



**Hewlett Packard
Enterprise**

HPE Workload Aware Security Version 1.3.0 for Linux Install and Setup Guide

Abstract

This guide provides the installation and setup steps for HPE Workload Aware Security for Linux (WASL) version 1.3.0. 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.

Part Number: P12140-002
Published: June 2019
Edition: 1

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.

Confidential computer software. Valid license from Hewlett Packard Enterprise 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.

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[®], 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.

Contents

About this guide.....	5
New and changed information.....	5
Revision History.....	6
Workload Aware Security for Linux Overview.....	7
Supported hypervisors and versions.....	7
Browser requirement.....	7
Deployment and architecture.....	8
WASL ISO image content.....	10
Signature verification.....	11
Verify using the GPG method.....	11
Verify using the RPM method.....	11
Deploying the WASL virtual appliance.....	13
Using the VMware vSphere (5.0 or newer) client.....	13
Using the VMware ESXi web interface.....	16
Logging in to the console.....	20
Locking and unlocking the root account.....	23
Unlocking the root account.....	23
Locking the root account.....	23
Setting up and running WASL SMS.....	24
Couchbase server setup.....	24
SMS security settings setup.....	24
Certificates configuration.....	25
Starting and stopping SMS.....	26
Starting the SMS.....	26
Stopping the SMS.....	26
Logging in to the SMS.....	27
Node packages installation and setup.....	28
Prerequisites for installing Node packages.....	28
Automatic Node package installation and setup from SMS.....	29
Manual Node package installation and setup from node.....	31
Installing node packages.....	31
Run <code>wasl-setup</code> to provide user privileges.....	32
Create certificates for waslhanauser users.....	34

Add sudoers for waslhanauer	34
Migrating to WASL Version 1.2 or later.....	35
Backup WASL SMS Version 1.1.....	35
Migrate to WASL Version 1.2 or later.....	36
Backup of WASL SMS Virtual Appliance Version 1.2 or later.....	37
Removing and reinstalling node packages.....	39
Extending the disk partitions.....	41
Best practices.....	43
Websites.....	44
Support and other resources.....	45
Accessing Hewlett Packard Enterprise Support.....	45
Accessing updates.....	45
Customer self repair.....	46
Remote support.....	46
Warranty information.....	46
Regulatory information.....	47
Documentation feedback.....	47
Sample run of SMS setup.....	48
Setup showing import of signed certificate.....	52
WASL Logs.....	53
Hardened WASL SMS appliance	55
Disk partitions extension.....	55
Acronyms.....	57

About this guide

New and changed information

Changes to the P12140-002 manual

- Updated standard profiles details in the [Workload Aware Security for Linux Overview](#) section.
- Updated [WASL ISO image content](#) section.
- Updated operating system details in the [Prerequisites for installing Node packages](#) section.
- Updated [Stopping the SMS](#) section.
- Updated version details in the following sections:
 - [Migrating to WASL Version 1.2 or later](#)
 - [Backup of WASL SMS Virtual Appliance Version 1.2 or later](#)
- Added [Extending the disk partitions](#) section.
- Added [Hardened WASL SMS appliance](#) section.
- Added [Disk partitions extension](#) section.

Changes to the P12140-001 manual

Added following sections:

- [Supported hypervisors and versions](#)
- [Browser requirements](#)
- [WASL ISO Image Content](#)
- [Deploying the appliance](#)
- [Logging in to the console](#)
- [Migrating to WASL Version 1.2](#)

Updated details of the following sections:

- [Signature Verification](#)
- [Setting up and running WASL SMS](#)
- [Starting and stopping SMS](#)
- [Node packages installation and setup](#)
- [Removing and reinstalling node packages](#)

Revision History

Part Number	Published
P12140-002	June 2019
P12140-001	December 2018
P03767-001	April 2018

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 together by a single-click from centralized system (called Security Management Station). WASL can evaluate a workload (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 and shows the details of specific evaluations and remediations. WASL also offers a feature to roll back any remediation done and gets back the workload configuration to a previously known configuration state.

WASL is shipped with basic and advanced licensing. Basic license offers SUSE Linux Enterprise Server (SLES) and Red Hat Enterprise Linux (RHEL) OS hardening profiles whereas advanced licensing offers SAP HANA profiles and basic licensing.

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

- OS Security for SLES 12 (SP1, SP2, SP3, and SP4)
- Draft OS Security for SLES 15
- OS Security for SLES SAP HANA 12 (SP1, SP2, SP3, and SP4) (OS Security tailored for SAP HANA database)
- Draft OS Security for SLES SAP HANA 15 (OS Security tailored for SAP HANA database)
- OS Security for RHEL 7 (7.2, 7.3, 7.4, 7.5, and 7.6)
- SAP HANA 1.0 Database
- SAP HANA 2.0 Database
- OS extended profile for SLES 12 SAP HANA (SP1, SP2, SP3, and SP4) and SLES SAP HANA 15 (extra OS protection for securing SAP HANA database)

Supported hypervisors and versions

WASL version 1.2 is released as a virtual appliance and is supported on VMWare vSphere ESXi (6.0, 6.5, and 6.7) hypervisor.

Following configurations are required to host the WASL virtual appliance:

- Four 4-GHz or greater virtual CPUs
- 16 GB of memory
- 40 GB of thick-provisioned disk space

NOTE: You can increase the disk space based on the number of planned workloads and operations. Each evaluation or remediation operation requires 5 MB of disk space to store the reports. 40 GB of disk space can store up to 8,000 reports of evaluation or remediation operations.

To increase the disk space, see [Extending the disk partition](#) section.

Browser requirement

Use Chrome Version 62.0.3202.94 or above to access WASL Security Management Station (SMS).

Deployment and architecture

A typical deployment of WASL consists of a 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 following workloads:

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

The SMS is a web-based application accessible on HTTPS default port (443). It offers a rich set of GUI that is accessible through Chrome and supports a varied set of roles for users to log in and perform activities.

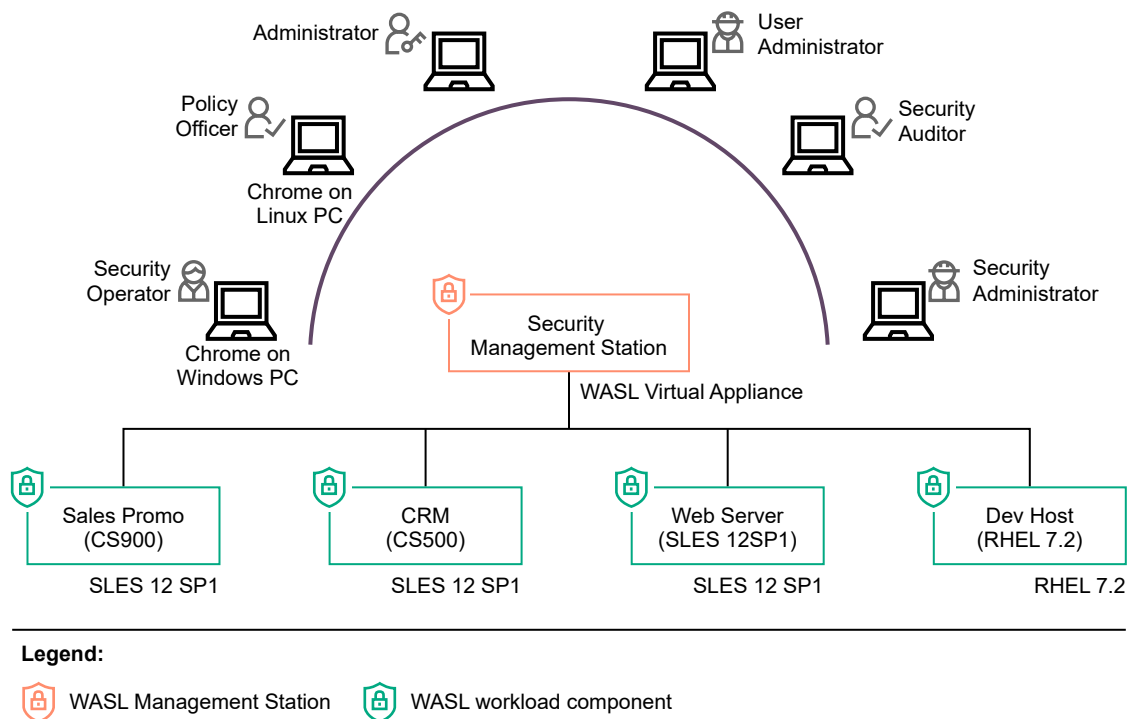


Figure 1: WASL Deployment Scenario

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 can also 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 through default port 8091). 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 an 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.

