Abstract
This document describes about HPE WASL 1.3.1, its features, known issues, and the installation requirements.
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.


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

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>P25505-001</td>
<td>December 2019</td>
</tr>
<tr>
<td>P12138-002a</td>
<td>November 2019</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Part Number</th>
<th>Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>P12138-002</td>
<td>June 2019</td>
</tr>
<tr>
<td>P12138-001</td>
<td>December 2018</td>
</tr>
<tr>
<td>P03765-001</td>
<td>April 2018</td>
</tr>
</tbody>
</table>
Contents

HPE WASL 1.3.1.................................................................................................................. 6
  Introduction..................................................................................................................... 6
  What's new in HPE WASL 1.3.1.................................................................................. 6
  What's new in HPE WASL 1.3.0.................................................................................. 6
  What's new in HPE WASL 1.2.0.................................................................................. 7
  HPE WASL features..................................................................................................... 7
    Evaluation................................................................................................................... 7
    Remediation............................................................................................................... 7
    Rollback................................................................................................................... 8
    Security Policies....................................................................................................... 8
    License Information................................................................................................. 9

WASL Installation and Setup......................................................................................... 10
  Overview..................................................................................................................... 10
  Compatibility and installation requirements................................................................ 10
    Security Management Station (SMS)....................................................................... 10
    Node......................................................................................................................... 11
    Browser requirement............................................................................................... 14
  Installation Instructions............................................................................................. 14
  Migration to WASL 1.3.1......................................................................................... 14

Recommendations....................................................................................................... 15
  Backup the Encryption Root Keys............................................................................. 15

Known problems and workaround............................................................................. 17
  Install and setup........................................................................................................ 17
  Workload.................................................................................................................... 17
  Settings...................................................................................................................... 17
  Miscellaneous............................................................................................................ 17
  Node............................................................................................................................ 18

Limitations.................................................................................................................... 19
  Install and setup........................................................................................................ 19
  Policy........................................................................................................................ 19
  Settings...................................................................................................................... 19
  Miscellaneous............................................................................................................ 19
  Node............................................................................................................................ 19

Documentation Addendum......................................................................................... 21
  Migrating to WASL Virtual Appliance Version 1.2 or later...................................... 21
  Backup WASL SMS Virtual Appliance Version 1.1................................................. 21
  Backup WASL SMS Virtual Appliance Version 1.2 or later.................................. 23
  Migrating to WASL Version 1.2 or later.................................................................. 25
HPE WASL 1.3.1

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 1.3.1

Support for SAP HANA 2.0 SPS04 database

The WASL 1.3.1 Node packages support operations on SAP HANA 2.0 SPS04 database. This WASL version also ships the following new policies to secure SAP HANA 2.0 SPS04 system database:

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

WASL 1.3.1 defect fixes

WASL 1.3.1 includes the following defect fixes:

QXCR1001720868 - On hardening SAP HANA that enables data and backup encryption, if the encryption root keys are not backed up, recovery of data from the backup fails.

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 SUSE Linux Enterprise Server (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.
**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 1.3.1 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\(^1\)
- OS Security extras for SAP HANA - update 1\(^2\)
- Draft OS Security Level 1 for SLES 15\(^2\)
- Draft OS Security Level 2 for SLES 15\(^2\)
- Draft OS Security Level 1 for SLES for SAP Applications 15\(^2\)
- Draft OS Security Level 2 for SLES for SAP Applications 15\(^2\)

SAP HANA Database Policies

The following policies are updated to include the fix for defect QXCR1001720868 in HPE WASL 1.3.1:

- SAP HANA 1.0 DB Security Level 1
- SAP HANA 1.0 DB Security - Level 2
- SAP HANA 2.0 DB Security - Level 1\(^1\)
- SAP HANA 2.0 DB Security - Level 1 - update 1\(^2\)
- SAP HANA 2.0 DB Security - Level 2\(^1\)
- SAP HANA 2.0 DB Security - Level 2 - update 1\(^2\)
- SAP HANA 2.0 DB Security - Level 1 - update 2\(^3\)
- SAP HANA 2.0 DB Security - Level 2 - update 2\(^3\)

