HPE Workload Aware Security for Linux version 1.1.0 Release Notes

Abstract

This document describes about HPE WASL 1.1.0, its features, known issues and the installation requirements.

Published: April 2018

Links to 3rd party web-site takes to outside Hewlett Packard Enterprise Development website. Hewlett Packard Enterprise Development has no control over and is not response for information outside the Hewlett Packard Enterprise Development website.

Acknowledgements

Table of Contents

Introduction 4

Key Features in HPE WASL 1.1.0 4

Evaluation 4

Remediation 4

Rollback 4

Security Policies 4

License Information 5

Basic 5

Advanced 5

WASL Installation and Setup 5

Compatibility and installation requirements 6

Security Management Station (SMS) 6

Node 7

Supported Browser 8

Installation Instructions 8

Known problems and workaround 8

Install and setup 8

Workload 8

Policy 9

Settings 9

Limitations 9

Install and setup 9

Policy 9

Settings 9

References 10

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 rollback any remediation done and restore 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. Note that the SAP HANA profiles are available only with Advance license version of the product.

Key Features in HPE WASL 1.1.0

The desired security state of a workload is defined by a set of rules which constitute 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 1.1.0 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 1.1.0 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

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 2

Policy Customization

WASL supports a methodology to customize the default and user-defined policies. It also allows to import a new profiles (that is defined as per specification) and use in 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 1 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

A typical deployment of WASL consists of a Security Management Station (SMS) and a set of workloads (Figure 1). 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.

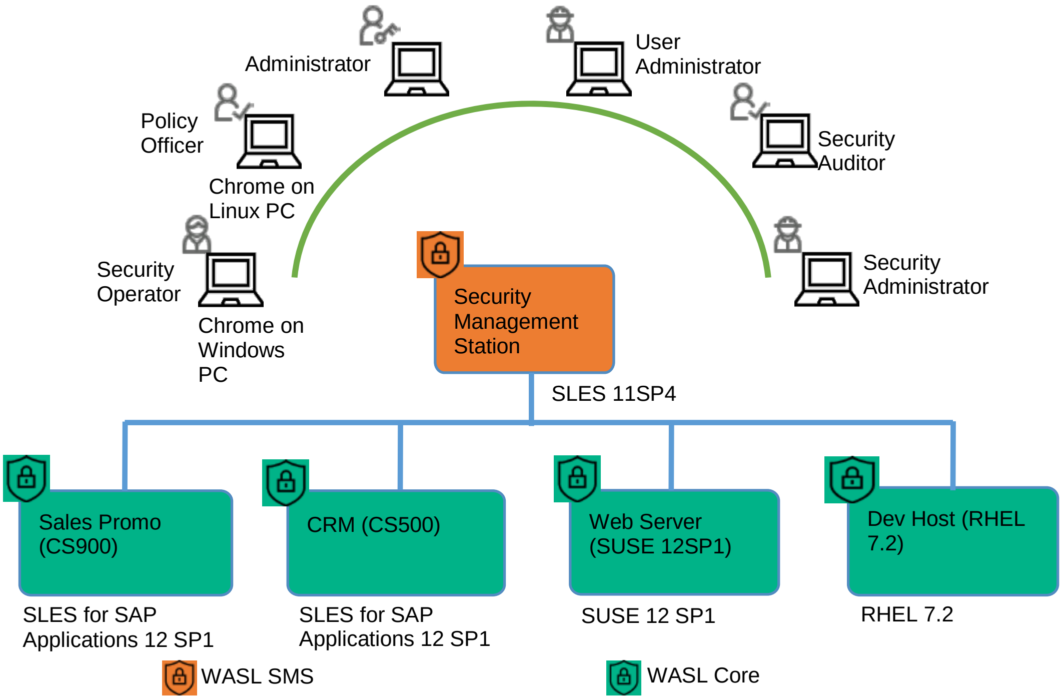

Figure 1: Typical WASL Deployment Scenario

Multiple workloads that needs to be secured can be registered in the SMS. SMS interacts with via a secure shell session 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

The following are the pre-installation requirements in-order to setup WASL SMS and the nodes (that run the workloads) that needs to be secured.