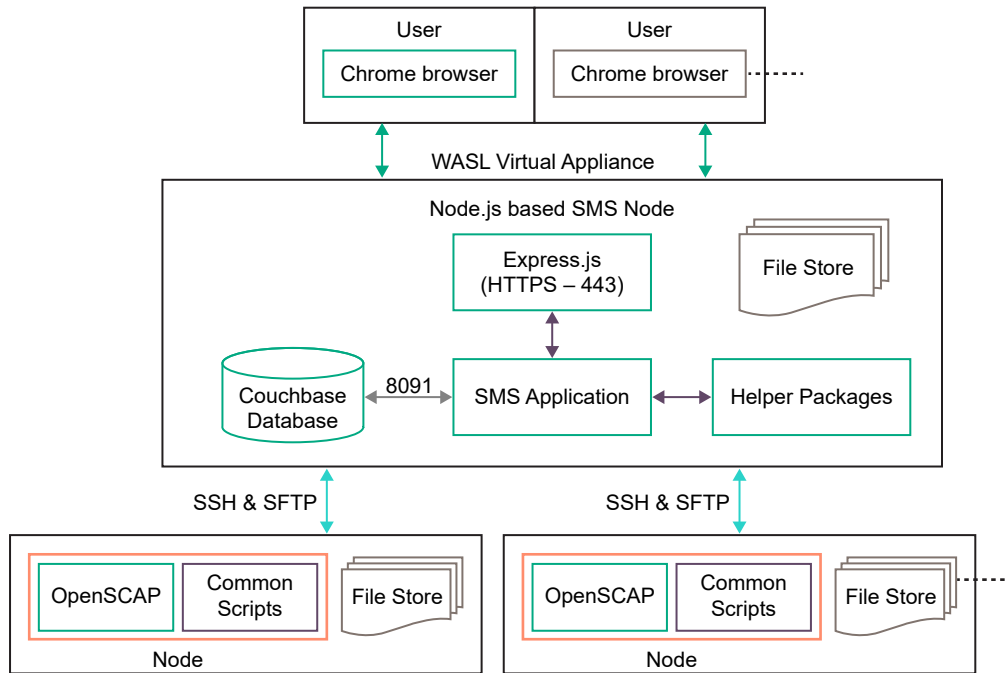


Figure 2: WASL Architecture flow

WASL ISO image content

The following is the list of packages bundled in the ISO image:

- WASL Virtual Appliance is available at */WASL/VMware* directory
- Backup Package for WASL SMS 1.1 is available at */WASL/SLES/SLES11/* directory
- Node Packages for SLES 12 are available at */WASL_Node/SLES/SLES12/* directory
- Node Packages for RHEL 7 are available at */WASL_Node/RedHat/RedHat7/* directory

```
/WASL_Read_Before_Install.txt
/End_User_License_Agreement.PDF
/WASL
/WASL/VMware
/WASL/VMware/Q8K94-11003.ova
/WASL/VMware/Q8K94-11003.ova.sig
/MISC
/MISC/SLES
/MISC/SLES/SLES11
/MISC/SLES/SLES11/hpe-wasl-sms-backup-1.1.0-1.x86_64.rpm
/WASL_Node/SLES
/WASL_Node/SLES/SLES11
/WASL_Node/SLES/SLES11/hpe_wasl_os-1.3.0-1.sles11.x86_64.rpm
/WASL_Node/SLES/SLES11/hpe_wasl_saphana-1.3.0-1.sles11.x86_64.rpm
/WASL_Node/SLES/SLES11/hpe_wasl_core-1.3.0-1.sles11.x86_64.rpm
/WASL_Node/SLES/SLES11/openscap_1-1.2.15-1.0.x86_64.rpm
/WASL_Node/SLES/SLES12
/WASL_Node/SLES/SLES12/hpe_wasl_os-1.3.0-1.sles12.x86_64.rpm
/WASL_Node/SLES/SLES12/hpe_wasl_core-1.3.0-1.sles12.x86_64.rpm
/WASL_Node/SLES/SLES12/openscap_1-1.2.15-1.0.x86_64.rpm
/WASL_Node/SLES/SLES12/hpe_wasl_saphana-1.3.0-1.sles12.x86_64.rpm
/WASL_Node/RedHat
/WASL_Node/RedHat/RedHat7
/WASL_Node/RedHat/RedHat7/hpe_wasl_os-1.3.0-1.rhel7.x86_64.rpm
/WASL_Node/RedHat/RedHat7/hpe_wasl_saphana-1.3.0-1.rhel7.x86_64.rpm
/WASL_Node/RedHat/RedHat7/hpe_wasl_core-1.3.0-1.rhel7.x86_64.rpm
/WASL_Node/RedHat/RedHat7/openscap_1-1.2.15-1.0.x86_64.rpm
```

Signature verification

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

Download the Keys

To download the keys:

1. Copy the compressed tar file *HPE-GPG-Public-Keys.tar.gz* from <https://downloads.hpe.com/pub/keys/HPE-GPG-Public-Keys.tar.gz> to the local directory.
2. Transfer this keys compressed tar file to the client machine from where the WASL virtual appliance is deployed.
3. To verify the Node Packages, copy the tar file to the WASL Node where the node packages must be installed.

Verify using the GPG method

Do the following to verify the WASL Virtual Appliance:

Procedure

1. Login as an administrator.
2. Run the following command to import the public keys, one at a time:

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

3. Run the command to verify the Virtual Appliance:

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

You can find the *<filename>.ova.sig* 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 the file does not pass the verification or the HPE public key is not installed, it displays the following error:

```
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.

Verify using the RPM method

Do the following to verify WASL Node packages and WASL SMS Version 1.1.0 Backup package:

Procedure

1. Login as a root user.
2. Run the following command to import the public keys, one at a time:

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

For example:

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

3. Run the `rpm --checksig` command to validate and verify the digital signature of the signed file:

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

The following command output indicates the validity of the signature:

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

If the file does not pass the verification or the HPE public key is not installed, it displays the following error:

```
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.

NOTE: For more information, see [HPE GPG or RPM Signature Verification](#).

Deploying the WASL virtual appliance

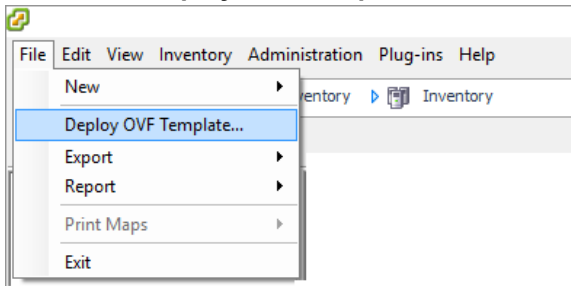
You can deploy the WASL virtual appliance in the following ways:

- Using the VMware vSphere (5.0 or newer) client
- Using the VMware vSphere web interface

Using the VMware vSphere (5.0 or newer) client

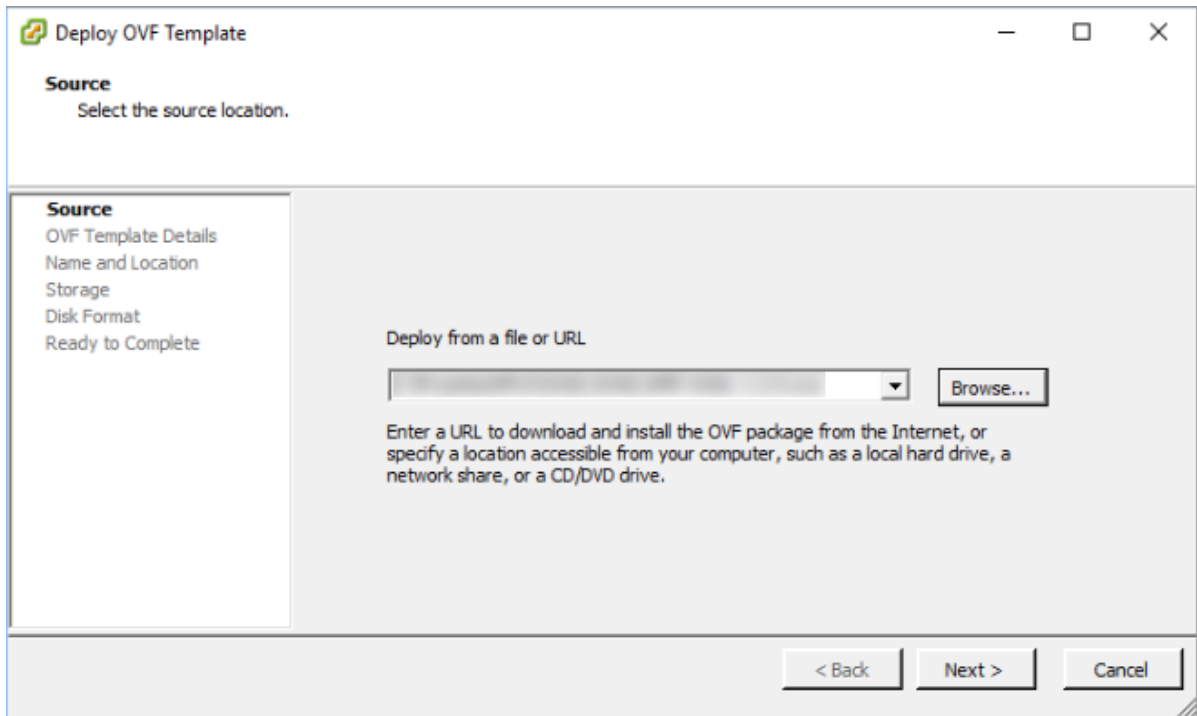
Procedure

1. Log on to the system.
2. Click **File > Deploy OVF Template....**

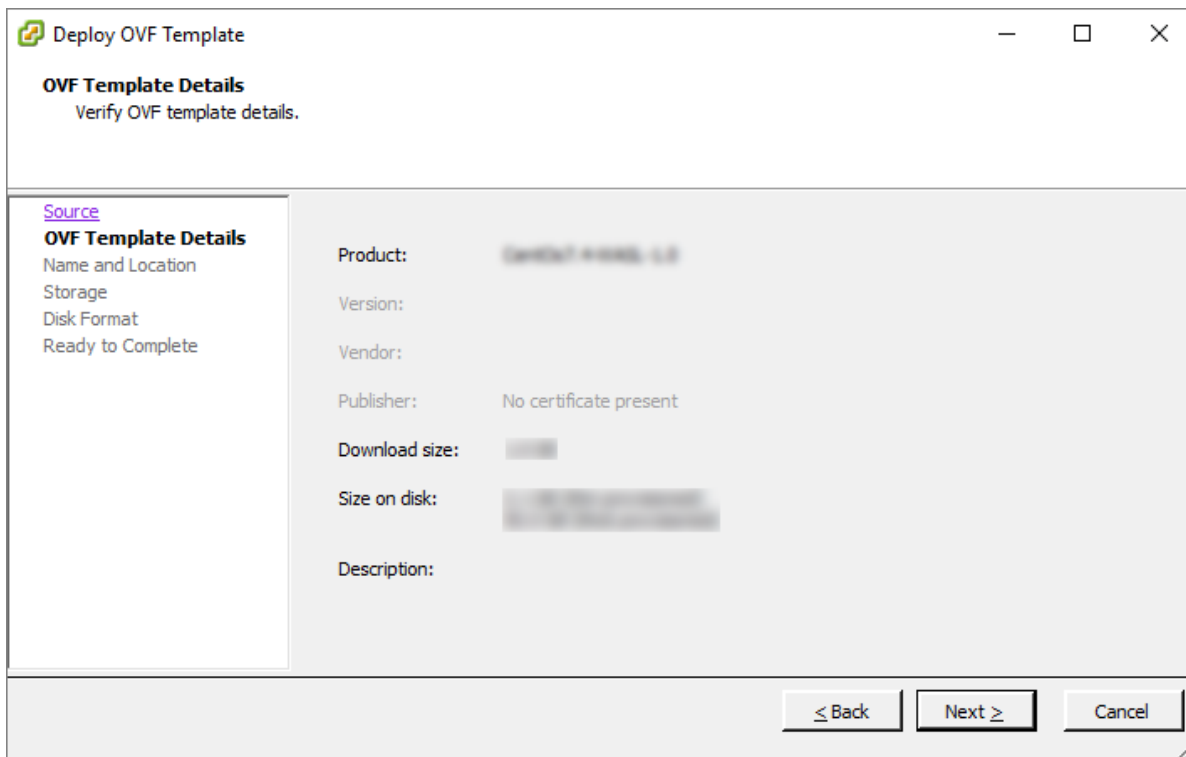


3. Click **Browse** to select the OVF template or OVA file from the location where the file is stored and click **Next**.