RHEL Policies

---

1 Deprecated from WASL version 1.3.0 and later
2 Policies added in WASL version 1.3.0 and later
3 Policies added in WASL version 1.3.1 and later
• OS Security Level 1 for RHEL 7
• OS Security Level 2 for RHEL 7

**WASL SMS Virtual Appliance policy**

OS Security policy for WASL SMS 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 1.3.1 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:
<table>
<thead>
<tr>
<th>Items</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>• HPE ProLiant Rack-Optimized servers (DL Servers)</td>
</tr>
<tr>
<td></td>
<td>• HPE ProLiant Blade Servers (BL Servers)</td>
</tr>
<tr>
<td></td>
<td>• HPE Mission Critical x86 Servers such as HPE Superdome X and MC990 X Server</td>
</tr>
<tr>
<td></td>
<td>For a detailed list of supported servers, see <em>HPE Workload Aware Security for Linux QuickSpecs.</em></td>
</tr>
<tr>
<td>Memory</td>
<td>Minimum 16 GB (increase based on the number of planned workloads and operations).</td>
</tr>
<tr>
<td>CPUs</td>
<td>4 X 4GHz or greater virtual CPUs</td>
</tr>
<tr>
<td>Disk requirement</td>
<td>40 GB minimum (thick-provisioned disk space)</td>
</tr>
</tbody>
</table>

**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 Workload Aware Security for Linux 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:
<table>
<thead>
<tr>
<th>Items</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>• HPE ProLiant Rack-Optimized servers (DL Servers)</td>
</tr>
<tr>
<td></td>
<td>• HPE ProLiant Blade Servers (BL Servers)</td>
</tr>
<tr>
<td></td>
<td>• HPE Mission Critical x86 Servers such as HPE Superdome X and MC990 X Server</td>
</tr>
<tr>
<td></td>
<td>• HPE ConvergedSystem 900, HPE ConvergedSystem 500, and Tailored Data Center Integration solutions for SAP HANA</td>
</tr>
</tbody>
</table>

For a detailed list of supported servers, see the *HPE Workload Aware Security for Linux QuickSpecs*.

| Operating System               | • SUSE Linux Enterprise Server (SLES) 12 (SP1, SP2, SP3, and SP4 versions only) ¹ |
|                               | • SUSE Linux Enterprise Server for SAP Applications 12 (SP1, SP2, SP3, and SP4 versions only) ¹ |
|                               | • SUSE Linux Enterprise Server 15 ¹                                           |
|                               | • SUSE Linux Enterprise Server for SAP Applications 15 ¹                      |
|                               | • Red Hat Enterprise Linux 7 (7.2, 7.3, 7.4, 7.5, and 7.6 versions only) ¹    |

**List of software that is required for WASL base scripts**

Multiple packages such as python, different python2 modules, OpenSSH, libopenssl, gconf2, libstdc++ are part of the base operating system. If these packages are not available on the target Node, install them.

*Table Continued*
<table>
<thead>
<tr>
<th>Items</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of software that is required for operating system security</td>
<td>Multiple packages such as perl-base (on SLES), perl (on RHEL), audit, sed, gawk, python, python 2 modules, and so on, are part of the base operating system.</td>
</tr>
<tr>
<td>Software database packages required for SAP HANA security (SAP HANA Database Security policies are supported on SUSE Linux Enterprise Server (SLES) for SAP applications operating system.)</td>
<td>• One of the following versions of SAP HANA database is required:</td>
</tr>
<tr>
<td></td>
<td>◦ SAP HANA 1.0 SPS12 2</td>
</tr>
<tr>
<td></td>
<td>◦ SAP HANA 2.0 SPS02 2</td>
</tr>
<tr>
<td></td>
<td>◦ SAP HANA 2.0 SPS03 2</td>
</tr>
<tr>
<td></td>
<td>◦ SAP HANA 2.0 SPS04 2</td>
</tr>
<tr>
<td></td>
<td>• SAP HANA Client - HDB_CLIENT provided with SAP HANA database. WASL product uses SAP HANA Client - HDB_CLIENT tool provided along with the 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, WASL connects as SAP HANA OS admin user ( &lt;sid&gt;adm) for all WASL operations and searches for HDB_CLIENT tool in different locations. For more information, see Add or Register Workload section in the HPE Workload Aware Security for Linux User Guide.</td>
</tr>
<tr>
<td></td>
<td>NOTE: For SAP HANA Client 2.0 SPS04, install the HDB_client at /usr/sap/hdbclient location. After installing HDB_CLIENT, install the python drivers using the following command:</td>
</tr>
<tr>
<td></td>
<td># cd /usr/sap/hdbclient</td>
</tr>
<tr>
<td></td>
<td>#/usr/bin/easy_install-2.7 hdbcli-&lt;n.n.n&gt;.tar.gz</td>
</tr>
<tr>
<td></td>
<td>(The &lt;n.n.n&gt; maps to the actual version number, say hdbcli-2.4.126.tar.gz)</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/easy_install-2.7 is provided as part of python-setuptools RPM package on SLES 12 and python2-setuptools RPM package as a part of SLES 15. Install this package, if it is not already installed on the system.</td>
</tr>
<tr>
<td></td>
<td>If you encounter an error while installing the python drivers, see the Node section under Known problems and workaround. For more information, see Install the Python Driver section in the SAP HANA Client Interface Programming Reference for SAP HANA Platform.</td>
</tr>
<tr>
<td></td>
<td>• On SLES for SAP Applications 15, python-enum34 package is not included in the base operating system. It must be installed on the target node to perform the security operations using SAP HANA policies on SLES 15.</td>
</tr>
</tbody>
</table>

