Hewlett Packard Enterprise

HPE Workload Aware Security for Linux 1.1.0 version Install and Setup guide

Abstract

This guide provides the installation and setup steps for HPE Workload Aware Security for Linux (WASL) version 1.1.0. This document is targeted for admin users and support personnel who provide installation and startup service. This guide covers steps on how to install and configure the product. The technical support individuals may find many general questions answered by this material, but it is not necessary to know all the information in order to use the product.

Published: April 2018

Acknowledgements

Table of Contents

1 Workload Aware Security for Linux Overview

Workload Aware Security for Linux (WASL) provides a way to secure the operating system instance and the associated application running on the operating system together by a single-click from centralized system (called Security Management Station). WASL can evaluate a workload (just operating system or operating system with associated application) to access the current security level, do remediation to increase the security level of the workload. It also offers rich reports from which details of specific evaluations and remediation can be easily obtained. WASL also offers a feature to rollback any remediation done and get back the workload configuration to a previously known configuration state.

WASL is shipped with basic license offering SLES and RHEL OS hardening profiles and advanced licensing offering SAP HANA profiles in addition to basic licensing.

WASL uses a profile based on the global benchmark standards (XCCDF) and currently provides the following standard profiles:

- OS Security for SLES 12 (SP1, SP2 & SP3)
- OS Security for SLES SAP HANA 12 (SP1 & SP2) (OS Security for SLES 12 (SP1 & SP2) tailored for SAP HANA database)
- OS Security for RHEL 7 (7.2, 7.3 & 7.4)
- SAP HANA 1.0 Database
- SAP HANA 2.0 Database
- OS extended profile for SAP HANA (SLES 12 SP1 & SLES 12 SP2) (extra OS protection for securing SAP HANA database)

1.1 WASL Deployment and Architecture

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 associated application installed on it. WASL can secure the workload in the following ways:

- Operating System only
- Operating System and associated application
- Associated application only

The Security Management Station (SMS) is a web based application accessible on HTTPS port (default port is 8116). It offers a rich set of GUI that is accessible by a Chrome web browser and supports a varied set of roles for users to login and perform activities.

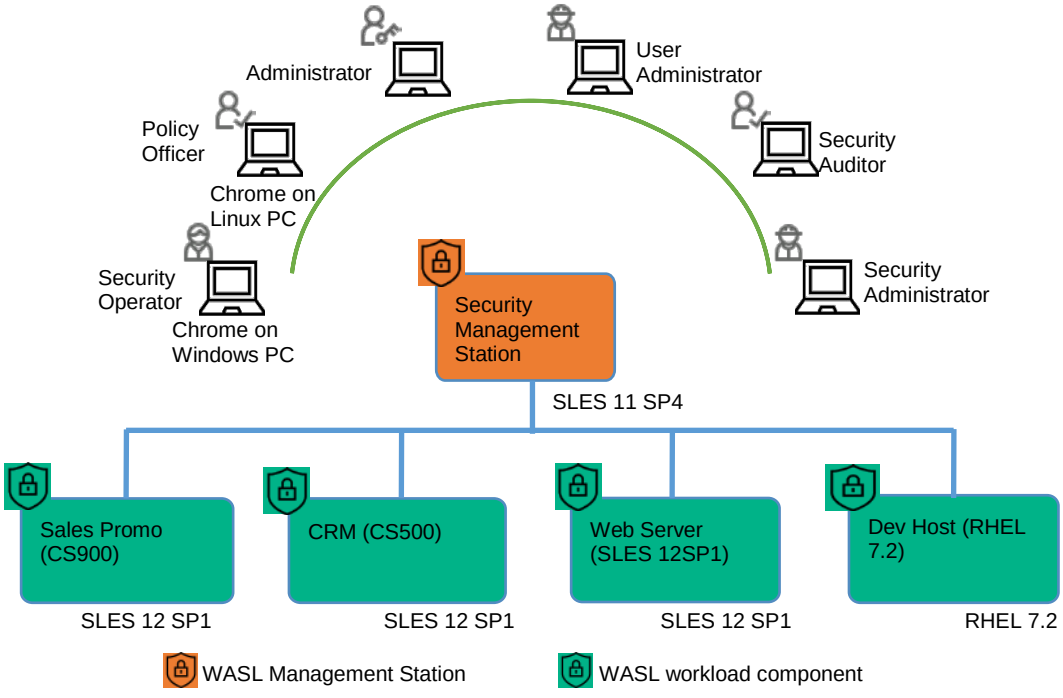


Figure 1: Typical WASL Deployment Scenario

Users can register multiple workloads in SMS. It captures the workload access credentials as a part of registration process. SMS interacts with these workloads establishing a secure shell session between the SMS node and the target node. It also provides an ability to automatically push the Node packages to target node and install remotely. It invokes the security tool to secure the workload element. A workload element can either be an OS or OS and the application running on the OS or only the application.

SMS stores information related to workloads in Couchbase server NOSQL database (accessible via default port 8901). Critical data like user passwords, workload credentials is encrypted and stored in the Couchbase server database using public/private keys protected by a master password. This master password is to be supplied during SMS startup. Some of the data like the reports of a workload evaluation/remediation, logs are stored as flat files.

SMS exposes a HTTPS based web interface using Express.js and Node.js based technologies and Grommet UX framework.

On the Node, WASL uses OpenSCAP product to perform evaluation and remediation of workload using security policies that are based on XCCDF specification. This specification is provided as a part of Security Content Automation Protocol (SCAP) standard maintained by National Institute of Standards and Technology (NIST). The use of this format allows WASL to import and work with many policies that are based on these standards.

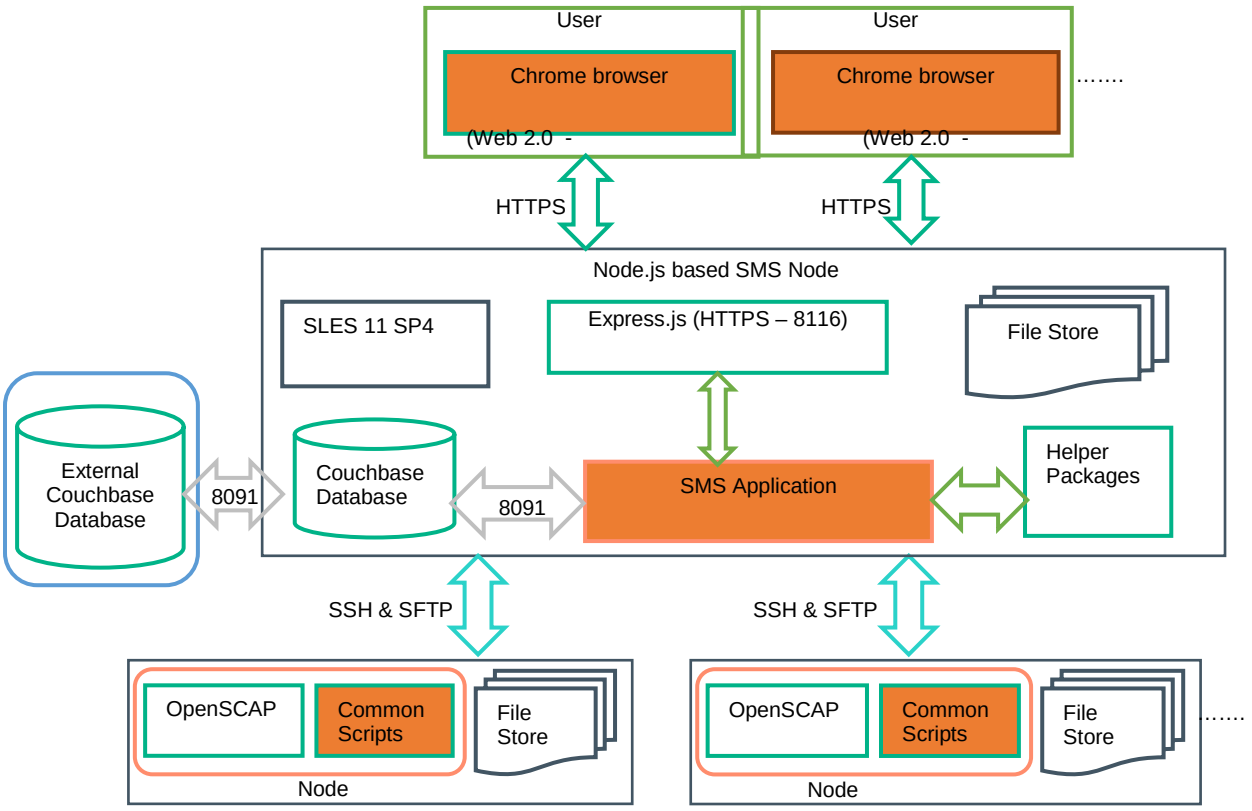


Figure 2: WASL Architecture flow

2 WASL Packages

WASL install media consists of two sets of packages – Security Management Station Packages and Node Packages. Node Packages are supported on SLES and RHEL operating systems.

