Hewlett Packard
Enterprise

Read Before Installing
HPE Workload Aware Security for Linux® Basic (WASL) Software 1.1.0

==========

Read Before Installing
HPE Workload Aware Security for Linux® Basic (WASL) Software 1.1.0

==========

Edition: 2
Published: May 2018

Printed in Puerto Rico

Q8K93-96002

Introduction

HPE WASL assures security compliance to industry standards for Linux® operating system instances and for SAP HANA workloads. Automating security compliance to be as simple as a single-click on a centralized dashboard known as the WASL Security Management Station (SMS). In addition to server evaluations WASL can perform remediation for security compliance issue found in the evaluation process. WASL also offers rich actionable reports and log files from which details of evaluation issues and remediation steps are provided. WASL provides the ability to rollback any remediation done and restore the workload configuration to a pre-remediation state.

WASL uses 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

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

Package details

The HPE WASL Base license bundle contains the following products:

1. hpe-wasl-bs - HPE WASL SMS bootstrap package
   Creates the waslsms user and group for HPE WASL

2. nodejs_1-v6 - Node.js package
   NodeJS environment for HPE WASL SMS

3. hpe-wasl-npms - Node.js NPMs package
   Node.js Modules used by HPE WASL SMS

4. hpe-wasl-sms - HPE WASL SMS package
   WASL Security Management Station package

5. hpe-wasl-policies-template - HPE WASL SMS Policies Template
   Templates to register the default policies

==========
2. Supported Operating System, Server, Storage and Software
==========

WASL SMS:

SMS can be setup on a virtual machine or physical servers running:

* SUSE Linux® Enterprise Server 11 SP4.

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)
* Red Hat Enterprise Linux® 7 (7.2, 7.3, 7.4)

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

RHEL 7:

hpe_wasl_core-1.1.0-1.rhel7.x86_64.rpm
hpe_wasl_os-1.1.0-1.rhel7.x86_64.rpm
hpe_wasl_saphana-1.1.0-1.rhel7.x86_64.rpm
openscap_1-1.2.15-1.0.x86_64.rpm

SLES 12:

hpe_wasl_core-1.1.0-1.sles12.x86_64.rpm
hpe_wasl_os-1.1.0-1.sles12.x86_64.rpm
hpe_wasl_saphana-1.1.0-1.sles12.x86_64.rpm
openscap_1-1.2.15-1.0.x86_64.rpm

==========

4. Signature verification

==========

Overview

The packages 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 has not been manipulated by a third party.

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 validity of the signature:

"filename_of_the_rpm.rpm: sha1 md5 OK"

Run the following command to verify:

```
# rpm --checksig sample_file.rpm
```

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#s)"

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

==========