

Virtual Appliance Policy

OS Security policy for virtual appliance

Policy Customization

WASL supports a methodology to customize the default and user-defined policies. It also allows importing new profiles (that are defined as per specification) and are used in the WASL environment.

License Information

There are two variants of the WASL license:

- **Basic**: This is the base version of the product used to assure security compliance of the Linux operating system.

  One non-transferable Basic license is required for each active instance of Red Hat Linux OS or SUSE Linux OS supported by WASL. This includes both physical and virtual servers.

- **Advanced**: This version of the license includes the Basic license functionality and adds security compliance checking for Scale-up SAP HANA workloads running on both appliances and TDI deployments.

  One non-transferable advanced license is required for each active instance of SAP HANA supported by WASL.

Each license purchase includes one year of 24x7 Technical Support and Software Updates Service. Beyond the first year, an exclusive HPE product support license is required to receive WASL updates.

WASL Installation and Setup

Overview

A typical deployment of WASL consists of a Security Management Station (SMS) and a set of workloads. A workload can be just an instance of operating system or it can be an instance of operating system with an associated application (for example, SAP HANA) installed on it. WASL can be used to secure either the operating system; or the operating system and associated application; or the application only.

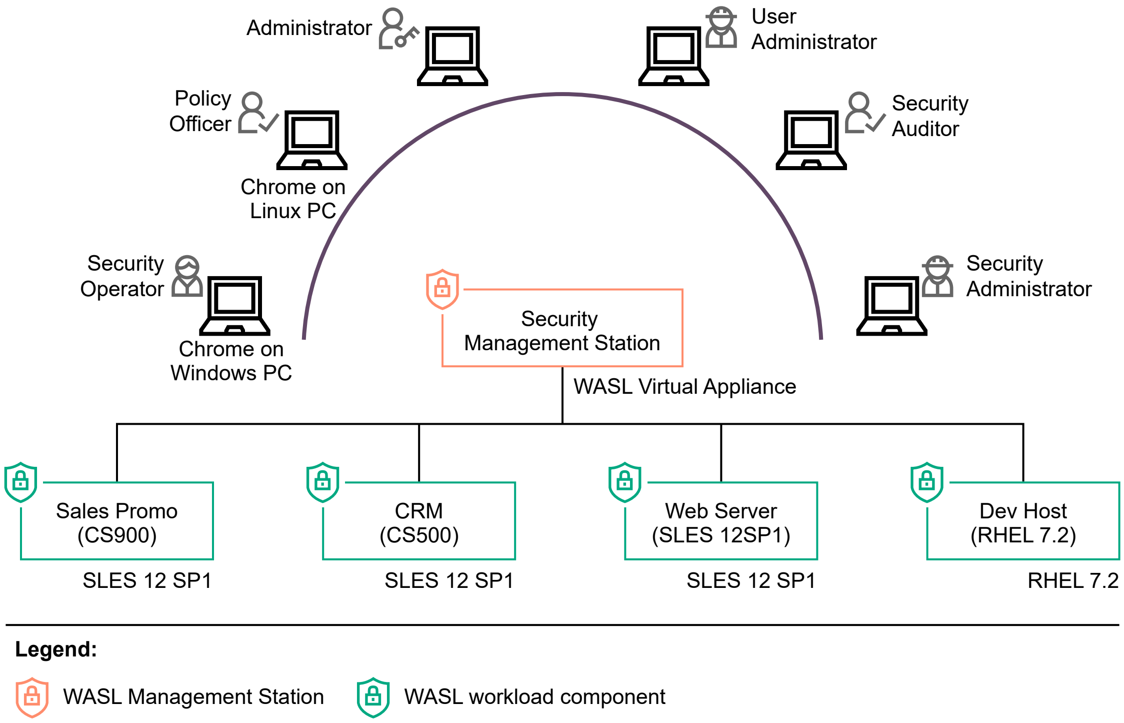

Figure 1: WASL Deployment Scenario

Multiple workloads that must be secured can be registered in the SMS. SMS communicates using secure shell tunnel to the Node (or system) running the workload. It manages the workloads - starting with registration including WASL Core packages deployment and installation; to securing the workloads on an ongoing basis. SMS can be accessed from a chrome browser on a client machine.

Compatibility and installation requirements

There are pre-installation requirements in-order to set up WASL SMS and the nodes (that run the workloads) that must be secured.

Security Management Station (SMS)

WASL version 1.3.0 is released as a virtual appliance and is supported on VMWare vSphere ESXi hypervisor.