2.1 Security Management Station (SMS) Packages

SMS packages includes all the required and dependent products for running the centralized SMS server. It consists of centralized server to manage various workloads, security policies, users, activities and environment settings over a web interface. Following are the list of SMS packages:

Package Name	Description
hpe-wasl-sms	Files that renders the SMS server and web pages (GUI).
hpe-wasl-npms	Open Source NPM used for achieving various features of SMS. (https://npms.io/)
hpe-wasl-bs	Bootstrap package - Creates users and groups required for running SMS
hpe-wasl-help	Online Help for WASL SMS
nodejs_1	Web server packages that runs Node.js application.(https://nodejs.org/)
couchbase-server-community	Database to store all data and actions performed on SMS. (https://www.couchbase.com/)
hpe-wasl-policies-template	Files that registers multiple policies to SMS
hpe-wasl-policies-system	Pre-defined default policies to secure Operating System
hpe-wasl-policies-hana (Available only with advanced license product**)**	Pre-defined default policies to secure SAP HANA database

2.2 Node Packages

Node packages includes all the required and dependent products for securing the individual workloads. It should be installed on the Node where the workload is present. The SMS packages already embeds the Node Packages. It can either be installed from SMS GUI or installed separately (manually by admin). They are provided separately to facilitate manual installation. Following are the list of Node packages:

Package Name	Description
hpe_wasl_core	Main package which creates basic environment, scripts for WASL to operate
openscap_1	Tool that utilizes the standard Extensible Configuration Checklist Description Format (XCCDF) checklist and performs evaluation and remediation on the workloads. (https://www.open-scap.org/)
hpe_wasl_os	To secure Operating system workload
hpe_wasl_saphana	To secure SAP HANA workload

2.3 Contents of ISO Image

The SMS and Node Packages are provided as an ISO image. Following is a sample layout of a WASL advanced package ISO contents:

- SMS Packages are located under **/WASL/SLES/SLES11/** directory
- Node Packages for SLES 12 are provided under **/WASL_Node/SLES/SLES12/** directory
- Node Packages for RHEL 7 are provided under **/WASL_Node/RedHat/RedHat7/** directory

```
/Readme_Before_Install.txt
/WASL
/WASL/SLES
/WASL/SLES/SLES11
/WASL/SLES/SLES11/couchbase-server-community-4.5.0-suse11.x86_64.rpm
```

```
/WASL/SLES/SLES11/hpe-wasl-bs-1.1.0-1.x86_64.rpm
/WASL/SLES/SLES11/hpe-wasl-npms-1.1.0-1.x86_64.rpm
/WASL/SLES/SLES11/hpe-wasl-policies-hana-1.1.0-1.x86_64.rpm
/WASL/SLES/SLES11/hpe-wasl-policies-system-1.1.0-1.x86_64.rpm
/WASL/SLES/SLES11/hpe-wasl-policies-template-1.1.0-1.x86_64.rpm
/WASL/SLES/SLES11/hpe-wasl-sms-1.1.0-1.x86_64.rpm
/WASL/SLES/SLES11/nodejs_1-v6.14.1-1.x86_64.rpm
/WASL_Node
/WASL_Node/RedHat
/WASL_Node/RedHat/RedHat7
/WASL_Node/RedHat/RedHat7/hpe_wasl_core-1.1.0-1.rhel7.x86_64.rpm
/WASL_Node/RedHat/RedHat7/hpe_wasl_os-1.1.0-1.rhel7.x86_64.rpm
/WASL_Node/RedHat/RedHat7/hpe_wasl_saphana-1.1.0-1.rhel7.x86_64.rpm
/WASL_Node/RedHat/RedHat7/openscap_1-1.2.15-1.0.x86_64.rpm
/WASL_Node/SLES
/WASL_Node/SLES/SLES12
/WASL_Node/SLES/SLES12/hpe_wasl_core-1.1.0-1.sles12.x86_64.rpm
/WASL_Node/SLES/SLES12/hpe_wasl_os-1.1.0-1.sles12.x86_64.rpm
/WASL_Node/SLES/SLES12/hpe_wasl_saphana-1.1.0-1.sles12.x86_64.rpm
/WASL_Node/SLES/SLES12/openscap_1-1.2.15-1.0.x86_64.rpm
/WASL_Node/SLES/SLES11
/WASL_Node/SLES/SLES11/hpe_wasl_core-1.1.0-1.sles12.x86_64.rpm
/WASL_Node/SLES/SLES11/hpe_wasl_os-1.1.0-1.sles12.x86_64.rpm
/WASL_Node/SLES/SLES11/hpe_wasl_saphana-1.1.0-1.sles12.x86_64.rpm
/WASL_Node/SLES/SLES11/openscap_1-1.2.15-1.0.x86_64.rpm
```

Note: The following package is not available in Basic ISO image:

```
/WASL/SLES/SLES11/hpe-wasl-policies-hana-1.1.0-1.x86_64.rpm
```

3 WASL SMS Installation

3.1 Pre-requisites for installing WASL SMS Packages

The WASL 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

3.2 Install SMS Packages

Insert the WASL ISO CD, FTP or copy the contents of **/WASL/SLES/SLES11/** to the SMS machine into a temporary package location (e.g.: /tmp/rpms/). Login to the SMS machine as root user and install the packages.

For **Advanced license package** ISO Installation including Signature verification, installing Couchbase server and HANA advanced policies use the following command:

```
# cd /tmp/rpms/
```

Signature verification: The packages are signed with private digital keys held by HPE and the integrity of the packages can be verified before installing.

1. Download the HPE public keys compressed tar file (HPE-GPG-Public-Keys.tar.gz) from the following link to your local directory and extract the public keys:

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

   # tar -zxvf HPE-GPG-Public-Keys.tar.gz

2. Import the keys for RPM, one at a time while logged in as root by running the following command:

   # rpm --import /path_to_the_key/file_name_of_the_key

   Example:
   # rpm --import /path_to_the_key/B1275EA3.pub

3. To verify the signature of WASL RPM's, use the rpm --checksig command to validate and verify the digital signature of the signed file:
   # rpm --checksig <filename_of_the_rpm.rpm>

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

   Example output:
   hpe-wasl-bs-1.0.0-1.x86_64.rpm: rsa sha1 (md5) pgp md5 OK

   If your file does not pass verification or you do not have the HPE public key installed, the following error is displayed during installation:
   Example output:
   "hpe-wasl-bs-1.0.0-1.x86_64.rpm:: (SHA1) DSA sha1 md5 (GPG) NOT OK (MISSING KEYS: key#s)"

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

See the following link for more details:
https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

RPM Installation:

For **Advanced license package:**

cd /tmp/rpms/

```
# zypper install couchbase-server-community*.rpm nodejs_1*.rpm hpe-wasl-bs*.rpm hpe-wasl-npms*.rpm hpe-wasl-help*.rpm hpe-wasl-sms*.rpm hpe-wasl-policies-template*.rpm hpe-wasl-policies-system*.rpm hpe-wasl-policies-hana*.rpm
```

For **Basic license package**:

```
# cd /tmp/rpms/
# zypper install couchbase-server-community*.rpm nodejs_1*.rpm hpe-wasl-bs*.rpm hpe-wasl-npms*.rpm hpe-wasl-help*.rpm hpe-wasl-sms*.rpm hpe-wasl-policies-template*.rpm hpe-wasl-policies-system*.rpm
```

In case, if you have a different instance of Couchbase server (NoSQL database) already running and wish to reuse it, then SMS can be configured accordingly. In such case, you do not need to install the Couchbase-server-community package.

For Advanced package ISO Installation not including installing Couchbase server use the following command:

cd /tmp/rpms/

```
# zypper install nodejs_1*.rpm hpe-wasl-bs*.rpm hpe-wasl-npms*.rpm hpe-wasl-help*.rpm hpe-wasl-sms*.rpm hpe-wasl-policies-template*.rpm hpe-wasl-policies-system*.rpm hpe-wasl-policies-hana*.rpm
```

For Basic package ISO Installation not including installing Couchbase server use the following command:

```
# cd /tmp/rpms/
# zypper install nodejs_1*.rpm hpe-wasl-bs*.rpm hpe-wasl-npms*.rpm hpe-wasl-help*.rpm
hpe-wasl-sms*.rpm hpe-wasl-policies-template*.rpm hpe-wasl-policies-system*.rpm
```

3.3 Post installation check

Ensure that the SMS web server port (default is TCP port 8116) is not blocked by firewall.

- You can use the YAST tool on SLES system to check the firewall settings. You will have to edit the advanced firewall settings in YAST tool to enable this port.
- If you are provided an alternative port by your organization, edit the /opt/hpe/wasl/sms/config/custom_config.js file and change or add the "config.web.https_port" to use the appropriate port that is enabled before starting SMS.