1 The last date of WASL support for the Operating System version is the earliest end of support by either OS vendor or HPE support.

2 The last date of WASL support for the SAP HANA database version is the earliest end of support by either SAP® or HPE support.
**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 Install and Setup Guide* in order to install and setup WASL SMS and nodes.

**Migration to WASL 1.3.1**

The following default policies are updated in WASL 1.3.1:

- 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

The following default policies are newly added in WASL 1.3.1:

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

To get the latest updates available in WASL 1.3.1, migrate from the earlier versions to WASL 1.3.1. For information about the WASL SMS data migration, see [Documentation Addendum](#). During migration, ensure that all the policies are updated, undeployed, and deployed again, on all the workloads.
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

For SAP HANA database policies version 1.3.1 and later, the following changes are added to the rules to check or enable the encryption features: (See the evaluation report of SAP HANA database 1.3.1 version of policy under Protecting data at rest group for more details.)

- The rules will check if the encryption root keys are backed up.

  On SAP HANA 2.0 SPS02 and later, the rules check if the encryption root keys are backed up using the SYS_DATABASES.ENCRYPTION_ROOT_KEYS database view. During evaluation or remediation operation, if the encryption keys are not backed up, the rules return an ERROR status.

  On the earlier versions of SAP HANA database, by default these rules return an ERROR status.

To override this check, create a custom policy and redefine the confirm_ssfs_root_keys_backed_up XCCDF variable to true.

**NOTE:** The rules identify if the encryption root keys are backed up on SAP HANA 2.0 SPS02 and later. However, the encryption root keys must be securely stored on a different remote system. Remember the corresponding root key backup passwords for backup recovery. The rules cannot identify whether the encryption root keys are securely stored in different systems as this is a manual process.

- For encryption rules that support remediation, new XCCDF variables are added to each rule to stop remediation of the rules, by default.

  These rules return an ERROR status on remediation. See the documentation in the evaluation report of these rules to identify the XCCDF variables. To start remediation, create a custom profile and redefine the specific XCCDF variable to true.
Ensure that all the SAP HANA database policies deployed on all the workloads are migrated to WASL 1.3.1 or later to get the latest rule changes.
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.
1. **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](https://bugzilla.redhat.com/show_bug.cgi?id=1381997). Updating OpenSSH to 7.4p1-1 version or higher addresses this issue.

2. **Issue:** When trying to install the hdbcli python drivers for SAP HANA 2.0 SPS04 or later using the `easy_install` command, the following error is displayed:

   This hdbcli installer is not compatible with your Python interpreter.

   **Workaround:** Use the following steps to install the hdbcli python drivers by extracting the python drivers `hdbcli-<n.n.n>.tar.gz`:
   
   a. **Extract** `hdbcli-<n.n.n>.tar.gz`.
      