Security Management Station (SMS)

The centralized SMS can be installed on a virtual machine or a physical server based on the following requirements.

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 refer to the WASL Quick Specs.

Memory	Minimum 16 GB (increase based on the number of planned workloads and operations)
CPU's	Minimum 4 cores recommended
Disk requirement	minimum 20 GB (increase based on the number of planned workloads and operations, each evaluation and remediation operation requires ~3MB)
Operating System	SUSE Linux Enterprise Server 11 SP4

Node

The target node to secure should 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.

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 refer to the WASL Quick Specs.
Operating System	• SUSE Linux Enterprise Server 12 (SP1, SP2 and SP3) or • SUSE Linux Enterprise Server for SAP Applications 12 (SP1 and SP2) or • Red Hat Enterprise Linux 7 (7.2, 7.3 and 7.4)
List of software that are required for WASL base scripts	Install the following packages if they are not available on the target node • python-base • OpenSSH • libopenssl1_0_0 (on SUSE)
List of software that are required for Operating System security	Multiple package such as perl-base, audit, sed, gawk, etc; are part of base operating system.
Software package required for SAP HANA security	• SAP HANA Database o SAP HANA 1.0 SPS11 o SAP HANA 1.0 SPS12 o SAP HANA 2.0 SPS00 o SAP HANA 2.0 SPS01

	o SAP HANA 2.0 SPS02 • SAP HANA Client - HDB_CLIENT provided with SAP HANA database (WASL uses the client to connect to SAP HANA via Python PyDBAPI provided with SAP HANA Client in /usr/sap/hdbclient/hdbcli/dbapi.py)

Supported Browser

WASL SMS supports Google Chrome web browser with 62.0.3202.94 version and later.

Note: The recommended screen resolution can be adjusted as per viewing needs. For example with 14 inch screen laptop, 1600 X 900 screen resolution can be used.

Installation Instructions

Refer to the installation and setup instructions available in the "HPE WASL Install and Setup Guide” in-order to install and setup WASL SMS and nodes.

Known problems and workaround

This section lists the known issues and the corresponding workloads under different categories.

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.

Policy

1) **Issue:** Default policies are not listed in the Policies tab in SMS.

   Workaround: This issue may occur if the product is re-installed without correctly removing the previous installation. Follow the instructions given in the "Removing and Reinstalling WASL SMS Packages" section of the Install and Setup Guide.

2) **Issue:** SMS UI freezes when importing policies.
   Workaround: If you see this problem,
   1) Restart the SMS Server from the product CLI ('wasl_sms.sh –restart').
   2) Ensure policy import guidelines as mentioned in the user guide before importing the user-defined policy.

Settings

1) **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.

Limitations

Install and setup

1) Couchbase Server "memcached' type buckets are not supported by WASL SMS.
2) Backspace is not honoured, while entering Couchbase password. If a wrong value is provided for the password field, re-try the operation.

Policy

1) WASL by default do 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

1) Browser 'Back' button does not work if the user tries to access un-authorized URL by entering the URL directly in the address bar.

Node

1) In "SAP HANA DB" policies, rollback will not happen for the following rule: "PERSISTENCE_ENCRYPTION_KEYS should 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 to use 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. However, the "OS Security" policies has rule that modifies static audit files which makes similar changes to as the rules that modify audit records in memory. These changes to static audit files will be remediation and rollback properly. Whenever the system is rebooted, the changes to these static audit files will get reloaded as audit records in memory.

For more information on troubleshooting steps on install, setup, and operations, see the *HPE WASL version 1.1.0 Troubleshooting Guide*.

NOTE: For information about the latest updates on the product refer to the WASL product page at HPE Software Depot and navigating to Linux → Mission Critical x86 Software, or visit: https://h20392.www2.hpe.com/portal/swdepot/displayProductsList.do?category=LNXMCSW

References

For latest information on the WASL product, see the following 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