4 WASL SMS Setup (wasl_sms.sh -setup) and run

After installing WASL SMS, it needs to be setup for the first time before starting or using WASL. Login as root user to perform these operations. Run the following script with "-setup" option:

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

This command internally runs as '**waslsms**' user and configures:

a) Couchbase Server (database for SMS)
b) SMS security settings (Master and Recovery key)
c) Certificates (To enable https connection)

Note: The wasl_sms.sh is a wrapper script and can be used for doing most of the command line operations like starting and stopping of WASL SMS, resetting Master and Recovery Key passwords etc.

Run the script with "-help" option as shown below to display all available options. The wasl_sms.sh does a sudo to 'waslsms' user before doing any operation.

"/opt/hpe/waslx/sms/tools/wasl_sms.sh -help"

4.1 Setup Couchbase server

There are 2 configuration options to perform "Couchbase Server" setup – "**Typical"** and "**Advanced**". The default is **Typical**.

Setup Type	Description
Typical	Configures an instance of 'Couchbase Server Community Edition' for WASL SMS using the pre-defined defaults. In this setup type, a new Couchbase cluster with username 'Administrator' is created and made accessible on port 8091. A Couchbase bucket by name 'wasl_sms_bucket' is created to store the WASL SMS data. **Note:** We can make WASL SMS to create and use a different Couchbase cluster username, cluster port and bucket name by setting "setupConfig.db.cluster_username", "setupConfig.db.cluster_port" and "setupConfig.db.bucket_name" in /opt/hpe/wasl/sms/config/custom_setupConfig.js if required. These parameters cannot be changed once the Couchbase server setup phase is completed.
Advanced	This options should be selected if there is already an existing instance of Couchbase Server present and running on the system. WASL SMS does not create any Couchbase cluster or Couchbase bucket, but expects these information to be already present in the Couchbase server. This setup will ask for the following information: - IP address and port number where Couchbase server is running - The bucket name and its password that is already existing in Couchbase server. This bucket will be used by WASL SMS to store its data. A new bucket is not created by WASL SMS.

4.2 Setup SMS security settings

This phase requires to enter the master and recovery passwords to protect the Master and Recovery key.

- **Master key**: This is root key that protects all the security critical data in WASL SMS. A separate 'master password' is required, which encrypts this 'master key'.

- ‘Master password’ needs to be provided while starting WASL SMS, so that WASL SMS can decrypt/encrypt the critical data.
- ‘Master password’ can be stored during setup in a stash file (/opt/hpe/wasl/sms/data/stashfile). In such case, SMS can pick up the password from this file and start SMS automatically during system startup. If stash file is not used to store the master password, then WASL SMS should be started manually using “wasl_sms.sh -startup” command every time. “wasl_sms.sh -startup” commands prompts for ‘master password’ to be entered during startup.
- ‘Master password’ can be modified at a later time if,
  - the earlier master password is known
  - the earlier master password was stored in stash file
  - the earlier password was recovered

The password can be reset by the following command:

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

- **Recovery Key**: is used to recover the master password when the master password is lost or forgotten. A separate ‘recovery password’ is required, which encrypts this Recovery key.
  - Use of ‘Recovery key’ is optional
  - ‘Recovery password’ can be modified at a later time if,
    - the earlier master password is known
    - the earlier master password was stored in stash file
    - the earlier password was recovered

  The password can be reset by the following command:

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

4.3 Setup Certificates

In this phase, SMS sets up the certificate required for the HTTPS connection to browsers. There are 2 options provided to configure the certificates:

- **Create a Self-signed certificate:** A self-signed certificate will be created by SMS during this phase
- **Import a signed certificate:** Import a base64 encoded pem certificate signed by an external third party with CA certificates and key files

If you want to regenerate a certificate or import a new set of certificate at a later time, you can use the following command:
`/opt/hpe/wasl/sms/tools/wasl_sms.sh -setup_cert`

Note: The self-signed certificate is set to default expire after 365 days

4.4 Starting and stopping SMS

4.4.1 Start Couchbase

Before starting SMS, ensure that ‘couchbase-server’ service is running.

If you have used “Typical Setup”, the ‘couchbase-server’ service will run on the same system where WASL SMS is installed. You can check if ‘couchbase-server’ service is configured by default to start during system startup by the command.

```
# chkconfig --list couchbase-server
couchbase-server          0:off  1:off  2:off  3:on   4:off  5:on   6:off
```

To check if ‘couchbase-server’ service is running, use the command:

```
# service couchbase-server status
couchbase-server is running
```

You can use the following command to start ‘couchbase-server’ service:

```
# service couchbase-server start
```

Note: couchbase runs as 'couchbase' user

4.4.2 Start SMS

The following are the two ways to start SMS service:

Note: SMS runs as '**waslsms'** user.

1. Starting SMS service

'hpe-wasl-sms' service is registered at run level 3 and 5, to startup automatically during system startup and shutdown.

```
# chkconfig --list hpe-wasl-sms
hpe-wasl-sms              0:off  1:off  2:off  3:on   4:off  5:on   6:off
```

The SMS gets started automatically only if the WASL SMS is setup to store the master password into a stash file during setup.

You can also start or restart the hpe-wasl-sms service manually using the following command:

```
# service hpe-wasl-sms start
```

OR

```
# service hpe-wasl-sms restart
```

2. Start SMS using wasl_sms.sh

For starting or restarting SMS from command line by manually entering master password, use the command:

```
# /opt/hpe/wasl/sms/tools/wasl_sms.sh –start
```

OR

```
# /opt/hpe/wasl/sms/tools/wasl_sms.sh –restart
```

Provide the master password at the appropriate prompt.

4.4.3 Stop SMS

The following are the two options to stop SMS service:

1. Stop the SMS service by the command:

   ```
   # service hpe-wasl-sms stop
   ```

   Ensure that the process related to wasl is stopped by the command:

   ```
   # ps -ef | grep -i wasl
   ```

2. Alternatively, Stop SMS via the command line argument:

   ```
   # /opt/hpe/wasl/sms/tools/wasl_sms.sh –stop
   ```

   Ensure that the process related to wasl is stopped by the command:

   ```
   # ps -ef | grep -i wasl
   ```

3. Stop the 'couchbase-server' service also using following command:

   ```
   # service couchbase-server stop
   ```

   Note: If you are using Couchbase server as a database for other applications apart from SMS, do not stop couchbase-server service.

4.5 Login to SMS

Use Chrome browser to access the SMS at the URL https://<IPAddress of SMS host>:8116. User can authenticate to SMS using the default administrator account username="admin" and password="admin".

You are prompted to change the password on first login. Use this account for admin purposes only. It is recommended to add other SMS user with different roles to perform operations in SMS.

5 Node Packages Installation and setup

Node packages include all the required and dependent products for securing the individual workloads and should be installed on the Node where the workload is present. The SMS packages already embeds the Node Packages. The Node Packages can either be installed from SMS GUI or installed separately (manually).

5.1 Pre-requisites for installing Node Packages

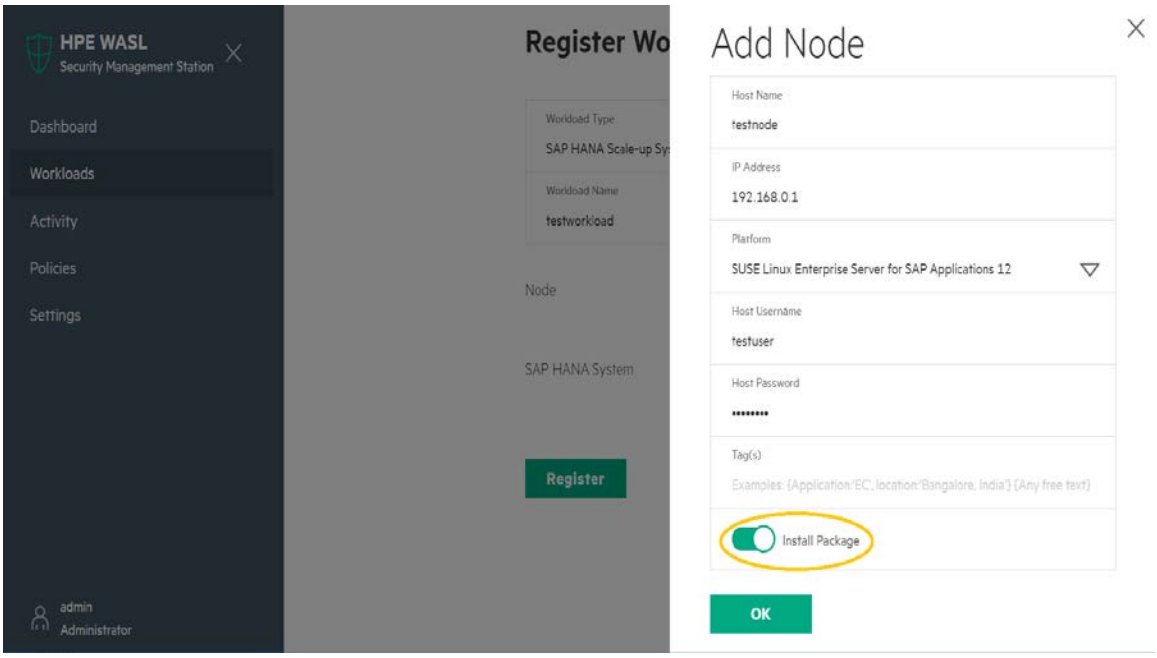
The WASL Node Packages can be installed on a virtual machine or a physical server based on the following requirements

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.
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 (Both SSHD and SFTP should be enabled) • libopenssl1_0_0 (on SUSE)
Disk requirement	5 GB minimum
List of software that are required for Operating System security	Multiple package such as perl-base (on SLES), perl (on RHEL), audit, sed, gawk, etc; are part of base operating system.

