



Hewlett Packard Enterprise

Read Before Installing

HPE Workload Aware Security for Linux (WASL) Software 1.2.0

=====
Read Before Installing
HPE Workload Aware Security for Linux (WASL) Software 1.2.0
=====

Edition: 3
Published: Jan 2019
(C) Copyright 2019 Hewlett Packard Enterprise Development LP

Confidential computer software. Valid license from HPE 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 HPE products and services are set forth in the express warranty statements accompanying such products and services.

Nothing herein must be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

Printed in Puerto Rico



Q8K93-96003

=====
Contents
=====

1. Overview
2. Supported Operating System, Server, Storage and Virtual appliance
3. Software and RPM Bundles
4. Signature Verification
5. Installation Instructions
6. Related Documentation

=====
1. Overview
=====

Introduction

HPE WASL is an easy-to-use security compliance tool designed to secure Operating System instances and Applications. It automates security compliance for SAP HANA workloads and the underlying Linux Operating System, reducing with a single click.

Centralized dashboard, WASL Security Management Station (SMS), can evaluate system compliance and perform remediation with the push of a button. WASL SMS displays overall compliance score and alerts users new policy updates.

WASL also offers rich actionable reports and log files post evaluation and recommends remediation steps. WASL provides the ability to rollback remediation action and restore the workload configuration to a pre-remediation state.

WASL uses compliance profiles built using XCCDF specification language enabling extensibility of the profile set. It currently provides the following standard profile set addressing the global benchmark standards for OS and SAP HANA application

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

Licensing Information

There are two variants of the WASL license:

- 1) WASL Basic - Designed to automate security compliance of the Linux operating system.

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

- 2) WASL Advanced - Designed for SAP HANA customer seeking SAP HANA and Linux Operating System security compliance on HPE appliances and/or TDI deployments.

Each license purchase includes 1 year of 24x7 Technical Support and Software Updates Service.

Note: All Standard profile sets are included in the HPE WASL virtual appliance. Based on the license purchased the profile will be applicable.

NOTE: For information about the latest updates on the product Refer to the WASL product page at HPE Software Depot and navigate to Linux -> Mission Critical x86 Software, or visit: <https://hpe.com/servers/wasl>

=====

2. Supported Operating System, Server, Storage and Virtual appliance

=====

HPE WASL SMS:

HPE WASL SMS is packaged and shipped as a virtual appliance (OVA format) that can be provisioned on a VMware vSphere Hypervisor 6.0, 6.5 and 6.7 versions.

WASL Nodes:

Nodes that can be registered and secured using HPE WASL should run one of the following operating system variants.

- * SUSE Linux Enterprise Server 12 (SP1, SP2, SP3)
- * SUSE Linux Enterprise Server for SAP Applications 12 (SP1 , SP2 & SP3)
- * Red Hat Enterprise Linux 7 (7.2, 7.3, 7.4, 7.5)

For detailed information on the supported Operating System, Server, Storage and virtual appliance requirements, see "HPE WASL Install and Setup Guide".

=====

3. Software and RPM Bundles

=====

The following is the list of packages bundled in the virtual appliance for the WASL SMS and the Nodes.

1. WASL SMS Virtual appliance

The following ova file can be provisioned on a VMware vSphere Hypervisor.

Q8K94-11003.ova

2. WASL SMS 1.1.0 backup package

The following rpm package is required to take a backup of WASL 1.1.0 setup. This can be installed only on SLES 11 SP4 node running WASL1.1.0 SMS.

hpe-wasl-sms-backup-1.1.0-1.x86_64.rpm

3. WASL Node packages

RHEL 7:

hpe_wasl_core-1.2.0-1.rhel7.x86_64.rpm
hpe_wasl_os-1.2.0-1.rhel7.x86_64.rpm
hpe_wasl_saphana-1.2.0-1.rhel7.x86_64.rpm
openscap_1-1.2.15-1.0.x86_64.rpm

SLES 12:

hpe_wasl_core-1.2.0-1.sles12.x86_64.rpm
hpe_wasl_os-1.2.0-1.sles12.x86_64.rpm
hpe_wasl_saphana-1.2.0-1.sles12.x86_64.rpm
openscap_1-1.2.15-1.0.x86_64.rpm

4. Signature verification

Overview

The HPE WASL Virtual appliance and node rpms are signed with private digital keys held by HPE and the integrity of the packages can be verified before installing. This ensures that the packages have not been manipulated by a third party.

Download the keys

Copy the compressed tar file (HPE-GPG-Public-Keys.tar.gz) from

the link below to your local directory.

<https://downloads.hpe.com/pub/keys/HPE-GPG-Public-Keys.tar.gz>

Transfer this keys compressed tar file to the client machine from which the WASL Virtual appliance is being deployed. In-order to verify the Node Packages, copy the tar file to the WASL Node where the node packages need to be installed.

1) WASL Virtual appliance can be verified using the GPG methodology described below.

Import the key for gpg:

Import the public keys, one at a time while logged in with an administrator account by running the following command on the host:

```
C:\Users\admin> gpg --import <Key#>.pub
```

Verifying HPE WASL Virtual appliance:

```
-----  
C:\Users\admin>gpg --verify <filename>.ova.sig <filename>.ova
```

```
<filename>.ova.sig file can be found in the same location of  
<filename>.ova file
```

Example output:

```
C:\Users\admin> gpg --verify Q8K94-11003.ova.sig Q8K94-  
11003.ova  
gpg: Signature made <Time stamp>using RSA <key ID #>  
gpg: Good signature from "Hewlett Packard Enterprise Company  
RSA-2048-48  
<signhp@hpe.com>"
```

If your file does not pass verification or you do not have the HPE public key Installed, the following error is displayed:

Example output:

```
gpg: Signature made Tue Nov 27 22:02:59 2018 IST using RSA  
key ID 78DD34EE  
gpg: Can't check signature: public key not found
```

If the verification fails, then do not use the WASL SMS virtual appliance as the file has been modified since it was released from HPE.

2) WASL Node Packages and WASL SMS 1.1.0 backup package can be verified using the RPM methodology described below.

Import the keys for RPM:

Import the public keys, one at a time while logged in as root by running the following command on the installing host:

```
# rpm --import /path_to_the_key/file_name_of_the_key
```

Example:

```
# rpm --import /path_to_the_key/B1275EA3.pub
```

Verify using RPM

Use the rpm --checksig command to validate and verify the digital signature of the signed file.

```
# rpm --checksig filename_of_the_rpm
```

The following example command output indicates the validity of the signature:

```
"filename_of_the_rpm.rpm: sha1 md5 OK"
```

If your file does not pass verification or you do not have the HPE public key installed, the following error is displayed:

Example output:

```
"sample_file.rpm: (SHA1) DSA sha1 md5 (GPG) NOT OK  
(MISSING KEYS: key#)"
```

If the verification fails, then do not install the rpm as the file has been modified since it was released from HPE.

See the following link for more details:

<https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

=====
5. Installation Instructions
=====

If you are installing HPE WASL for the first time, follow the instructions mentioned in "HPE WASL Install and Setup Guide".

=====
6. Related Documentation
=====

For the latest documentation, go to HPE Software Depot and navigate to WASL under Linux -> Mission Critical x86 Software, or visit:

<https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=WASL>

- * HPE WASL Release Notes
 - * HPE WASL User Guide
 - * HPE WASL Install and Setup Guide
 - * HPE WASL Troubleshooting Guide
- =====