      This command creates a new folder `hdbcli-<n.n.n>`. The `<n.n.n>` maps to the actual version number, say `hdbcli-2.4.126.tar.gz`.
      
      **Example:**
      
      #tar -xzvf hdbcli-2.4.126.tar.gz
   
   b. **Check umask of the terminal session.**
      
      **NOTE:** Ensure that the umask value provides read and execute permissions to all the users (for example, umask value 0022). With the umask value, the python drivers allow all the users to access it.
      
      **Example:**
      
      #umask 0022
   
   c. **Install the python drivers using the extracted directory** `hdbcli-<n.n.n>`.
      
      **Example:**
      
      #/usr/bin/easy_install-2.7 hdbcli-2.4.126
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

Securing SAP HANA Database

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 the SAP HANA database by this rule remediation. Once a new key is generated, the SAP HANA database will start using it and will not allow using old keys for encrypting data pages.

2. SAP HANA 2.0 SPS04 supports storing encryption keys in a separate lightweight Local Secure Store (LSS) on non-production systems. WASL SAP HANA policies are not supported on this configuration.

   **NOTE:** Do not use SAP HANA 2.0 SPS04 policies on the system configured with LSS.

3. WASL currently connects to the system database on SAP HANA and performs evaluation or remediation of different security parameters. It does not directly connect to the tenant databases to secure its parameter. In many cases, the tenant database uses the ini file security configuration provided in the system database as the default configuration. A Tenant Administrator can, however, change some of these parameters if the parameters are not blacklisted in the multidb.ini file.

4. In the SAP HANA 2.0 SPS04, audit policies can be created on different tenant databases from the system database using the SAP HANA Cockpit tool. In the previous versions of SAP HANA database, the creation of these audit policies on the tenant database is not possible from the system database. WASL does not support creating audit policies on the tenant databases for all versions of the SAP HANA database.

5. WASL currently connects to the system database on SAP HANA and performs evaluation or remediation of different security parameters. In many cases, newly created tenant databases attempt to inherit the system database settings. On performing a rollback of WASL SAP HANA policy, the changes inherited by the tenant database are not rolled back.

   **Example 1:**
The newly created tenant database on SAP HANA 2.0 SPS02 and earlier versions inherit the encryption settings of the system database enabled by the following rules:

- Data at rest is encrypted (Rule ID: xccdf_com.hpe.wasl.data_mpersistence_1)
- Redo logs should be encrypted (Rule ID: xccdf_com.hpe.wasl.data_redolog_enable_encryption)
- Backup encryption should be enabled (Rule ID: xccdf_com.hpe.wasl.data_backup_enable_encryption)

On performing a rollback, the encryption status of the newly created tenant database is not modified. However, during remediation, only the system database configuration changes done by the rules are rolled back.

**Example 2:**

The newly created tenant database on SAP HANA 2.0 SPS03 and later versions has encryption enabled that is based on the system database configuration. This system database configuration is set by the following rules:

- Initial database data volume encryption is enabled (Rule ID: xccdf_com.hpe.wasl.database_initial_persistence_encryption)
- Initial database redo log encryption is enabled (Rule ID: xccdf_com.hpe.wasl.database_initial_log_encryption)
- Initial database backup encryption is enabled (Rule ID: xccdf_com.hpe.wasl.database_initial_backup_encryption)

On performing a rollback, the encryption status of the newly created tenant database is not modified. However, during remediation, only the system database configuration changes done by the rules are rolled back.

6. On performing remediation of Data at rest is encrypted rule, the rule PERSISTENCE_ENCRYPTION_KEYS should be within timeout is shown as FIXED. This happens because the process of enabling the data encryption triggers SAP HANA database to auto-generate a persistence encryption key.

**Securing Operating System**

In OS Security policies, the remediation and rollback may not happen for rules that modify 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 include rules that modify the static audit files, which make similar changes like the rules that modify audit records in memory. These audit records in memory are remediated or rolled back only when the system is rebooted.

For more information on troubleshooting steps on install, setup, and operations, see the HPE Workload Aware Security for Linux Troubleshooting 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.
The following section provides information about migrating to WASL Virtual Appliance version 1.2 or later, and is not yet updated in the *HPE Workload Aware Security for Linux Install and Setup Guide*. The following procedure is also applicable to migrate to WASL 1.3.1 from the earlier versions.