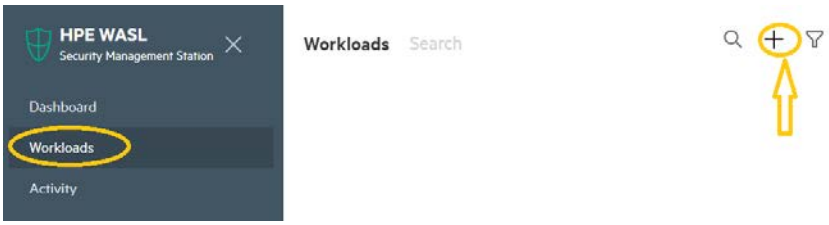
Software package required for SAP HANA security	• SAP HANA Database
	  • SAP HANA 1.0 SPS11
	  • SAP HANA 1.0 SPS12
	  • SAP HANA 2.0 SPS00
	  • SAP HANA 2.0 SPS01
	  • SAP HANA 2.0 SPS02
	• SAP HANA Client - HDB_CLIENT provided with SAP HANA database (WASL uses the client to connect to SAP HANA via Python PyDBAPI provided with SAP HANA Client in /usr/sap/hdbclient/hdbcli/dbapi.py OR /usr/sap/<SID>/HDB<INSTANCE_NUMBER>/exe/python_support/hdbcli/dbapi.py locations)

5.2 Automatic Node Package installation and setup from SMS

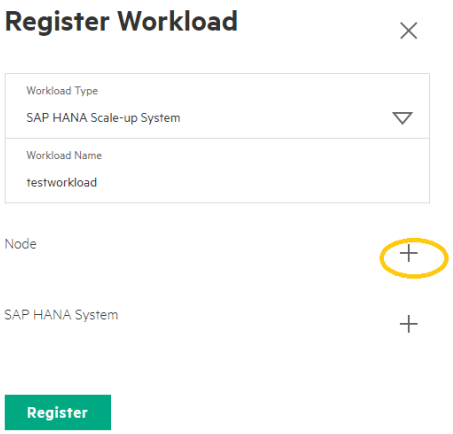
To automatically install and setup SMS on the Node, turn ON the **Install Package** option from the **Add Node** screen during workload registration on SMS (for any **Workload Type**).



You will see the 'Add Node' Screen while registering a new workload in SMS. Select the "**+**" sign under the **Workload** screen to add the new Workload.



You will see the **Add Node** screen, by selecting the "**+**" sign opposite to the Node in the **Register Workload** screen:



SMS connects to this node via secure shell using the credentials provided in the **Add Node** screen to login and perform installation and setup. If the **Host Username** provided in the **Add Node** screen is not "root", then perform the following steps before installing on the Node:

On a **SLES 12 node** create /etc/sudoers.d/waslcore_install file with following content:

```
Cmnd_Alias WASL_NODEKITS = /usr/bin/zypper --non-interactive install hpe_wasl_core.rpm, \
                        /usr/bin/zypper --non-interactive install hpe_wasl_os.rpm, \
                        /usr/bin/zypper --non-interactive install hpe_wasl_saphana.rpm, \
                        /usr/bin/zypper --non-interactive install openscap.rpm
Cmnd_Alias WASL_NODESETUP = /opt/hpe/wasl/core/bin/wasl-setup
<username> ALL=(root) NOPASSWD: WASL_NODEKITS
<username> ALL=(root) NOPASSWD: WASL_NODESETUP
Defaults!WASL_NODEKITS !requiretty
Defaults!WASL_NODESETUP !requiretty
```

Replace <username> with the user name mentioned under "**Host username" field** in the **Add Node** screen of SMS. These commands gives privilege for < username> to install and setup the Node Packages.

On **RHEL node** system create /etc/sudoers.d/waslcore_install file with following content:

```
Cmnd_Alias WASL_NODEKITS = /usr/bin/yum --assumeyes install hpe_wasl_core.rpm, \
                        /usr/bin/yum --assumeyes install hpe_wasl_os.rpm, \
                        /usr/bin/yum --assumeyes install hpe_wasl_saphana.rpm, \
                        /usr/bin/yum --assumeyes install openscap.rpm
Cmnd_Alias WASL_NODESETUP = /opt/hpe/wasl/core/bin/wasl-setup
<username> ALL=(root) NOPASSWD: WASL_NODEKITS
<username> ALL=(root) NOPASSWD: WASL_NODESETUP
Defaults!WASL_NODEKITS !requiretty
Defaults!WASL_NODESETUP !requiretty
```

Replace <username> with the user name mentioned under "**Host username" field** in the **Add Node** screen of SMS. These commands gives privilege for < username> to install and setup the Node Packages.

To know the detailed steps of what happens during automatic installation, see the "Manual Node Package installation and setup from Node" section.

5.3 Manual Node Package installation and setup from Node

Perform the following steps to install and setup the Node Packages manually as "root" user:

5.3.1 Install node packages

Insert the WASL ISO CD, FTP or copy the Node package contents to the Node machine into a temporary package location (e.g.: /tmp/rpms/). Login to the Node machine as root user and install the packages.

- The Node Packages for SLES 12 are provided under **/WASL_Node/SLES/SLES12/** directory of ISO.
- The Node Packages for RHEL 7 are provided under **/WASL_Node/RedHat/RedHat7/** directory of ISO.

```
# cd /tmp/rpms/
```

For **SLES OS** workload install the following:

```
# zypper install openscap_1*.rpm  hpe_wasl_core*.rpm  hpe_wasl_os*.rpm
```

For **SLES for SAP HANA** workload also install the hpe_wasl_saphana.rpm RPM:

```
# zypper install openscap_1*.rpm  hpe_wasl_core*.rpm  hpe_wasl_os*.rpm
hpe_wasl_saphana*.rpm
```

For **RHEL OS** workload install the following:

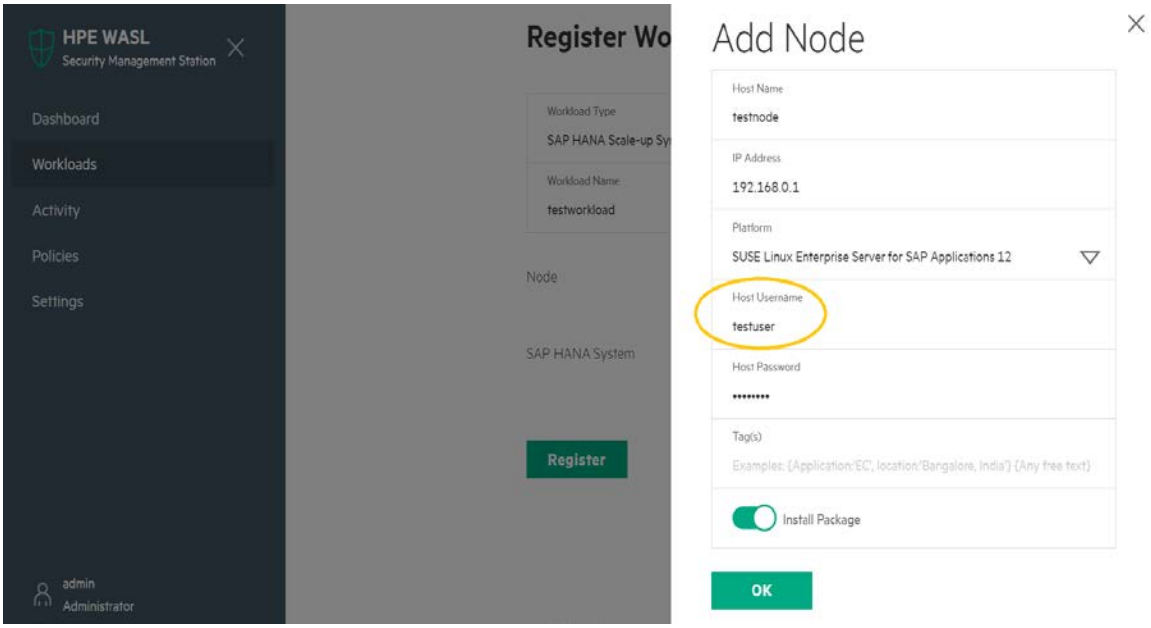
```
# yum install openscap_1*.rpm  hpe_wasl_core*.rpm  hpe_wasl_os*.rpm
```