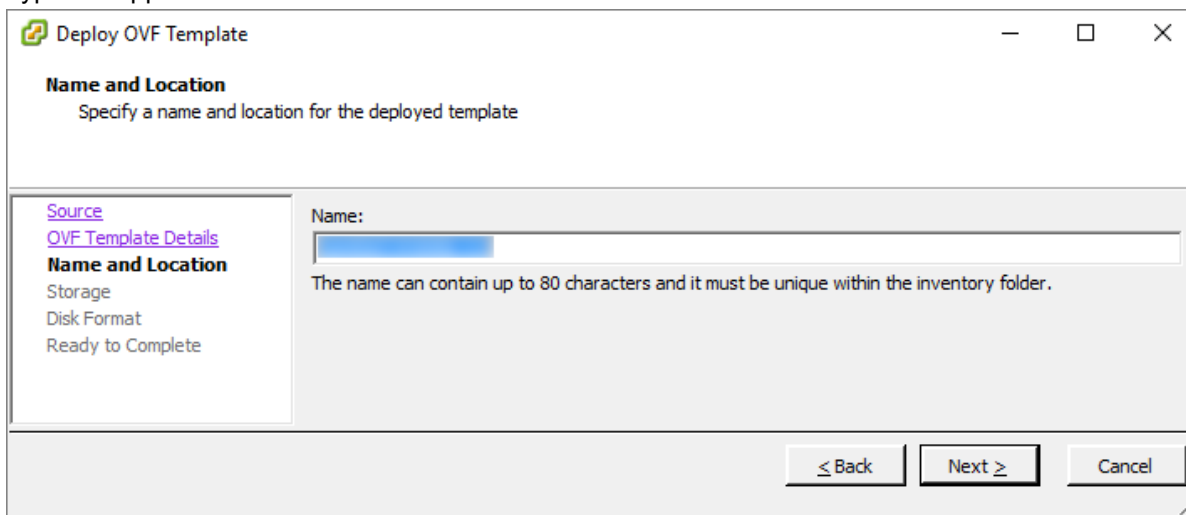
The OVA file is available at *WASL/VMware* in the ISO Image file.



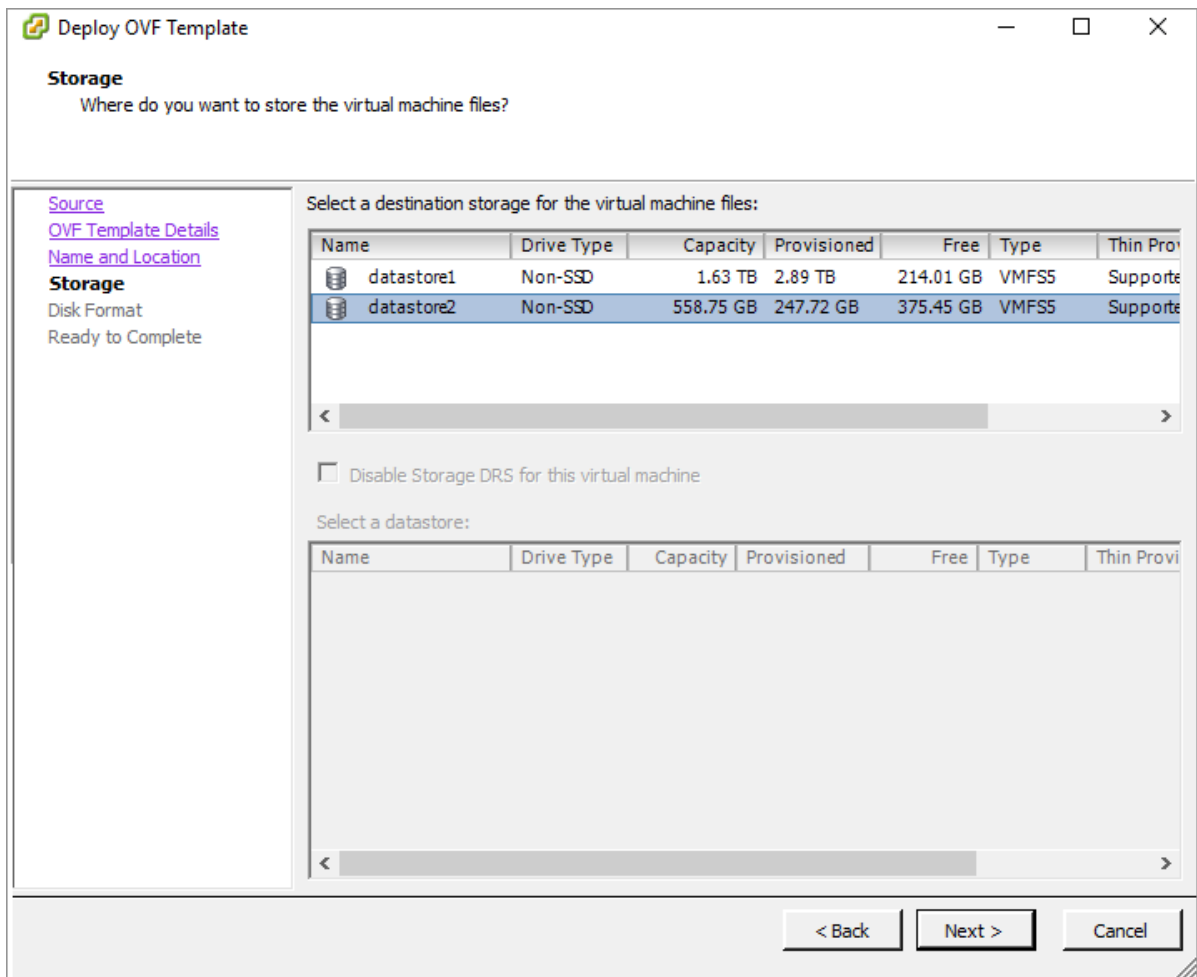
4. Verify the **OVF Template Details** and click **Next**.