### Migrating to WASL Virtual Appliance Version 1.2 or later

To migrate the SMS data from the old version of WASL SMS Virtual Appliance to the current version:

1. Create a new WASL SMS Virtual Appliance.
   
   For more information, see *Deploy WASL SMS Virtual Appliance* section in the *HPE Workload Aware Security for Linux Install and Setup Guide*.

2. Setup this new WASL SMS Virtual Appliance with a new master key.
   
   **NOTE:** The final migrated data is encrypted using this new master key. Remember the master password used for the new SMS Virtual Appliance.

3. Backup the WASL SMS data from the old version.
   
   Depending on the WASL SMS version you want to backup, you can create a backup using one of the following methods:

   - *Backup WASL SMS Virtual Appliance Version 1.1*
   - *Backup WASL SMS Virtual Appliance Version 1.2 or later*

4. **Migrate to WASL SMS Virtual Appliance Version 1.2 or later.**

5. **Update the policies to the latest version.**

6. **Update the policies on each of the workloads to the latest version.**

### Backup WASL SMS Virtual Appliance Version 1.1

To protect the critical data from being lost due to an untimely event, you must backup the data:

**Prerequisites**

Ensure that the WASL SMS is up and running.

**Procedure**

1. Mount the WASL ISO, and run the following command to install the MISC/SLES/SLES11hpe-waslsms-backup-1.1.0-1.x86_64.rpm.

   ```
   # zypper install hpe-wasl-sms-backup-1.1.0-1.x86_64.rpm
   ```

2. Log in to the new WASL SMS Virtual Appliance as **wasladmin** user.

3. Run the following command to stop SMS:

   ```
   # /opt/hpe/wasl/sms/tools/wasl_sms.sh -stop
   ```
4. Run the following command to create backup:

```
# /opt/hpe/wasl/sms/tools/wasl_backup.sh -create_backup -description <description_text>
```

**NOTE:** The `-create_backup` option supports different types of backup such as reports backup only, logs nbackup only and so on. HPE recommends using `-type all` option.

Example:

```
# /opt/hpe/wasl/sms/tools/wasl_backup.sh -create_backup -description Backup1
```

5. Type **Yes** to continue.

The backup is created successfully.

The backup data is saved in the `<BACKUP>.ebck` and `<BACKUP>.json` files. The backup filename and location are displayed on the screen.

6. Run the following command to display the list of all backup files:

```
# sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -list_backup
```

The latest backup along with the description is listed at the end of the backup list.

**Example:**

Run the following command to display a specific backup file:

```
# /opt/hpe/wasl/sms/tools/wasl_backup.sh -list_backup -name 2018-12-3T12-56-55_all_WASLSMS.ebck
```

The following output is displayed:

```
2018-12-3T12-56-55_all_WASLSMS.ebck
```

The system displays the location (`/var/opt/hpe/wasl/sms/backup`) of the backup data.

7. Run the following command to list the created files:

```
# ls -l /var/opt/hpe/wasl/sms/backup/<filename>_all_WASLSMS.*
```

**Example:**

```
# ls -l /var/opt/hpe/wasl/sms/backup/2018-12-3T12-56-55_all_WASLSMS.*
```

The output of the above example displays the following files:

- `rw-r--r-- 1 waslsms waslsms 53783104 Dec 3 12:57 /var/opt/hpe/wasl/sms/backup/2018-12-3T12-56-55_all_WASLSMS.ebck`
- `rw-r--r-- 1 waslsms waslsms 317 Dec 3 12:56 /var/opt/hpe/wasl/sms/backup/2018-12-3T12-56-55_all_WASLSMS.json`

8. Copy `.ebck` and `.json` files to the new installation of WASL SMS Virtual Appliance 1.2 or later for restoration.
NOTE:

- The stash file is not backed up. You need to back up the stash file (/opt/hpe/wasl/sms/data/stashfile) separately. This file contains the master password. To restore the backup, you must either remember the master password, or provide the stash file (/opt/hpe/wasl/sms/data/stashfile).

- If you have forgotten the master password, you can also reset the master password before backing up the data. For resetting the password, run the following command:

  # /opt/hpe/wasl/sms/tools/wasl_sms.sh -reset_password

- Restoration is possible only on WASL SMS Virtual Appliance version 1.2 or later.