5.3.2 Run wasl-setup to provide user privileges

Run the "`/opt/hpe/wasl/core/bin/wasl-setup`" tool with "-a" option as "root" to allow users to run WASL workload operations with privileges on the Node. Use of wasl-setup tool varies for different workload Types:

a. **"Operating System Only" Workload Type:**
Operating System workload Type is used to secure the Operating System and other critical components which usually requires "root" user access. If the **Host Username** provided in the **Add Node** screen during workload registration on SMS is other than "root", then run the following command, to allow the user specified in **Host Username** of **Add Node** screen to obtain temporary privileged access as root while performing WASL operations:

```
/opt/hpe/wasl/core/bin/wasl-setup -a <Host username provided in Add Node screen of SMS>:root
```



b. **"SAP HANA Scale-up System" Workload Type:**
SAP HANA Workload has two components to be secured: **Operating System** and **SAP HANA database.**

To secure the "Operating System", perform the same steps as "Operating System Only Workload Type". I.e. In case the **Host Username** provided in the **Add Node** screen of SMS is other than "root", then run the following command, to allow the user specified in **Host Username** of **Add Node** screen to obtain temporary privileged access as root while performing WASL operations:

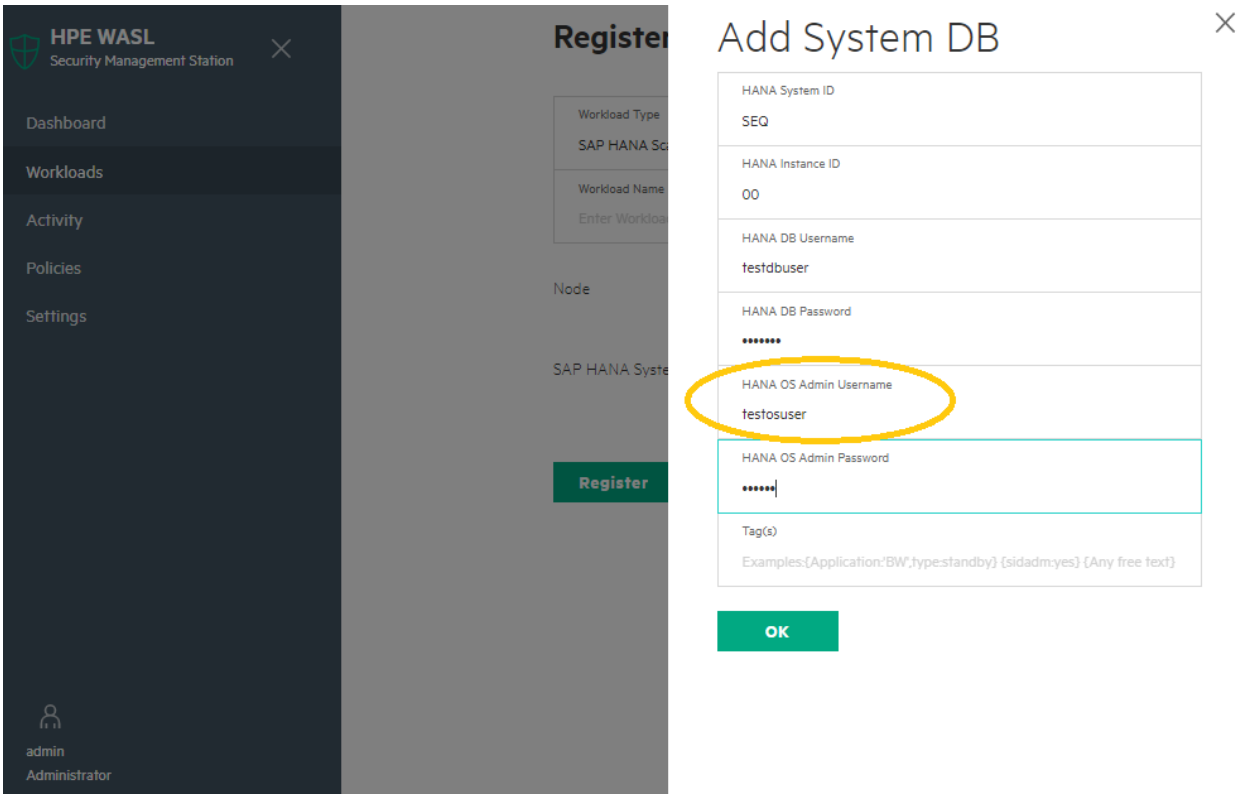
```
/opt/hpe/wasl/core/bin/wasl-setup -a <Host username provided in Add Node screen of SMS>:root
```

For Securing SAP HANA database, WASL uses a newly created non privileged user "**waslhanauser**" to connect to the SAP HANA database and secure it. If the **HANA OS Admin Username** provided in **Add System DB** screen of SMS is other than "root", then run the following command:

```
/opt/hpe/wasl/core/bin/wasl-setup -a <HANA OS Admin Username provided in Add System DB screen of SMS>:waslhanauser
```

Note: The SAP HANA workload registration allows to use the <SID>adm OS user account instead of using the "**waslhanauser**" user by WASL. In such case, creation of certificates for "**waslhanauser**" is not required. For more

information on using <SID>adm OS user account instead of using the "**waslhanauser**" user, see the *HPE WASL User Guide*.



The "/opt/hpe/wasl/core/bin/wasl-setup -a **<user_name_a>:<user_name_b>**" script does the following:

- Adds **<user_name_b>** to waslcore group. This group has read and write access to most of the files related to WASL on the Node.
- Adds **<user_name_a>** to waslcoreshare group. This group has limited read and write access to some directories of WASL on the node (write access to /var/opt/hpe/wasl/core/tmp and read access to /var/opt/hpe/wasl/core/reports)
- Creates the following entry in /etc/sudoers.d/hpewasl, so that the **<user_name_a>** can run the workload operations (like deploy, evaluation, remediation, rollback) as **<user_name_b>** with privileges:
  <user_name_a> `ALL=(`**<user_name_b>**`) NOPASSWD: /opt/hpe/wasl/core/bin/wasl`

5.3.3 Create certificates for walshanauser users

For Securing SAP HANA database, WASL uses a newly created non privileged user "**waslhanauser**" to connect to the SAP HANA database and secure it. The SAP HANA database can be configured such that only secure communication is possible to the SAP HANA database. In such cases, the "**waslhanauser**" should have its certificate setup and signed by the SAP HANA server certificate in order to connect to SAP HANA database. To generate this signed signatures run the following command as "root" user:

```
# /opt/hpe/wasl/core/bin/wasl-setup --waslhanauser_cert_gen --sidadm=<sid>adm
```

Note: The SAP HANA workload registration allows to use the <SID>adm OS user account instead of using the "**waslhanauser**" user by WASL. In such case, creation of certificates for "**waslhanauser**" is not required. For more information on using <SID>adm OS user account instead of using the "**waslhanauser**" user, see the *HPE WASL User Guide*.

The "/opt/hpe/wasl/core/bin/wasl-setup --waslhanauser_cert_gen --sidadm=<sid>adm" script does the following:

- Creates a /home/waslhanauser/.ssl directory with appropriate privileges if it is not existing
- Creates a RSA 2048 certificate that is valid for 365 days and a key
  - The certificate needs to be regenerated after 365 days
- Does a sudo to <SID>adm user and signs the newly created certificate using the master certificate of SAP HANA database

6 Removing and Reinstalling WASL SMS Packages

This section covers the details about removing and reinstalling the WASL SMS packages on the SMS system. In order to remove the node packages on the Workloads registered on this SMS, follow the steps in “Removing and Reinstalling Node Packages” section.

6.1 Remove or Reinstall WASL SMS:

Step 1: Stop the hpe-wasl-sms service and the ‘couchbase-server’ service. See “Stop SMS” section for details.