5. Type the appliance name and click **Next**.

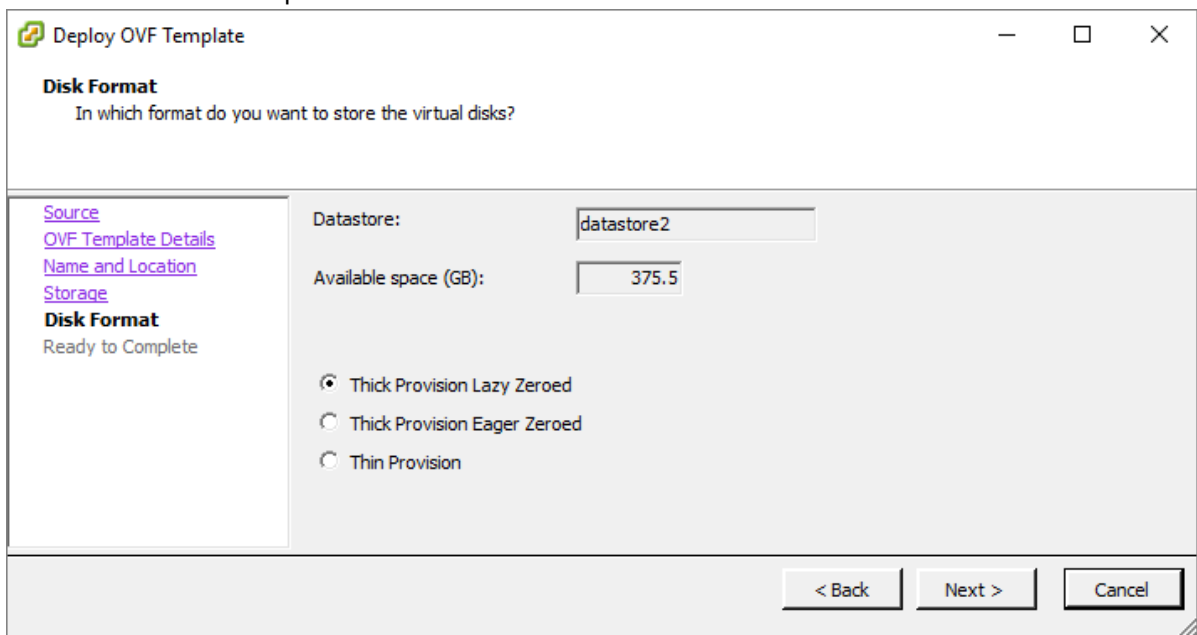


6. Select the required storage location to store the virtual machine files and click **Next**.

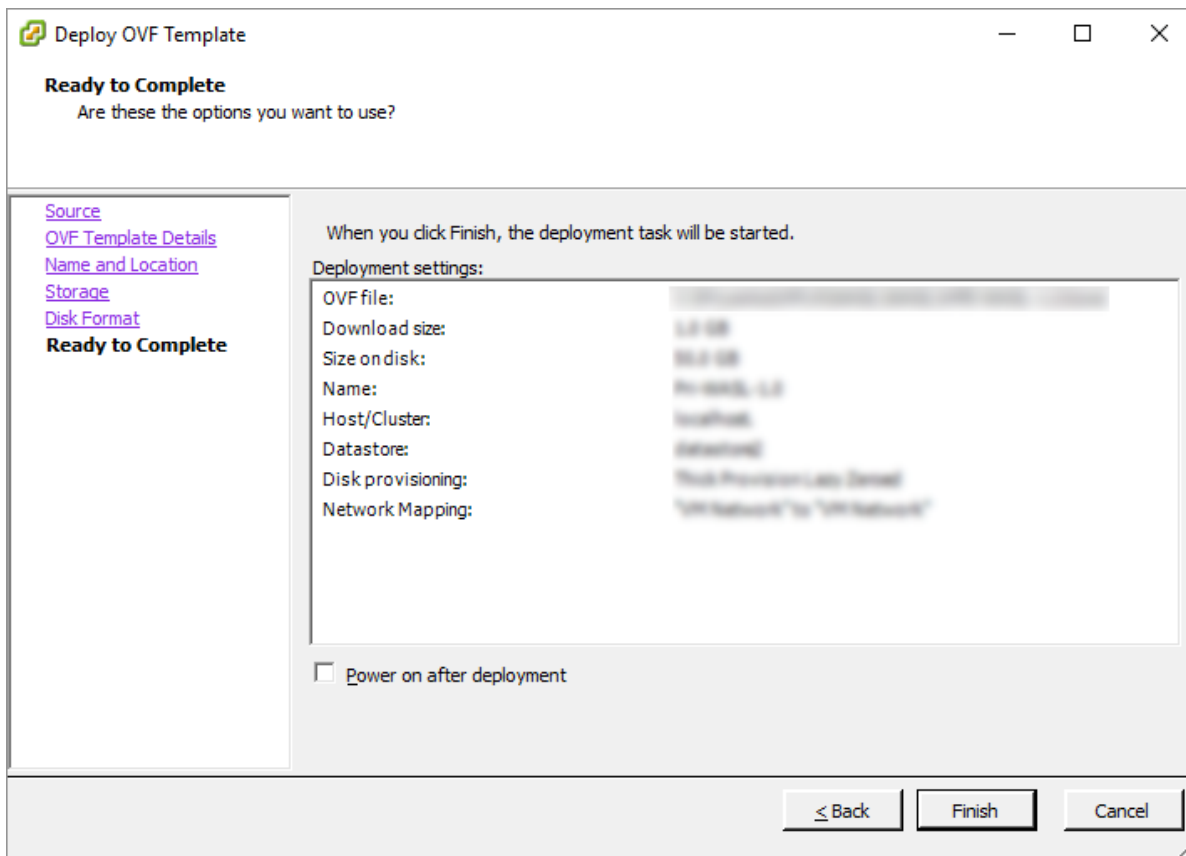


NOTE: Based on the requirement, select the storage such as space, data type, and accessibility.

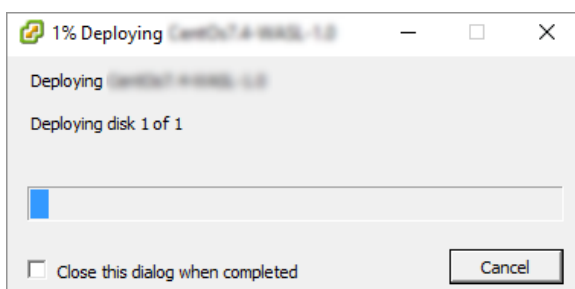
7. Select the disk format option to store the virtual disks and click **Next**.



8. Verify the **Deployment settings** and click **Finish**.



The window displays the status of the deployment process in progress.

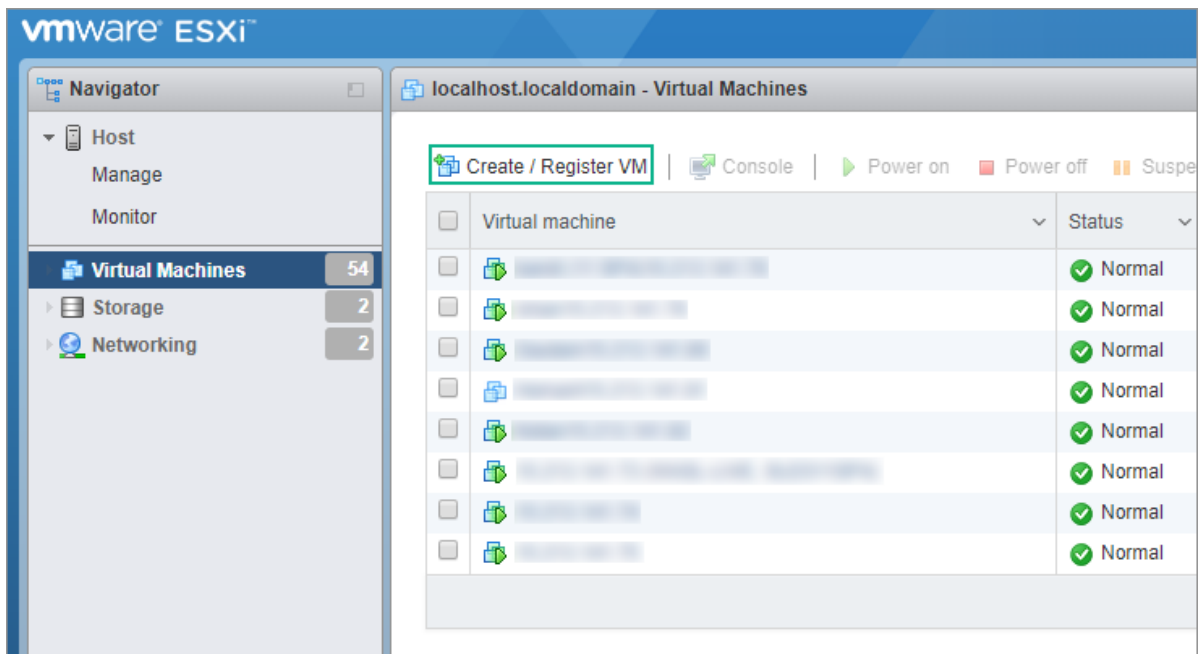


9. Once the WASL virtual appliance is deployed, click the **Virtual Machines** tab.
The system displays the list of available virtual machines.
10. Right-click the required virtual machine name, point to **Power**, and click **Power On** to start the virtual machine.

Using the VMware ESXi web interface

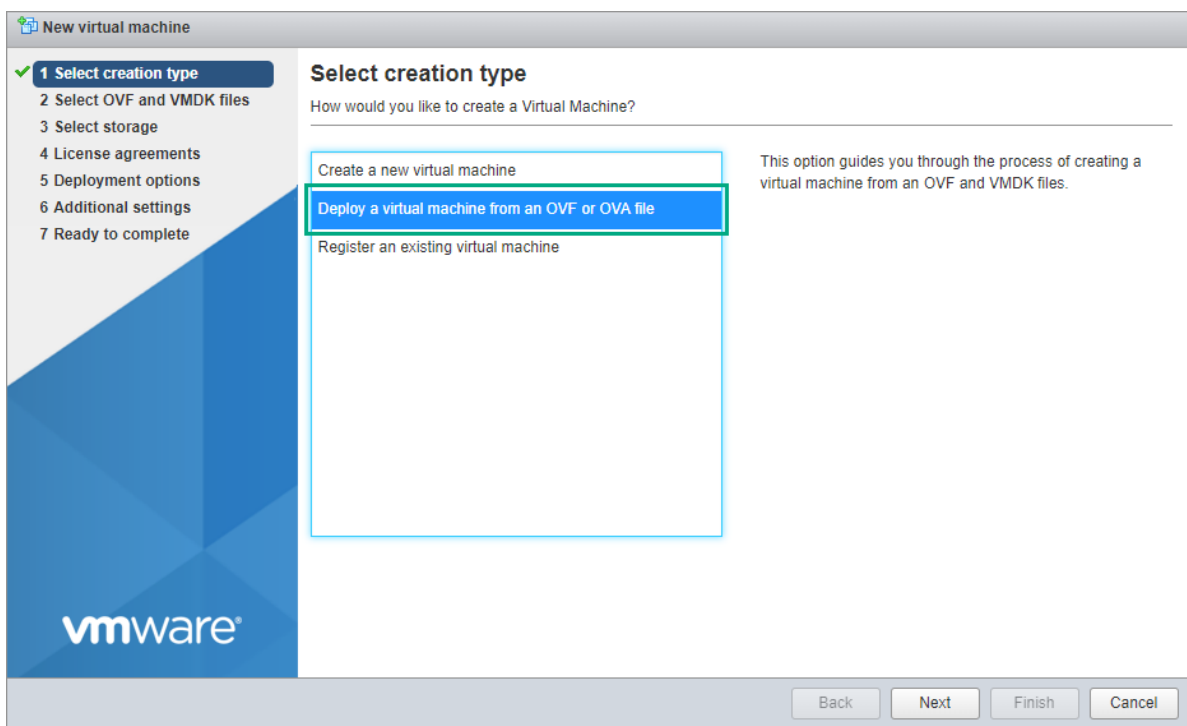
Procedure

1. Log on to the VMware ESXi.
2. Type the **User name** and **Password** and click **Log in**.
3. In the **Navigator** pane, click **Virtual Machines**.