Example:

To copy the backup files from the old WASL SMS Virtual Appliance to the new WASL SMS Virtual Appliance:

a. Navigate to the directory where the old backup files are stored:
   
   cd /var/opt/hpe/wasl/sms/backup/

b. Run the following command for transferring the backup files to the new WASL SMS Virtual Appliance:
   
   scp 2018-12-3T12-56-55_all_WASLSMS.ebck wasladmin@192.x.x.x:/var/opt/hpe/wasl/sms/backup
   
   scp 2018-12-3T12-56-55_all_WASLSMS.json wasladmin@192.x.x.x:/var/opt/hpe/wasl/sms/backup

   **NOTE:** Enter wasladmin password every time you execute the `scp` command.

9. To restore the backup, you must either remember the master password, or backup the stash file (/opt/hpe/wasl/sms/data/stashfile) separately.

10. **Migrate to WASL SMS Virtual Appliance version 1.2 or later.**

**Backup WASL SMS Virtual Appliance Version 1.2 or later**

To protect the critical data from being lost due to an untimely event, you must backup the data:

**Prerequisites**

Ensure that the WASL SMS is up and running.

**Procedure**

1. Log in to the WASL SMS Virtual Appliance as `wasladmin` user.

2. Run the following command to stop WASL SMS:

   # sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -stop

3. Run the following command to create a backup:

   # sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -create_backup -type all -description <description_text>
NOTE: The -create_backup option supports different types of backup such as reports backup only, logs nbackup only, and so on. Hewlett Packard Enterprise recommends using -type all option.

```
Example:
# /opt/hpe/wasl/sms/tools/wasl_backup.sh -create_backup -description Backup2
```

4. Type Yes to continue.

The backup is created successfully.

The backup data is saved in the <BACKUP>.ebck and <BACKUP>.json files. The backup file name and location are displayed on the screen.

5. Run the following command to display the list of all backup files:

```
# sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -list_backup
```

The latest backup along with the description is listed at the end of the backup list.

```
Example:
Run the following command to display a specific backup file:

# sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -list_backup -name 2018-12-3T15-9-19_all_WASLSMS.ebck
```

The following output is displayed:

```
2018-12-3T15-9-19_all_WASLSMS.ebck
```

The system displays the location (/var/opt/hpe/wasl/sms/backup) of the backup data.

6. Run the following command to list the created files:

```
# ls -l /var/opt/hpe/wasl/sms/backup/<filename>_all_WASLSMS.*
```

```
Example:
# ls -l /var/opt/hpe/wasl/sms/backup/2018-12-3T15-9-19_all_WASLSMS.*
```

The output of the above example displays the following files:

- `rw-r--r--. 1 waslsms waslsms 49016144 Dec 3 15:09 /var/opt/hpe/wasl/sms/backup/2018-12-3T15-9-19_all_WASLSMS.ebck`
- `rw-r--r--. 1 waslsms waslsms 306 Dec 3 15:09 /var/opt/hpe/wasl/sms/backup/2018-12-3T15-9-19_all_WASLSMS.json`

7. Copy the .ebck and .json backup files to the new installation of WASL SMS Virtual Appliance 1.2 or later for restoration.
NOTE:

- The stash file is not backed up. You need to back up the stash file (/opt/hpe/wasl/sms/data/stashfile) separately. This file contains the master password. To restore the backup, you must either remember the master password, or provide the stash file (/opt/hpe/wasl/sms/data/stashfile).

- If you have forgotten the master password, you can also reset the master password before backing up the data. For resetting the password, run the following command:
  
  # /opt/hpe/wasl/sms/tools/wasl_sms.sh -reset_password

- Restoration is possible only on WASL SMS Virtual Appliance version 1.2 or later.