Step 2: Remove WASL SMS and Couchbase server packages, by running the following command:

```
# zypper remove couchbase-server-community nodejs_1 hpe-wasl-bs hpe-wasl-npms
hpe-wasl-help hpe-wasl-sms hpe-wasl-policies-hana hpe-wasl-policies-system hpe-
wasl-policies-template
```

In case, you have not installed couchbase-server-community, during installation of WASL SMS, you can remove only the other packages as follows:

```
# zypper remove nodejs_1 hpe-wasl-bs hpe-wasl-npms hpe-wasl-help hpe-wasl-sms
hpe-wasl-policies-hana hpe-wasl-policies-system hpe-wasl-policies-template
```

Step 3: Some of the files like reports, imported policies, certificates, logs, couchbase bucket database are not removed by the package removal.

a. The following configuration files are retained in WASL SMS directories:
   i. /opt/hpe/wasl/sms/config/custom_config.js is saved is saved as /opt/hpe/wasl/sms/config/custom_config.js.rpmsave
   ii. /opt/hpe/wasl/sms/config/custom_setupConfig.js is saved is saved as /opt/hpe/wasl/sms/config/custom_setupConfig.js.rpmsave
   iii. /opt/hpe/wasl/sms/config/auto-gen/setup_config.js is saved is saved as /opt/hpe/wasl/sms/config/auto-gen/setup_config.js.rpmsave
   iv. /opt/hpe/wasl/sms/config/auto-gen/credentials.js is saved is saved as /opt/hpe/wasl/sms/config/auto-gen/credentials.js.rpmsave

b. The following configuration files are retained in Couchbase directories, in case you removed the couchbase-server-community package:
   i. /opt/couchbase/var/lib/couchbase/config/config.dat is saved as /opt/couchbase/var/lib/couchbase/config/config.dat.rpmsave
   ii. /opt/couchbase/etc/couchdb/local.ini is saved as /opt/couchbase/etc/couchdb/local.ini.rpmsave

Step 4: These files and users are retained so that a reinstallation of WASL SMS packages will work fine. If you plan to reinstall WASL SMS once again do the following:

c. Follow the Installation Steps mentioned under “WASL SMS Installation” section. Do not follow the “WASL SMS Setup” section after this.
d. Stop the hpe-wasl-sms service and the ‘couchbase-server’ service, if it is started as part of installation, by following the steps in “How to Stop SMS” section.
   i. Copy back the old configuration following files related to WASL:

```
# cp /opt/hpe/wasl/sms/config/custom_config.js.rpmsave
/opt/hpe/wasl/sms/config/custom_config.js
# cp /opt/hpe/wasl/sms/config/custom_setupConfig.js.rpmsave
/opt/hpe/wasl/sms/config/custom_setupConfig.js
# cp /opt/hpe/wasl/sms/config/auto-gen/setup_config.js.rpmsave
/opt/hpe/wasl/sms/config/auto-gen/setup_config.js
# cp /opt/hpe/wasl/sms/config/auto-gen/credentials.js.rpmsave
/opt/hpe/wasl/sms/config/auto-gen/credentials.js
```

   ii. Copy back the following files in case you had earlier removed the couchbase-server-community package:

```
# cp /opt/couchbase/var/lib/couchbase/config/config.dat.rpmsave
/opt/couchbase/var/lib/couchbase/config/config.dat
# cp /opt/couchbase/etc/couchdb/local.ini.rpmsave
/opt/couchbase/etc/couchdb/local.ini
```

iii. Start the 'couchbase-server' service and the hpe-wasl-sms service using the steps provided in "Start SMS" section.

Step 5: In case you want to completely remove all the files and users generated by the different packages, do the following:

e. Remove all the directories created by the WASL SMS packages (Including the couchbase packages) by the commands:

```
# rm -rf /opt/hpe/wasl/sms/
# rm -rf /opt/hpe/wasl/nodejs/
# rm -rf /var/opt/hpe/wasl/sms/
# rm -rf /var/log/hpe_wasl_sms/
# rm -rf /opt/couchbase/   (Remove this only if you have removed the
couchbase-server-community package)
```

Step 6: There are also waslsms user and group and couchbase user and group that is not removed by the package removals. Retain these users and groups if you plan to reinstall WASL SMS once again.

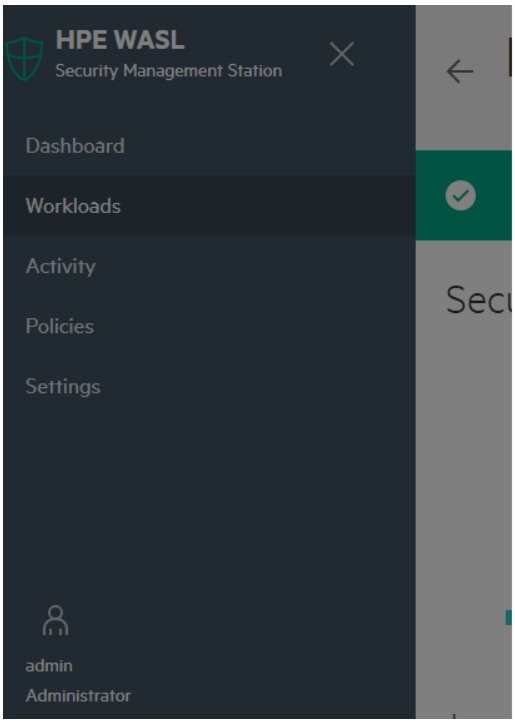
Step 7: In case you want to completely remove all the users and groups, run the following command:

```
# userdel waslsms
# groupdel waslsms
# userdel couchbase (Remove this only if you have removed the couchbase-
server-community package)
# groupdel couchbase (Remove this only if you have removed the couchbase-
server-community package)
```

6.2 Removing and Reinstalling Node Packages

Follow the following steps for removing and reinstalling the Node Packages

1. Removing of Node Packages will not remove any remediation done on the Workloads on the node. You will have to rollback or reset these remediation from the SMS GUI first before removing node packages.



Rollback

This operation will restore the system to a state prior to running last **Remediation**.

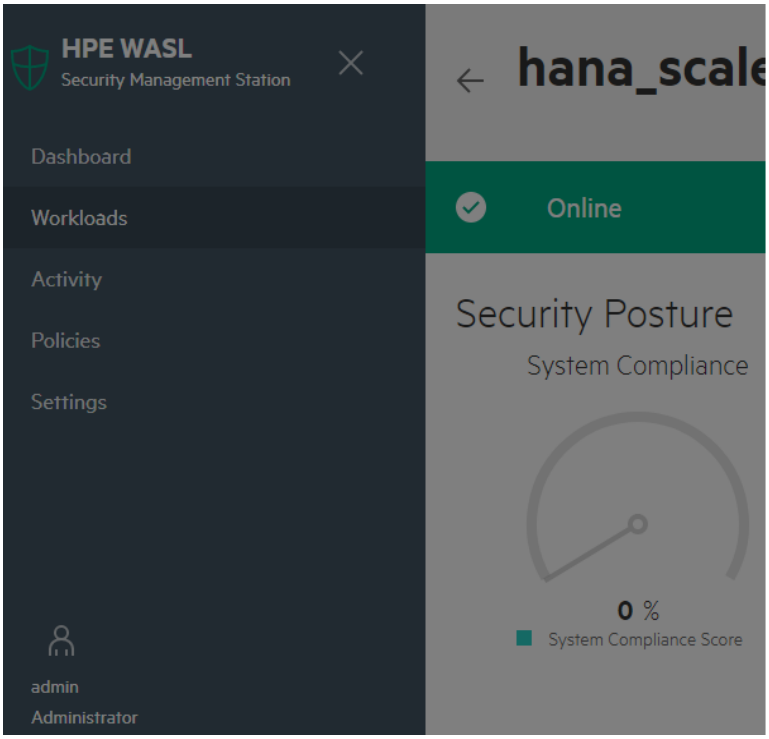
WARNING: All user changes will also be lost.

Rollback last remediation:

Last remediation performed at **September 28th, 2017 4:10 PM** on workload element **SEQ 00** with policy **SAP HANA 1.0 Security Policies for Single Host installation - Level 2**.

Advanced Rollback Options

Rollback



Reset

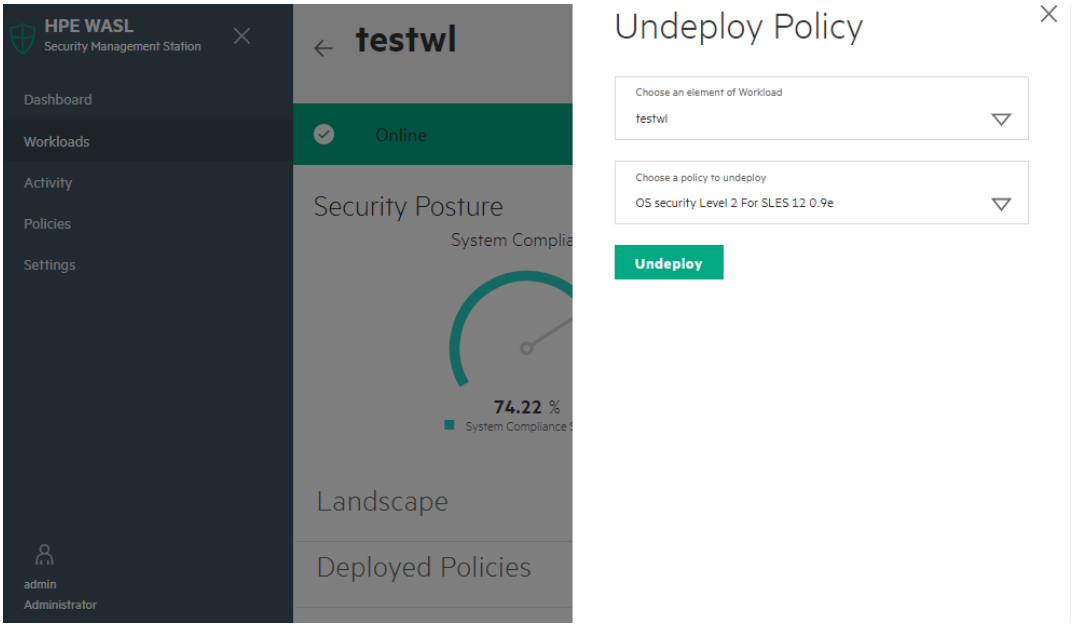
This operation will restore the system to a state prior to running **HPE WASL**.