4. Click **Create / Register VM**.

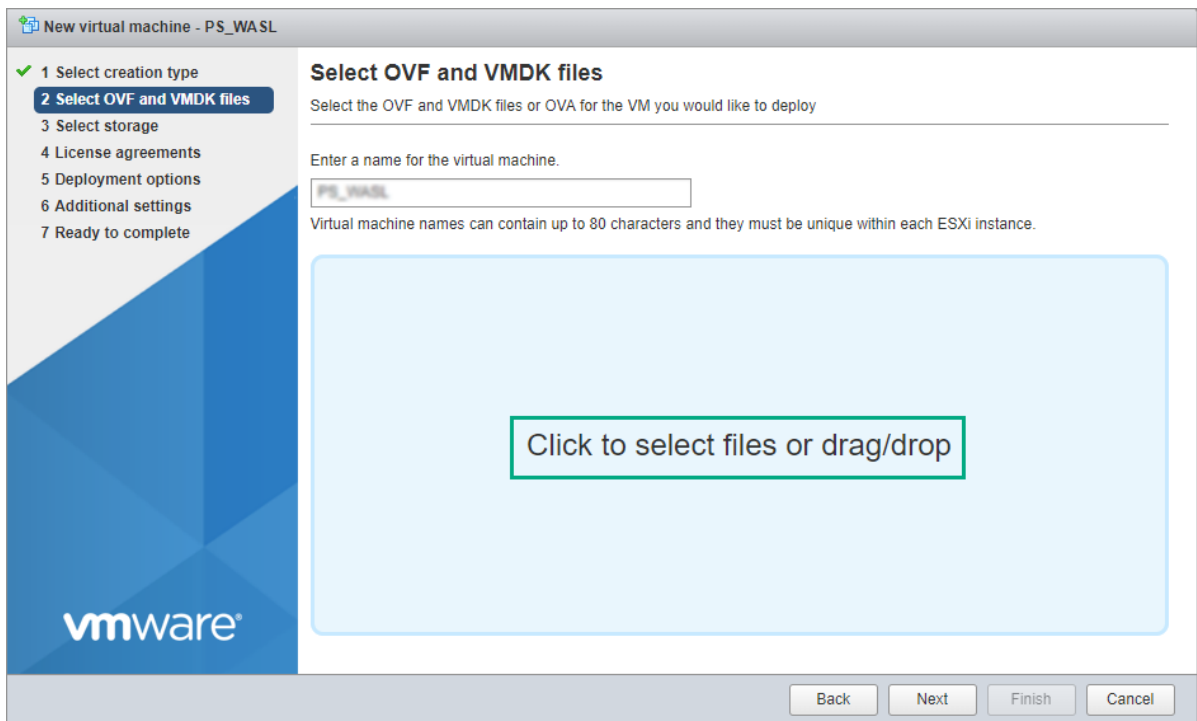
The **Select creation type** dialog box appears. It prompts you to select the creation type.



5. Click the **Deploy a virtual machine from an OVF or OVA file** and click **Next**.

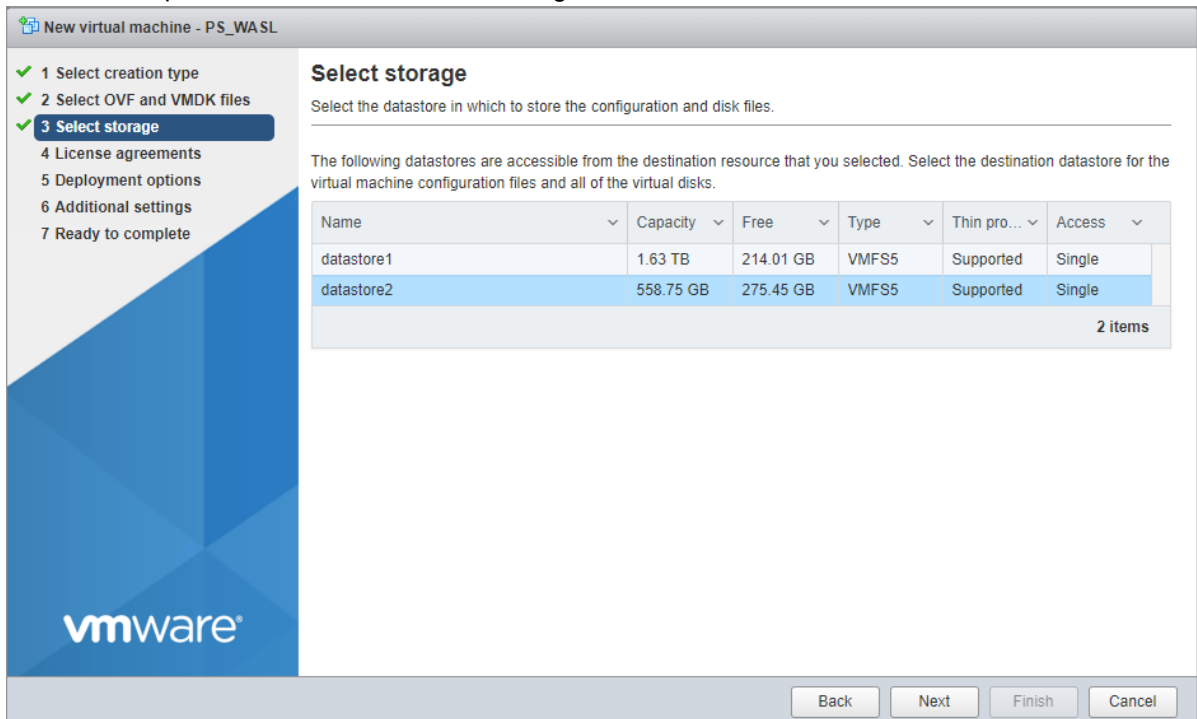
The **Select OVF and VMDK files** dialog box appears.

6. Enter the name for the virtual machine.
7. Click to select the template and click **Next**.
You can also drag and drop the template.



The **Select storage** dialog box appears.

8. Select the required datastore to store the configuration and disk files and click **Next**.



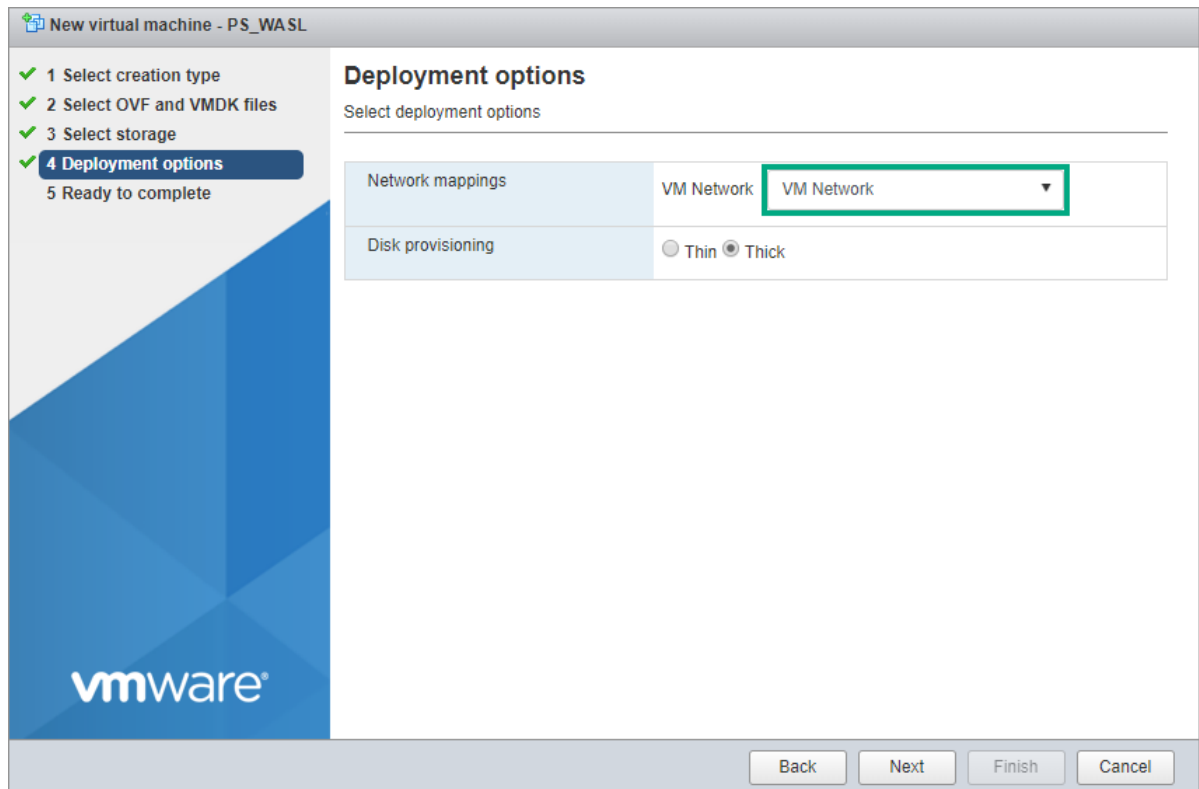
The **Deployment options** dialog box appears.

NOTE: Based on the requirement, select the storage such as space, data type, and accessibility.

9. Select **VM Network** from the drop-down list box.

The WASL SMS should be accessible on the selected network, hence select an appropriate network.

10. Click the required option to select **Disk provisioning** and click **Next**.



The **Ready to complete** dialog box appears.

11. Verify the settings details and click **Finish**.

The progress report appears. Once the VM is deployed, it shows the result as **Completed successfully**.

12. In the **Navigator** pane, click **Virtual Machines**.

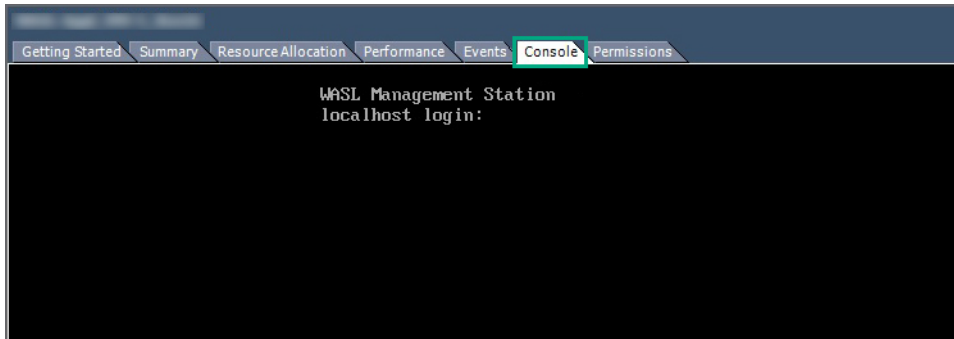
13. Click the checkbox for the required virtual machine and click **Power on** to start the virtual machine.