Example:

To copy the backup files from the old WASL SMS Virtual Appliance to the new WASL SMS Virtual Appliance:

a. Navigate to the directory where the old backup files are stored:
   
   cd /var/opt/hpe/wasl/sms/backup/

b. Run the following command for transferring the backup files to the new WASL SMS Virtual Appliance:
   
   scp 2018-12-3T12-56-55_all_WASLSMS.ebck
   wasladmin@192.x.x.x:/var/opt/hpe/wasl/sms/backup

   scp 2018-12-3T12-56-55_all_WASLSMS.json
   wasladmin@192.x.x.x:/var/opt/hpe/wasl/sms/backup

   **NOTE:** Enter wasladmin password every time you execute the `scp` command.

8. To restore the backup, you must either remember the master password, or backup the stash file (/opt/hpe/wasl/sms/data/stashfile) separately.

9. **Migrate to WASL SMS Virtual Appliance Version 1.2 or later.**

Migrating to WASL Version 1.2 or later

**Prerequisites**

1. Create a new WASL SMS Virtual Appliance. HPE recommends restoring WASL SMS on a fresh setup.

2. Copy `<BACKUP>.ebck` and `<BACKUP>.json` backup files to `/var/opt/hpe/wasl/sms/backup/` directory on the target WASL SMS Virtual Appliance.

3. During migration, the master password for `<BACKUP>.ebck` and `<BACKUP>.json` backup files must be provided, or the stashfile, which is backed up separately, must be copied to the `/var/opt/hpe/wasl/sms/backup/stashfile_backup` file.
4. Change the group owner of these copied files to `waslms`.

   - Run the following command `# chgrp waslms <filename>` to change the group:
     
     ```
     # chgrp waslms /var/opt/hpe/wasl/sms/backup/<BACKUP>.ebck
     # chgrp waslms /var/opt/hpe/wasl/sms/backup/<BACKUP>.json
     # chgrp waslms /var/opt/hpe/wasl/sms/backup/stashfile_backup
     ```

5. Ensure only read access is allowed to the owner and the group using the command `chmod 440 <filename>`:

   ```
   # chmod 440 /var/opt/hpe/wasl/sms/backup/<BACKUP>.ebck
   # chmod 440 /var/opt/hpe/wasl/sms/backup/<BACKUP>.json
   # chmod 440 /var/opt/hpe/wasl/sms/backup/stashfile_backup
   ```

**Procedure**

1. Log in to the new WASL SMS Virtual Appliance as `wasladmin` user.
2. Ensure that the new WASL SMS Virtual Appliance is set up and ready.
3. Run the following command to display the list of all backup files:

   ```
   # sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -list_backup
   ```

   All the backup files are displayed in the output. The latest backup is listed at the end of this list of backup files.
4. To restore the backup, run the following command:

   ```
   # sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -restore_backup
   ```
5. Type the Backup Name, which is listed in the output of step 3.
6. To provide old master password, select one of the following options:

   - Master password configured during the backup
   - Stash file (`/var/opt/hpe/wasl/sms/backup/stashfile_backup`) saved during the backup (Ensure that you delete it after restoration).
7. Type the Master and Recovery Password for the current WASL SMS Appliance setup.

   The system restores the data successfully.

   Check `/opt/hpe/wasl/sms/config/custom_config.js` for changing the custom settings such as port on which WASL SMS is configured.

**NOTE:**

- The critical data on the restored WASL SMS Appliance is encrypted with the new Master Password and the Recovery Key configured on the current WASL SMS Appliance setup.
- If you are restoring the old WASL SMS Virtual Appliance to the new WASL SMS Virtual Appliance, the database is automatically migrated to the new WASL SMS Virtual Appliance format.

8. Once the backup is restored successfully in the new WASL SMS Virtual Appliance, the existing policies from the old backup replace the latest policies that are originally present in the new WASL SMS Virtual Appliance. To get the latest updates available on the new WASL SMS Virtual Appliance, update to the latest policies in SMS.

   For more information on updating to the latest policies in SMS, see [Updating Policies](#).
## Updating Policies

The Policy update feature allows you to update or add new policies in the SMS. The **Update** icon on the **Policies** page blinks when an update or new policy is available.

### Prerequisites

![Policies page]

### Procedure

To perform policy update:

1. Log in to SMS.

   On the **Policies** page of the SMS, if the updates are available, the **Update** icon starts blinking.