The following configurations are required to host the WASL virtual appliance:

Items	Requirement
Hardware	• HPE ProLiant Rack-Optimized servers (DL Servers) • HPE ProLiant Blade Servers (BL Servers) • HPE Mission Critical x86 Servers such as HPE Superdome X and MC990 X Server For a detailed list of supported servers, see *WASL Quick Specs*.
Memory	Minimum 16 GB (increase based on the number of planned workloads and operations).
CPUs	4 X 4GHz or greater virtual CPUs
Disk requirement	40 GB minimum (thick-provisioned disk space) **NOTE:** The disk space requirement is based on the number of workloads and the operations performed. Based on this, the disk space must be provisioned accordingly. Each evaluation or remediation operation requires approximately 5 MB of disk space to store the reports. 40 GB of disk space can then store up to 8,000 reports of evaluation or remediation operations. To increase the disk space, follow the instructions mentioned in the corresponding *HPE WASL Install and Setup Guide*.
Hypervisors	VMware vSphere 6.0, 6.5, 6.7

Node

The target node to secure must have the WASL Node packages that include all the required and dependent products for securing the individual workloads. The Node Packages can either be installed from SMS GUI or installed separately (manually) on the target node.

The following are the requirements for installing Node Packages:

Items	Requirement
Hardware	• HPE ProLiant Rack-Optimized servers (DL Servers) • HPE ProLiant Blade Servers (BL Servers) • HPE Mission Critical x86 Servers such as HPE Superdome X and MC990 X Server • HPE ConvergedSystem 900, HPE ConvergedSystem 500, and Tailored Data Center Integration solutions for SAP HANA For a detailed list of supported servers, see the *WASL Quick Specs*.
Operating System	• SUSE Linux Enterprise Server 12 (SP1, SP2, SP3, and SP4) • SUSE Linux Enterprise Server for SAP Applications 12 (SP1, SP2, SP3, and SP4) • SUSE Linux Enterprise Server 15 • SUSE Linux Enterprise Server for SAP Applications 15 • Red Hat Enterprise Linux 7 (7.2, 7.3 , 7.4, 7.5, and 7.6)

Table Continued

Items	Requirement
List of software that is required for WASL base scripts	Multiple packages such as python, OpenSSH, libopenssl, gconf2, libstdc++; are part of base operating system. If these packages are not available on the target Node, install them.
List of software that is required for Operating System security	Multiple packages such as perl-base (on SLES), perl (on RHEL), audit, sed, gawk, and so on, are part of base operating system.
Software packages required for SAP HANA security	• One of the following SAP HANA Database version is required: ◦ SAP HANA 1.0 SPS11 ◦ SAP HANA 1.0 SPS12 ◦ SAP HANA 2.0 SPS00 ◦ SAP HANA 2.0 SPS01 ◦ SAP HANA 2.0 SPS02 ◦ SAP HANA 2.0 SPS03 • SAP HANA Client - HDB_CLIENT provided with SAP HANA database WASL product uses SAP HANA Client tool -`HDB_CLIENT` that is part of SAP HANA database to connect with the SAP HANA database. WASL searches for this tool either at `/usr/sap/hdbclient` or `/home/waslhanauser/sap/hdbclient` location. If `HDB_CLIENT` tool is not installed in any of these locations, then WASL can ssh to SAP HANA System as OS admin user (`<sid>adm`) and use the `HDB_CLIENT` ttool accessible only to `<sid>adm` user. For more information, see **Add or Register Workload** section of *WASL User Guide*. On SLES for SAP Applications 15, python-enum34 package is not included in the base operating system. It needs to be installed on the target node to perform the security operations using SAP HANA policies on SLES 15.

Browser requirement

Use Chrome Version 62.0.3202.94 or above to access WASL Security Management Station (SMS).

Installation Instructions

Refer to the installation and setup instructions available in the *HPE Workload Aware Security for Linux Version Install and Setup Guide* in-order to install and setup WASL SMS and nodes.

Recommendations

Backup the Encryption Root Keys

The SAP HANA database policies include several rules that enable encryption of data, redo logs, and data backup. There are also rules to check the encryption root keys and the master keys of the Instance Secure Store in the File System (SSFS) and the System Public Key Infrastructure SSFS. When the encryption features of SAP HANA are enabled, ensure that the encryption root keys are backed up. If the encryption root keys are not backed up, the data might become irrecoverable.

The encryption root keys for both the system database and all the tenant databases must be backed up. The backup must be done during the initial installation and whenever there is a change or addition of root keys. The change or addition of the root keys can happen in scenarios like creating a new tenant database, manually changing the root keys, and so on.

NOTE: It is recommended that the encryption settings are tested in the SAP HANA test environments, before enabling in production. Testing is highly recommended for backup and recovery operations (on two different systems) and for testing disaster recovery capability.

SAP HANA 2.0: To perform the encryption root keys backup for SAP HANA 2.0, see the sections *Change Encryption Root Keys*, *Back Up Root Keys*, and *Set the Root Key Backup Password* in the *SAP HANA Administrator Guide*. You can also see *SAP Note 2444090 - FAQ: SAP HANA Backup Encryption* to get more information.

SAP HANA 1.0: To perform encryption root keys backup for SAP HANA 1.0, backup the SSFS file and key file. For more information, see *SAP Note 2524649 - Backup Encryption Root Key*.