Logging in to the console

Log in to the console and configure the network using Network Manager Text User Interface (nmtui) tool.

Procedure

1. Click the **Console** tab.



2. Type the Username **wasladmin** and the Password.

The default password is **wasladmin**.

The system prompts you to change the password when you log in for the first time. Change the password.

NOTE:

- Starting from WASI Version 1.3.0, the password must be at least 14 characters in length. It must contain a number, a special character, and an uppercase letter.
- If it is Dynamic Host Configuration Protocol (DHCP) - enabled environment, WASL virtual appliance automatically picks up the IP address. You do not need to configure the IP address manually. After logging in to the console, run `ip` a command or click the **Summary** tab to determine the initial IP address for the virtual appliance.

3. Run `sudo nmtui` command to open NetworkManager Text User Interface tool to statically configure the IP address for WASL virtual appliance.

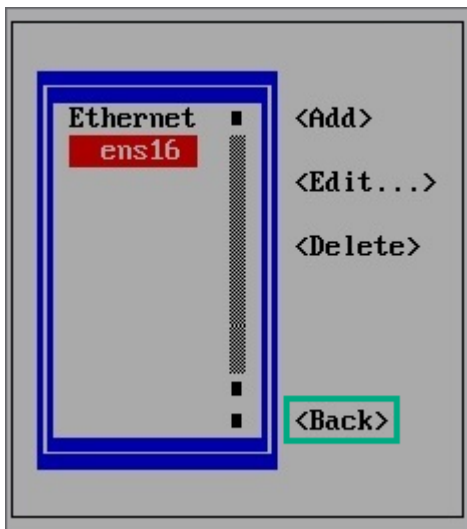
The **NetworkManager TUI** window appears.

4. Use Tab key or Up, Down, Left, and Right arrow key to select option in nmtui tool window. Select **Edit a connection** option, and press Enter key.



The system prompts you to select the Ethernet device from the list.

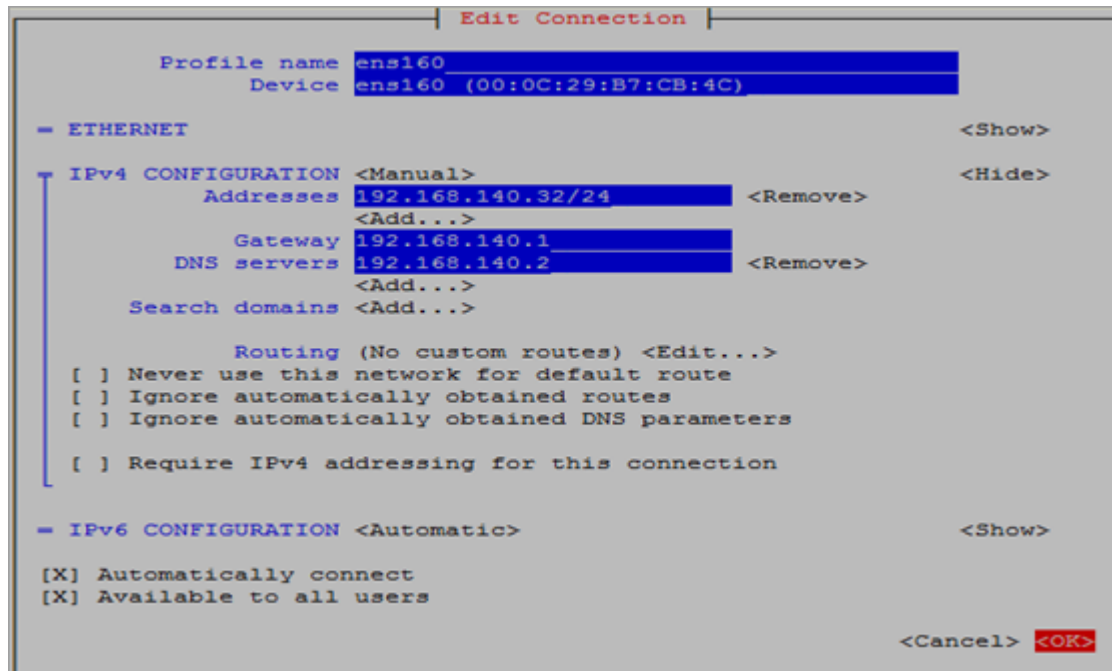
5. Select the Ethernet device to set the static IP address.



6. Select **<Edit... >** option and then press Enter key.

The **Edit Connection** window appears.

- a. Select IPv4 CONFIGURATION and press Enter key, and select **Manual** option.
- b. Select **show** option and press Enter key.



- c. Go to **Addresses** option, select the **<Add...>** option, and press **Enter** key.
 - d. Type the IP address and netmask bits in the Addresses input field.
For example: 192.168.140.32/24. In this example, 192.168.140.32 is the IP address and 24 is the netmask bits which indicates netmask is 255.255.255.0.

You can add more IP addresses using the **<Add...>** option or remove the specific IP address with the **<Remove>** option.
 - e. Go to **Gateway** input field and type the Gateway address.
 - f. Go to **DNS servers** option, select **<Add...>** option and press **Enter** key.
 - g. Type DNS server IP address.
 - h. Go to **<OK>** option and press Enter key.
7. Select **<Back>** option and press Enter key. Select **Quit** option to close nmtui tool window.



8. Run `sudo systemctl restart network` command. Once the network is configured and available for access, set up WASL.
9. Run `ip a` command to verify whether the IP address is configured or not.

Locking and unlocking the root account

By default, the root account is locked. Use wasladmin account to perform all admin activity.

You can unlock the root account to install any new or updated WASL Policy RPM packages or to resolve WASL Virtual Appliance-related issues (if any).

Unlocking the root account

Procedure

1. Run the following command as wasladmin user:

```
# sudo /opt/hpe/wasl/sms/tools/lockunlock_root.sh -unlock
```

2. Type the wasladmin password.
3. Type the new password for root user.
4. Retype the new password.

Locking the root account

Procedure

Run the following command:

```
# sudo /opt/hpe/wasl/sms/tools/lockunlock_root.sh -lock
```

```
root user is successfully locked .
```

NOTE: After completing the required activity, HPE recommends to lock the root account immediately.

Setting up and running WASL SMS

After configuring the WASL virtual appliance, set up WASL for the first time before starting or using it.

Procedure

1. Log in as a *wasladmin* user.
2. Run the following script with `-setup` option:

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

This command runs as *wasladmin* user and configures:

- **Couchbase Server (Database for SMS)**
- **SMS security settings (Master and Recovery key)**
- **Certificates (Enables HTTPS connection)**

It also provide following options:

- **Migrate to WASL Version 1.2¹**
- **Start WASL (at the end of the setup)**

The command prompts you to enter multiple data as explained in the subsequent section.

NOTE:

- The `wasl_sms.sh` is a wrapper script and can be used for doing command line operations such as starting and stopping of WASL SMS, resetting master and recovery key passwords, and so on.
- Run the script with `-help` option to view all the available options:

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

The `wasl_sms.sh` does a `sudo` to `waslsms` user before doing any operation.

Couchbase server setup

The Couchbase Server setup configures an instance of Couchbase Server Community Edition for WASL SMS using the predefined defaults. A new Couchbase cluster with username Administrator is created.

SMS security settings setup

This phase requires adding the master and recovery passwords to protect the critical data.

Master key

This is a root key that protects the critical security data in WASL SMS. A separate master password is required to encrypt this Master key.

¹ It is required only when a user is migrating to WASL Version 1.2.

- Master password must be provided while starting WASL SMS, so that WASL SMS can encrypt or decrypt the critical data.
- Master password can be stored during the setup in a stash file (*/opt/hpe/wasl/sms/data/stashfile*). If the stash file is set up, SMS picks the password from the stash file and starts SMS automatically during the WASL virtual appliance startup.

If the master password is not stored in the stash file, start the WASL SMS manually after starting the WASL virtual appliance. To start WASL SMS manually, see the [Starting and stopping SMS](#).

Recovery Key

It is used to recover the master password when the master password is lost or forgotten. A separate recovery password is required to encrypt this Recovery key. Use of Recovery key is optional.

Resetting the master and recovery password

Master key and Recovery key can be changed only if the current password (master and recovery) is known or stored in the stash file.

Run the following command to reset the master password or recovery password:

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

Certificates configuration

SMS sets up the certificate required for the HTTPS connection to browsers. Following are the two options to configure the certificates:

- Create a self-signed certificate — SMS creates a self-signed certificate.
- Import a signed certificate — You can 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, use the following command:

```
/opt/hpe/wasl/sms/tools/wasl_sms.sh -setup_cert
```

NOTE: The self-signed certificate expires in 365 days by default.

After the certificate is created, the HPE WASL SMS sets up successfully. If you are migrating to WASL Version 1.2, the system prompts you to restore the WASL SMS data. For more details, see the [WASL SMS Migration](#).

Starting and stopping SMS

Once you start or stop the WASL virtual appliance, the SMS starts and stops automatically as the master password is stored in the stash file.

If you want to manually start or stop the SMS, do the following:

Procedure

1. Starting the SMS
2. Stopping the SMS
3. Logging in to the SMS

Starting the SMS

Prerequisites

Ensure the couchbase-server service is running.

Procedure

1. Run the following command to check if the couchbase-server service is running or not:

```
sudo systemctl status couchbase-server
```

2. Run the following command to start couchbase-server service:

```
sudo systemctl start couchbase-server
```

NOTE: Couchbase runs as couchbase user.

3. Start the SMS either from command line or by starting SMS service:

- If the master password is not stored in the stash file:

- a. Run the following command to start SMS from command line:

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

- b. Enter the master password.