**NOTE:** Ensure that activities like evaluation, remediation, or rollback are not being performed on any of the workloads in SMS while the policies are being updated as it can result in issues.
If the **Update** icon is not blinking, log into WASL SMS Virtual Appliance through secure shell/console as `wasladmin` user and run the following command to recheck updates:

```
# sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -check_policy_updates
```

2. Click the **Update** icon to see the details of policies to be updated along with the new policies in SMS.
3. On the **Update Security Policies** page, click **Update** to add new policies and reflect the changes to the existing policies.

Once the policy update is complete, the final status is displayed.
4. Check the **Activity** page for the Policy Update status. If any issues are encountered during the update process, the Policy Update status displays "Additional Information".
Example:

Once the policy update is complete, the **Policies** page displays a list of new and updated policies. Click the **Policies** page to see the new policy **SAP HANA 2.0 DB Security Level 2 - update 2** added to the existing policy list. Click on each of the existing policies listed on the **Policies** page to identify the version updates made to each of them.

<table>
<thead>
<tr>
<th>New Policies</th>
<th>Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA 2.0 DB Security Level 1 - update 2</td>
<td>1.3.1</td>
<td>✔</td>
</tr>
<tr>
<td>SAP HANA 2.0 DB Security Level 2 - update 2</td>
<td>1.3.1</td>
<td>✔</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Updated Policies</th>
<th>From Version</th>
<th>To Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA 1.0 DB Security Level 1</td>
<td>1.3.0</td>
<td>1.3.1</td>
<td>✔</td>
</tr>
<tr>
<td>SAP HANA 2.0 DB Security Level 1</td>
<td>1.3.0</td>
<td>1.3.1</td>
<td>✔</td>
</tr>
<tr>
<td>SAP HANA 2.0 DB Security Level 1 - update 1</td>
<td>1.3.0</td>
<td>1.3.1</td>
<td>✔</td>
</tr>
<tr>
<td>SAP HANA 1.0 DB Security Level 2</td>
<td>1.3.0</td>
<td>1.3.1</td>
<td>✔</td>
</tr>
<tr>
<td>SAP HANA 2.0 DB Security Level 2</td>
<td>1.3.0</td>
<td>1.3.1</td>
<td>✔</td>
</tr>
<tr>
<td>SAP HANA 2.0 DB Security Level 2 - update 1</td>
<td>1.3.0</td>
<td>1.3.1</td>
<td>✔</td>
</tr>
</tbody>
</table>
5. After the updated policies and the new policies are successfully loaded on the SMS, the policies deployed on the workloads (end nodes) will still have the old policies. To get the latest fixes, update these deployed policies on each of the workloads.

For more information, see **Updating Deployed Policies on Workloads**.

---

**Updating Deployed Policies on Workloads**

To get the latest fixes for the deployed policies, ensure to update the latest policies and the existing policies in the WASL SMS Virtual Appliance, followed by updating the deployed policies on each of the workloads.

**Prerequisites**

**Procedure**

1. On the **Workloads** page, click the workload where the old policies are deployed. The top banner of the screen displays the following message:

   **Policy updates are available, please check "Deployed Policies."**
NOTE: This banner message does not appear for user-defined policy (custom policy) that are created when the default policies are customized and deployed on the workload.

It does not appear because the version number of the custom policy might not have incremented. In such scenarios, identify all the workloads where the custom policy is deployed and follow the steps to undeploy the custom policy and deploy that custom policy to get the latest fixes on the workload. For more information about undeploying and deploying a custom policy, see the Undeploy Policy and Deploy Policy sections in the HPE Workload Aware Security for Linux User Guide.

2. To see the policy details for a specific workload, click the arrow next to Deployed Policies section on the same page.

Example:

The policy SAP HANA 2.0 DB Security Level 1 - update 1 is deployed with the version 1.3.0 and an updated version 1.3.1 is available.

NOTE: For user-defined policies (custom policies), the policy versions might not get updated. In such cases even if you do not see any updates to the policy, undeploy the policy and deploy it again to get the latest fixes for those policies.
3. Undeploy the old policies from the workload.

HPE recommends that you install the latest WASL Node packages on the workload before deploying the updated policies.

To install the Node packages automatically:

a. Edit the workload on the Workloads page.

b. Click the Node option, and select Install Packages.

For more information, see Node packages installation and setup in the HPE Workload Aware Security for Linux Install and Setup Guide.

4. Deploy the same policies again on the workload to get the latest fixes for the policies.
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:
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.