WARNING: All user changes will also be lost.

Are you sure you want to reset **hana_02**?

Yes, reset

2. If you are not planning on reinstalling the Node Packages, Undeploy all profiles that is deployed on the Node from the SMS GUI.



2. Login to the node as root and remove the Node Packages.

   For **SLES OS** workload remove the following:

   ```
   # zypper remove openscap_1  hpe_wasl_core  hpe_wasl_os
   ```

   For **SLES for SAP HANA** workload also remove the hpe_wasl_saphana.rpm RPM:

   ```
   # zypper remove openscap_1  hpe_wasl_core  hpe_wasl_os hpe_wasl_saphana
   ```

   For **RHEL OS** workload install the following:

   ```
   # yum remove openscap_1  hpe_wasl_core  hpe_wasl_os
   ```

3. Some of the files like snapshots, reports, deployed policies, certificates, and logs are not removed. Also the waslcore, waslcoreshare group and waslhanauser user created during installation is not removed.

4. These files and users are retained so that a reinstallation of Node packages and monitoring it from the same WASL SMS to which it was originally registered will work fine. If you plan to reinstall the node packages from the same registered WASL SMS, follow the steps mentioned in "Node Package Installation and setup" section.

5. If you do not want any files, users or groups to be present, then run the following commands:

   ```
   # rm -rf /opt/hpe/wasl/core
   # rm -rf /var/opt/hpe/wasl/core
   # userdel waslhanauser
   # groupdel waslcore
   # groupdel waslcoreshare
   # rm /etc/sudoers.d/waslcore_install
   ```

The waslcore_install file might be manually created by you as a part of "Node Package Installation and Setup" phase.

7 Best practices

This section lists the user best practices

1. Couchbase Server works on all network interfaces (INADDR_ANY). Update the iptable rules to restrict access to Couchbase Server from external networks.

2. Node.js SDK library for Couchbase Server does not support SSL functionality. Instead of SSL, use IPsec tunnel between the SMS and the Couchbase Servers for securing the communication (This is applicable only when SMS and Couchbase Servers are hosted in different servers).

8 References

- HPE WASL User Guide
- OpenSCAP portal
- Couchbase Server documentation
- Grommet Portal
- Node.js Portal
- Express.js Portal
- Security Content Automation Protocol (SCAP) Portal

9 Appendix

9.1 Sample run of SMS setup

Sample runs of different SMS setup is given below as reference:

Typical Couchbase server setup

A sample run of a complete setup with typical Couchbase server setup is as follows:

```
# /opt/hpe/wasl/sms/tools/wasl_sms.sh -setup
====================== Setup HPE WASL SMS ===================================
This program will set up the Security Management Station (SMS) for Workload
Aware Security for Linux (HPE WASL). Would you like to continue? [yes]:

To accept the default shown in brackets, press the Enter key.

====================== Configure Couchbase Server ============================
'HPE WASL SMS' requires a Couchbase Server instance to store data.
Choose a Couchbase Server setup type:

0. Exit Setup

1. Typical - Set up a new instance of Couchbase Server

   Configures an instance of 'Couchbase Server Community Edition' for
   'HPE WASL SMS' using the pre-defined defaults on the local host.
   Note: This setup type is not valid for enterprise version of Couchbase Server.

2. Advanced - Use an existing instance of Couchbase Server

   Store 'HPE WASL SMS' data in an existing Couchbase Server instance.
   In-order to use this option, the Couchbase Server should be configured and
   a bucket created for 'HPE WASL SMS'. This setup type requires IP address,
   port number, bucket name and password of the instance.

Choose a Couchbase Server setup type [1]:

Successfully configured an instance of Couchbase Server

======================== HPE WASL SMS Security Settings =====================
The HPE WASL SMS master password is the root key that protects all the security
```

```
critical data. Please remember this password, as the HPE WASL SMS cannot be
started without this password.

Enter the master password: **********
Confirm the master password: **********

--------------------------------------------------------------------------------
The stash file is a copy of the master password that resides on the system's local
disk that will be protected with file permissions.

HPE WASL SMS can be started without prompting for master password if stash file is
setup. If you choose not to setup a stash file, the HPE WASL SMS will prompt you for
the master password each time it starts up.

Do you want to setup the stash file? [yes]:

--------------------------------------------------------------------------------
Recovery password is used to recover the master password when the master password is
lost or forgotten. It is recommended to setup the recovery password.

Do you want to setup a recovery password? [yes]:

Please remember this password. If you forget this password, the HPE WASL SMS
cannot be recovered when the master password is lost or forgotten.

Enter the recovery password: **********
Confirm the recovery password: **********
================================================================================
Certificate Setup for HPE WASL SMS

SMS can be accessed from (chrome) browser via HTTPS (secure HTTP) protocol
SMS Server certificates should be setup for it to communicate securely

Choose the certificate setup type:

   1. Create a Self-signed certificate
      Lets you create a self-signed certificate automatically.

   2. Import a signed certificate
      Import an existing Server Certificate
      Lets you import Server certificate signed by the Enterprise CA or third-party CA


   3. Exit

Choose a setup type [1]:

Creating Self-Signed Certificate....

waslsms001.localdomain
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [IN]:
State or Province Name (2 letter code) [KA]:
```

```
Locality Name (eg, city) [Bangalore]:
Organization Name (eg, company) [Hewlett Packard Enterprise]:
Organizational Unit Name (eg, section) [Security Lab]:
Common Name (eg, YOUR name) [waslsms001]:
Email Address [user@hostname.com]:

Successfully created Self-signed certificates for HPE WASL SMS
```

Advanced Couchbase server setup

A sample run of a setup showing advanced Couchbase server setup is as follows:

```
# /opt/hpe/wasl/sms/tools/wasl_sms.sh -setup
====================== Setup HPE WASL SMS ====================================
This program will set up the Security Management Station (SMS) for Workload
Aware Security for Linux (HPE WASL). Would you like to continue? [yes]:

To accept the default shown in brackets, press the Enter key.

====================== Configure Couchbase Server ============================
'HPE WASL SMS' requires a Couchbase Server instance to store data.
Choose a Couchbase Server setup type:

0. Exit Setup

1. Typical - Set up a new instance of Couchbase Server

   Configures an instance of 'Couchbase Server Community Edition' for
   'HPE WASL SMS' using the pre-defined defaults on the local host.
   Note: This setup type is not valid for enterprise version of Couchbase Server.

2. Advanced - Use an existing instance of Couchbase Server

   Store 'HPE WASL SMS' data in an existing Couchbase Server instance.
   In-order to use this option, the Couchbase Server should be configured and a bucket
created for 'HPE WASL SMS'. This setup type requires IP address, port number, bucket
name and password of the instance.

Choose a Couchbase Server setup type [1]:2

------------------------------------------------------------------------------
Please provide the details of your Couchbase Server instance.

Enter the IP address [127.0.0.1]:

Enter the port number [8091]:8992

Enter the bucket name [wasl_sms_bucket]:wasl123_sms_bucket

Enter the bucket password: **********

======================== HPE WASL SMS Security Settings ======================
The HPE WASL SMS master password is the root key that protects all the security
critical data. Please remember this password, as the HPE WASL SMS cannot be started
without this password.

Enter the master password: **********
Confirm the master password: **********
```

```
--------------------------------------------------------------------------------
The stash file is a copy of the master password that resides on the system's local
disk that will be protected with file permissions.

HPE WASL SMS can be started without prompting for master password if stash file is
setup. If you choose not to setup a stash file, the HPE WASL SMS will prompt you for
the master password each time it starts up.

Do you want to setup the stash file? [yes]:

--------------------------------------------------------------------------------
Recovery password is used to recover the master password when the master password is
lost or forgotten. It is recommended to setup the recovery password.

Do you want to setup a recovery password? [yes]:

Please remember this password. If you forget this password, the HPE WASL SMS cannot be
recovered when the master password is lost or forgotten.

Enter the recovery password: **********
Confirm the recovery password: **********
================================================================================
Certificate Setup for HPE WASL SMS

SMS can be accessed from (chrome) browser via HTTPS (secure HTTP) protocol
SMS Server certificates should be setup for it to communicate securely

Choose the certificate setup type:

   1. Create a Self-signed certificate
      Lets you create a self-signed certificate automatically.


   2. Import a signed certificate
       Import an existing Server Certificate
       Lets you import Server certificate signed by the Enterprise CA or third-party
       CA
   3. Exit


Choose a setup type [1]:


Creating Self-Signed Certificate....

waslsms001.localdomain
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [IN]:
State or Province Name (2 letter code) [KA]:
Locality Name (eg, city) [Bangalore]:
Organization Name (eg, company) [Hewlett Packard Enterprise]:
Organizational Unit Name (eg, section) [Security Lab]:
Common Name (eg, YOUR name) [waslsms001]:
```

```
Email Address [user@hostname.com]:

Successfully created Self-signed certificates for HPE WASL SMS

Successfully set up the HPE WASL SMS
```