- If the master password is stored in the stash file:

- Run the following command to start SMS from command line

```
sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -start -use_stash_file
```

Or

- Run the following command to start or restart the hpe-wasl-sms service:

```
sudo systemctl start hpe-wasl-sms
```

Stopping the SMS

1. Run the following command:

- To stop the SMS service:

```
sudo systemctl stop hpe-wasl-sms
```

or

- To stop SMS through the command line argument:

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

If the master password is not stored in the stash file, enter the master password when the command prompts for it.

2. Run the following command to ensure that the process related to `wasl` is stopped:

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

3. Run the following command to stop the couchbase-server service:

```
sudo systemctl stop couchbase-server
```

NOTE:

- If you are using `systemctl` command to start the SMS, use `systemctl` command to stop the SMS. If you are using shell (`wasl_sms.sh`) command, then use shell command to stop the SMS.
 - If you are using Couchbase Server as a database for other applications apart from SMS, do not stop couchbase-server service.
-

Logging in to the SMS

Prerequisites

Use Chrome browser to access the SMS webpage.

Procedure

1. Type the URL `https://<IPAddress of SMS host>` into the address bar of the browser.
2. Type the **Username** and **Password** using the default administrator account.
Username = `admin` and Password = `admin`

The system prompts you to change the password on first login.

NOTE:

- After logging in to the system for the first time, the user must change the password.
 - The administrator account is for administrative purposes only. HPE recommends creating accounts with different roles to perform various operations in SMS.
-

Node packages installation and setup

Node packages include all the required and dependent products for securing the individual workloads and must 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).

Prerequisites for installing Node packages

Prerequisites

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

Items	Requirements
Hardware	<ul style="list-style-type: none">• 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 <p>For a detailed list of supported servers, see the <i>WASL Quick Specs</i>.</p>
Operating System	<ul style="list-style-type: none">• SUSE Linux Enterprise Server 12 (SP1, SP2, SP3, and SP4)• SUSE Linux Enterprise Server for SAP Applications 12 (SP1, SP2, SP3, and SP4)• SUSE Linux Enterprise Server 15• SUSE Linux Enterprise Server for SAP Applications 15• Red Hat Enterprise Linux 7 (7.2, 7.3 , 7.4, 7.5, and 7.6)
List of software that are required for WASL base scripts	Multiple package such as python, OpenSSH, libopenssl, gconf2, libstdc++, and so on, are part of base operating system. If these packages are not available on the target Node, install them.
Disk requirement	40 GB minimum

Table Continued

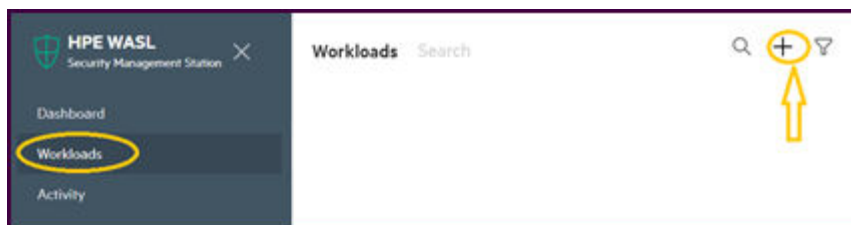
Items	Requirements
List of software that are required for Operating System security	Multiple package such as perl-base (on SLES), perl (on RHEL), audit, sed, gawk, and so on, are part of base operating system.
Software packages required for SAP HANA security	<ul style="list-style-type: none"> • One of the following versions of SAP HANA Database is required: <ul style="list-style-type: none"> ◦ 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 2.0 SPS03 • SAP HANA Client - HDB_CLIENT provided with SAP HANA database. (WASL product uses SAP HANA Client - HDB_CLIENT tool provided along with SAP HANA database to connect with the SAP HANA database. WASL searches for this tool either at <code>/usr/sap/hdbclient</code> or <code>/home/washanuser/sap/hdbclient</code> location. If HDB_CLIENT tool is not installed in any of these locations, then WASL can connect as SAP HANA OS admin user (<code><sid>adm</code>) for all WASL operations and can search for HDB_CLIENT tool in different locations. For more details, see Add or Register Workload section of <i>WASL User Guide</i>.) • On SLES for SAP Applications 15, python-enum34 package is not included in the base operating system. It needs to be installed on the target node to perform the security operations using SAP HANA policies on SLES 15.

Automatic Node package installation and setup from SMS

Do the following to automatically install and setup SMS on the Node:

Procedure

1. Log in to the SMS web service.
2. Click the + icon.



3. Click the + icon.
The **Add Node** screen appears.

SMS connects to this Node through secure shell using the credentials entered in the **Add Node** screen to login and perform installation and setup.

If the **Host Username** entered in the **Add Node** screen is not `root`, then do the following steps before installing on the required Node:

- On a **SLES 12 Node**, create `/etc/sudoers.d/waslcore_install` file with following content:

```

Cmdnd_Alias WASL_NODEKITS = /usr/bin/zypper --non-interactive --repo local --no-gpg-checks install hpe_wasl_core.rpm, \
/usr/bin/zypper --non-interactive --repo local --no-gpg-checks install hpe_wasl_os.rpm, \
/usr/bin/zypper --non-interactive --repo local --no-gpg-checks install hpe_wasl_saphana.rpm, \
/usr/bin/zypper --non-interactive --repo local --no-gpg-checks install openscap.rpm
Cmdnd_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. 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:

```

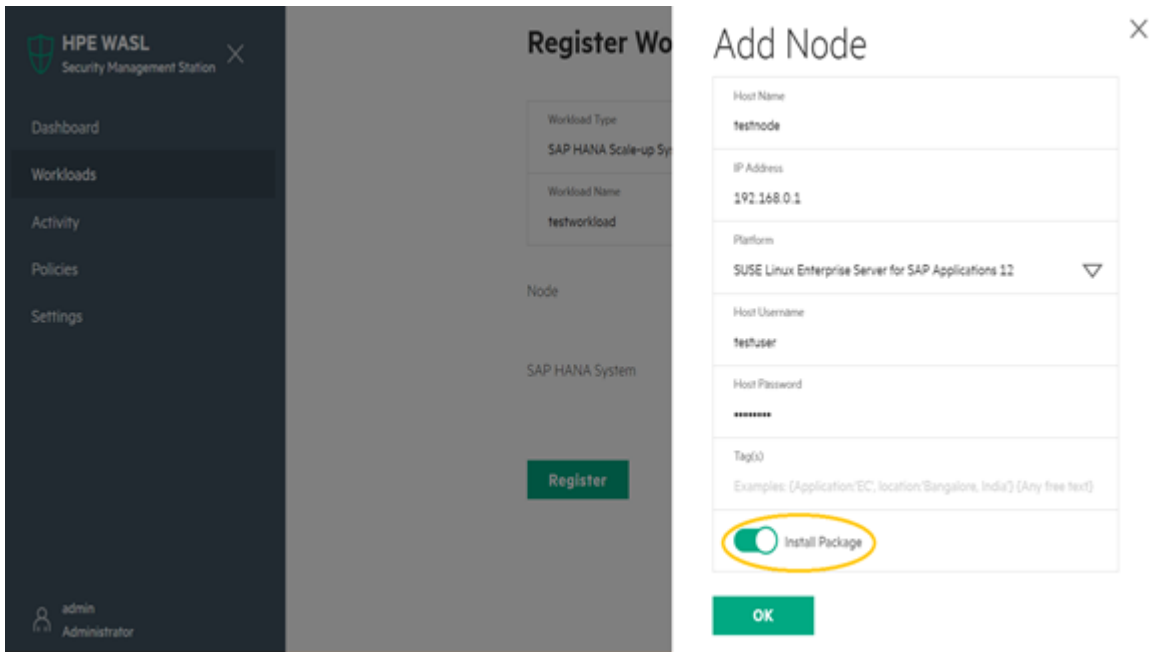
Cmdnd_Alias WASL_NODEKITS = /usr/bin/yum localinstall --nogpgcheck --assumeyes hpe_wasl_core.rpm, \
/usr/bin/yum localinstall --nogpgcheck --assumeyes hpe_wasl_os.rpm, \
/usr/bin/yum localinstall --nogpgcheck --assumeyes hpe_wasl_saphana.rpm, \
/usr/bin/yum localinstall --nogpgcheck --assumeyes openscap.rpm
Cmdnd_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. Use these commands to provide privilege for `<username>` to install and setup the Node packages.

NOTE: Home directory must be available and writable for the Host Username on the node.

4. Click the **Install Package** option from the **Add Node** screen during the workload registration (for any **Workload Type**).



The **Add Node** screen appears.

To know more details of what happens during automatic installation, see the [Manual Node Package installation and setup from Node](#) section.