For more information on different encryption rules and creating a backup of the root keys for WASL 1.3.0, see the following customer advisory:

https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00090851en_us.

Known problems and workaround

Install and setup

1. **Issue**: Terminal does not echo input characters after starting the SMS service.

   Workaround: This issue may occur if the user terminates the `wasl_sms.sh` command with Control-C signal while entering the master password. Enable the echo on the terminal using `stty echo` command on the same session.

2. **Issue**: The reset password (`wasl_sms.sh -reset_password`) tool crashes while creating a recovery user, if a Couchbase Server bucket password reset was done in the same session earlier.

   Workaround: Create recovery user using reset password tool (`wasl_sms.sh -reset_password`) in a new session.

3. **Issue**: Reset password tool (`wasl_sms.sh -reset_password`) crashes during master password or recovery password reset operation, if Couchbase Server bucket is not accessible.

   Workaround: Ensure the SMS configuration (Couchbase Server URL and bucket name) is valid and Couchbase Server is serving the bucket at the URL.

Workload

1. **Issue**: System Compliance Score and Application Compliance Score meters on the Workload Details page are not updated after reset and rollback operations.

   Workaround: Perform an evaluation (or a remediation) operation to update the compliance scores.

2. **Issue**: Workload `Edit` operation fails if the workload type is changed.

   Workaround: Disable the existing workload and register a new workload with required workload type instead of changing it.

3. **Issue:** Slow response from Couchbase Server, causes the SMS into an unexpected state.

   Workaround: Ensure that the Couchbase service has adequate resources (CPU and memory) allocated to it.

Settings

Issue: If the SMS admin account password is lost, it cannot be recovered.

Workaround: Create **`User Administrator`** role user. Any user with this role can reset the admin password by logging in.

Miscellaneous

Issue: In the search box across all the pages, using upper-case letters in the search strings do not result in any output.

Workaround: Use lower-case letters during search.

Node

Issue: In RHEL 7.3, sshd service might stop during multiple remediation and rollbacks of OS security profiles.

Workaround: This is due to a bug in OpenSSH mentioned on **https://bugzilla.redhat.com/show_bug.cgi?id=1381997**. Updating OpenSSH to 7.4p1-1 version or higher addresses this issue.

Limitations

Install and setup

Backspace is not honored, while entering Couchbase password. If a wrong value is provided for the password field, retry the operation.

Policy

WASL by default, does not provide rollback operation for user-defined policies. The users may create the snapshot and rollback APIs for the user-defined policies based on the policy customization steps.

Settings

The browser `Back` button does not work if the user tries to access unauthorized URL by entering the URL directly in the address bar.

Miscellaneous

In the search box, special character search does not work.

Node

1. In **SAP HANA DB** policies, rollback will not happen for the following rule: "PERSISTENCE_ENCRYPTION_KEYS must be within timeout". This rule checks different encryption keys used for data page encryptions. If these keys are old, then a new key will be requested to SAP HANA database by this rule remediation. Once a new key is generated, SAP HANA database will start using it and will not allow using old keys for encrypting data pages.
2. In **OS Security** policies, the remediation and rollback may not happen for rules modifying audit records in memory. This will be due to audit immutable flag (-e 2) turned on, which restricts any change to the audit records in memory. The **OS Security** policies have rule that modifies static audit files which makes similar changes, as the rules that modify audit records in memory. These audit records in memory will be remediated or rolled back only when the system is rebooted.

For more information on troubleshooting steps on install, setup, and operations, see the *HPE WASLTroubleshooting Guide*.

NOTE: For information about the latest updates on the product, see the WASL product page at HPE Software Depot: **https://h20392.www2.hpe.com/portal/swdepot/displayProductsList.do?category=LNXMCSW**.

References

For latest information on the WASL product, see the list of documentation by navigating to WASL under Mission Critical x86 Software at HPE Software Depot, or view the following page at **https://h20392.www2.hpe.com/portal/swdepot/displayProductsList.do?category=LNXMCSW**.

- HPE WASL User Guide
- HPE WASL Install and Setup Guide
- HPE WASL Troubleshooting Guide
- HPE WASL Online help is accessible from the SMS interface

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

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

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

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

Information to collect

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

Accessing updates

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

  Hewlett Packard Enterprise Support Center

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

  Hewlett Packard Enterprise Support Center: Software downloads

  https://www.hpe.com/support/downloads

  Software Depot

  https://www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

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

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

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

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

Remote support

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

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

Remote support and Proactive Care information

HPE Get Connected

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

HPE Proactive Care services

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

HPE Datacenter Care services

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

HPE Proactive Care service: Supported products list

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

HPE Proactive Care advanced service: Supported products list

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

Proactive Care customer information

Proactive Care central

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

Proactive Care service activation

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

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

https://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

https://www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

https://www.hpe.com/support/Storage-Warranties

HPE Networking Products

https://www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

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

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

https://www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

https://www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

https://www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.