9.2 Setup showing import of signed certificate

A sample run of a setup showing importing signed certificates is as follows:

####### Make sure that the path to certificates and the actual certificate is accessible to waslsms user ####

```
# mkdir /sign
# chown waslsms:waslsms /sign/
# cp * /sign/
# chown waslsms:waslsms /sign/*
# ll /sign/
total 16
-rw------- 1 waslsms waslsms 1375 Oct 11 04:06 rootCA.pem
-rw------- 1 waslsms waslsms 1273 Oct 11 04:06 sms.crt
-rw-r--r-- 1 waslsms waslsms 1045 Oct 11 04:06 sms.csr
-rw-r--r-- 1 waslsms waslsms 1675 Oct 11 04:06 sms.key
```

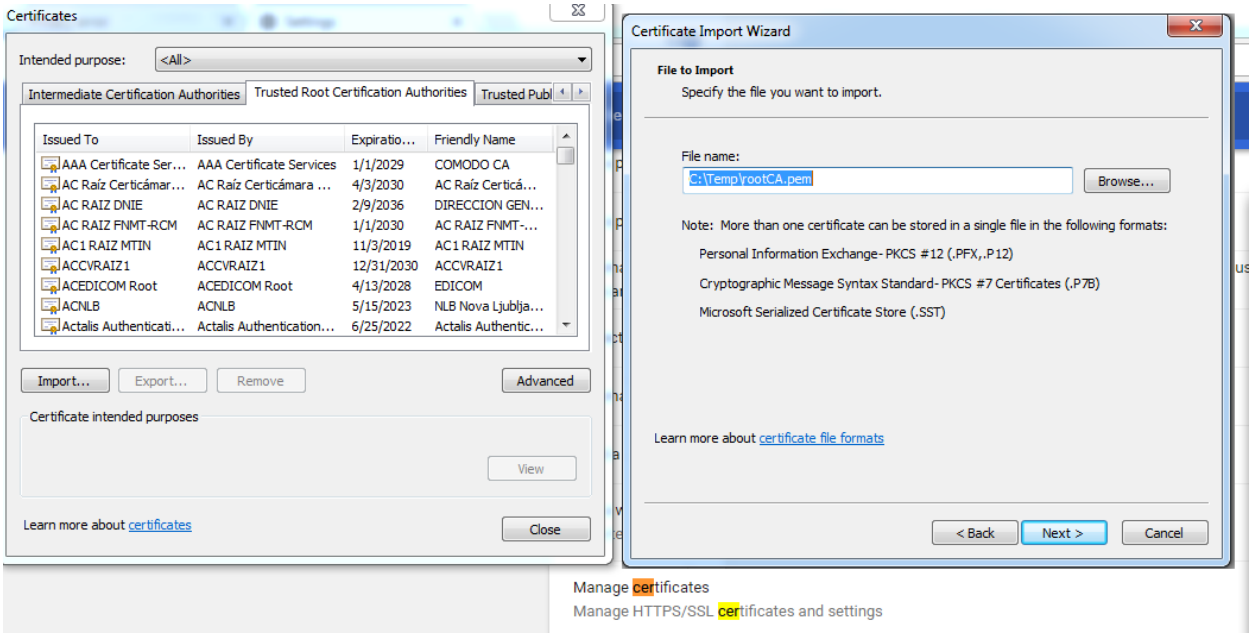
########## Do the WASL SMS setup or Just the certificate Setup ########################

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

OR

```
# /opt/hpe/wasl/sms/tools/wasl_sms.sh -setup_cert
-
-
================================================================================
Certificate Setup for HPE WASL SMS

SMS can be accessed from (chrome) browser via HTTPS (secure HTTP) protocol
SMS Server certificates should be setup for it to communicate securely

Choose the certificate setup type:

   1. Create a Self-signed certificate
      Lets you create a self-signed certificate automatically.

   2. Import a signed certificate
      Import an existing Server Certificate
      Lets you import Server certificate signed by the Enterprise CA or third-party CA

   0. Exit

Choose a setup type [1]:2


Note: All certificate and key files must be in PEM format.

Enter your server key location [/etc/ssl/certs/wasl/key.pem]:/sign/sms.key

Enter your server certificate location [/etc/ssl/certs/wasl/cert.pem]:/sign/sms.crt

Enter the CA certificate location [/etc/ssl/certs/wasl/ca.pem]:/sign/rootCA.pem

Successfully imported server certificates into HPE WASL SMS
Successfully set up the HPE WASL SMS
```

Now import the rootCA certificate to browser's trusted Root Certificate Authorities. (You can go to this via Menu->Settings->Advanced->Manage Certificate in Chrome browser).



9.3 WASL Logs

Following are the different source of Logs available on WASL SMS:

Location	Name	Description
/var/log/hpe_wasl_sms/	cert_gen.log	Certificate generation details
/var/log/hpe_wasl_sms/	wasl_sms.log	Main log file related to SMS. Many of the SMS errors gets logged here. We can enable HTTP/HTTPS access logs by setting config.web.logger to 'common' in configuration file: /opt/hpe/wasl/sms/config/custom_config.js This log file is auto rotated daily by the configuration in /etc/logrotate.d/hpe_wasl_sms file, using the standard Linux logrotate feature. The previous log files are compressed and saved in same directory. The old logs are retained based on the retention policy used in /etc/logrotate.conf file. You can change the retention period or the log rotation interval by editing the /etc/logrotate.d/hpe_wasl_sms file. For more information on using logtotate feature on Linux, see man page of logtotate.
/var/log/hpe_wasl_sms/	wasl_sms_daemon.log	Log created by the /etc/init.d/wasl_sms_init service
/var/log/hpe_wasl_sms/logs/	operationLog.txt	Logs of all operations performed on SMS
	WASLServerError.log	Any internal errors seen by WASL (currently only policy module errors)
SMS GUI Screen	Activity tab in SMS GUI	Activity link in SMS GUI provides details of all activities done in SMS and logged in the Couchbase server database.

Following are the different source of Logs available on individual Nodes that are managed by SMS:

Location	Name	Description
/var/opt/hpe/wasl/core/log/	./system/systemlog.txt	Generic logging of different activity on Node on system workload
	./hana/hanalog.txt	Generic logging of different activity on Node on SAP HANA workload

/var/opt/hpe/wasl/core/snapshot	./system/snapshot_<datetime>/snapshot/system_rollback.log	Logs related to system snapshots taken during remediation and rollback/reset
	./hana/snapshot_<datetime>/snapshot/snapshot.log	Logs related to SAP HANA snapshots taken during remediation and rollback/reset
	./hana/snapshot_<datetime>/reset.log	Logs related to SAP HANA rollback/reset
<user_home_dir_doing_node_page_automatic_install_from_SMS>	install_wasl_rpms.log	Logs related to Node Pakages auto installation and setup

Acronyms

Acronym	Abbreviation
WASL	Workload Aware Security for Linux
SMS	Security Management Station
RHEL	Red Hat Enterprise Linux
SLES	SUSE Linux Enterprise Server
SAP HANA	SAP High Performance Analytic Appliance
TDI	Tailored Data Center Integration
SP1, SP2, SP3	Service Pack 1, Service Pack 2, Service Pack 3
CS 500 / 900	ConvergedSystem 500 / 900
XCCDF	Extensible Configuration Checklist Description Format
GUI	Graphical User Interface
OpenSCAP	Open Security Containment and Automation Protocol
OVAL	Open Vulnerability and Assessment Language
FTP	File Transfer Protocol
DB	Database
SSH	Secure Shell
REST	Representational State Transfer
SFTP	Secure File Transfer Protocol