Manual Node package installation and setup from node

Do the following to install and set up the Node packages manually as *root* user:

Installing node packages

Procedure

1. Insert the WASL ISO CD.
2. FTP or copy the node package contents to the node machine into a temporary package location (e.g.: `/tmp/rpms/`).
3. Log in to the node machine as root user and install the packages to `# cd /tmp/rpms/:`
 - 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.
4. Run the following command to install the required package based on the workload:

- For SLES OS workload, install the following:

```
# zypper install openscap_1*.rpm hpe_was1_core*.rpm hpe_was1_os*.rpm
```
- For SLES for SAP HANA, workload also install the *hpe_was1_saphana.rpm* RPM:

```
# zypper install openscap_1*.rpm hpe_was1_core*.rpm hpe_was1_os*.rpm hpe_was1_saphana*.rpm
```
- For RHEL OS workload, install the following:

```
# yum install openscap_1*.rpm hpe_was1_core*.rpm hpe_was1_os*.rpm
```

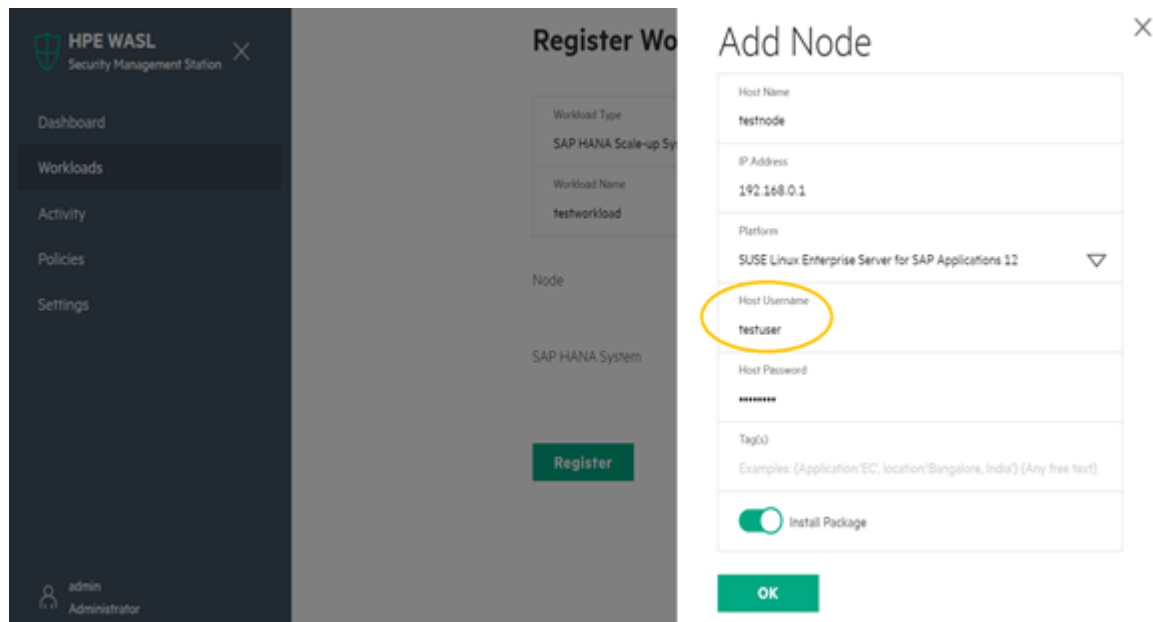
Run was1-setup to provide user privileges

Procedure

1. Run the `/opt/hpe/was1/core/bin/was1-setup` tool with `-a` option as *root* to allow users to run WASL workload operations with privileges on the node. Use of `was1-setup` tool varies for different types of workload:

- **Operating System Only** — This workload 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 not *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/was1/core/bin/was1-setup -a <Host username provided in Add Node screen of SMS>:root
```

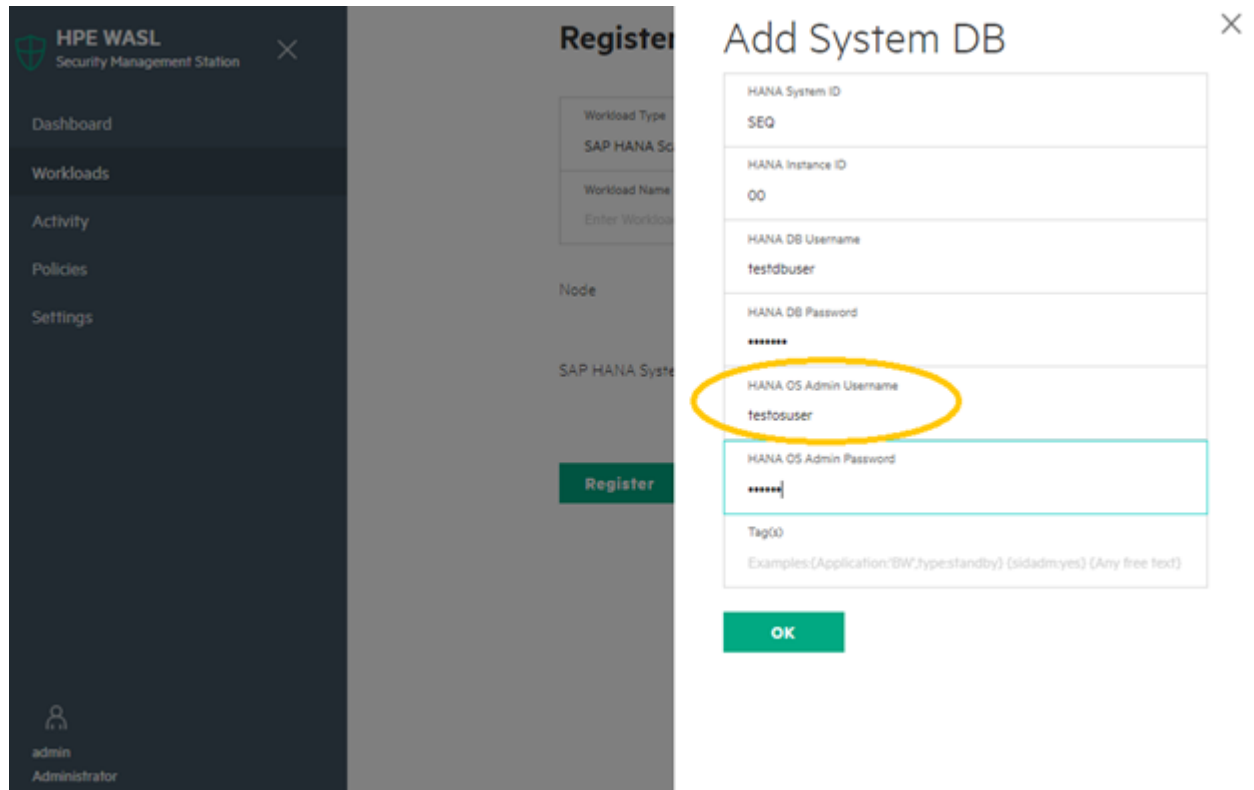


- **SAP HANA Scale-up System** — SAP HANA workload has following components to be secured:

- **Operating System** — To secure the operating system, perform the steps as mentioned in **Operating System Only**.
- **SAP HANA Database** — To secure SAP HANA database, WASL uses a newly created non-privileged user *waslhanauser* to connect to the SAP HANA database. If the **HANA OS Admin Username** provided in **Add System DB** screen of SMS is not *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 enables 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:

- Add `<user_name_b>` to `waslcore` group. This group has read and write access to most of the files related to WASL on the Node.
- Add `<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`).
- Create the following entry in `/etc/sudoers.d/hpewasl`, so that the `<user_name_a>` can run the workload operations (such as deploy, evaluation, remediation, and rollback) as `<user_name_b>` with privileges:


```
<user_name_a> ALL=(<user_name_b>) NOPASSWD: /opt/hpe/wasl/core/bin/wasl
```

Create certificates for waslhanauser users

Prerequisites

For securing SAP HANA database, WASL uses a newly created non privileged user `waslhanauser` to connect to the SAP HANA database. The SAP HANA database can be configured such that only secure communication is possible to the SAP HANA database. In such cases, the `waslhanauser` must have its certificate setup signed by the SAP HANA server certificate to connect to SAP HANA database.

Procedure

1. Run the following command as `root` user to generate this signed signatures:

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

NOTE: The SAP HANA workload registration enables 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*.

You can run `/opt/hpe/wasl/core/bin/wasl-setup --waslhanauser_cert_gen --sidadm=<sid>adm` script to:

- Create a `/home/waslhanauser/.ssl` directory with appropriate privileges if the directory is not existing.
- Create a RSA 2048 certificate that is valid for 365 days and a key. Regenerate this certificate after 365 days.
- Do `Sudo` to `<SID>adm` user and signs the newly created certificate using the master certificate of SAP HANA database.

Add sudoers for waslhanauser

- Run the following command to add sudoers for `waslhanauser` and to run specific scripts as root user:

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

- If you have selected `{sidadm=yes}` tag in the **Tags** field of the **Add System DB** screen, run the following command:

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

Migrating to WASL Version 1.2 or later

Before proceeding with the migration process, you must back up the data of WASL SMS Version 1.1. Once the backup process is completed successfully, you can restore the data on WASL Version 1.2 or later SMS Virtual Appliance.

Migration process involves the following:

1. **Backup WASL SMS Version 1.1** on page 35
2. **Migrate to WASL Version 1.2 or later** on page 36

Backup WASL SMS Version 1.1

Prerequisites

Ensure that the WASL SMS is up and running.

Procedure

1. Mount the WASL 1.2 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. Run the following command to stop the SMS

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

3. Run the following command to create backup:

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

4. Type **yes** to continue.

The backup gets created successfully.

5. Run the following command to list all the backup

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

The system displays the location of the backup data.

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

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

Following are the 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*

7. Copy *.ebck* and *.json* file which are related to the backup to the WASL 1.2 Virtual Appliance for restoration.

NOTE:

- The stash file is not backed up. You need to back up 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 `# /opt/hpe/wasl/sms/tools/wasl_sms.sh -reset_password` command.
 - Restoration is possible only on WASL Version 1.2 SMS Virtual Appliance.
-

Migrate to WASL Version 1.2 or later

Prerequisites

Before you begin, you must:

- Create the WASL Virtual Appliance. HPE recommends to restore WASL SMS on a fresh setup.
- Copy `<BACKUP>.ebck` and `<BACKUP>.json` backup files to `/var/opt/hpe/wasl/sms/backup/` directory and the *stashfile* (if master password is stored in *stashfile*) to a secure location, for example, `/var/opt/hpe/wasl/sms/backup/stashfile` on the target virtual appliance.
- Change the group owner of these copied files to `waslsms`.
 - Run `# chgrp waslsms <backupfiles>` to change the group. For example:

```
# chgrp waslsms /var/opt/hpe/wasl/sms/backup/<BACKUP>.ebck
# chgrp waslsms /var/opt/hpe/wasl/sms/backup/<BACKUP>.json
# chgrp waslsms /var/opt/hpe/wasl/sms/backup/stashfile
```
- Ensure only read access is allowed to the owner and the group using `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
```

Procedure

1. Log on to the WASL SMS Version 1.2 or later as `wasladmin`.
2. Type the username and password.
3. **Setup and run WASL SMS.**
4. Run the following command to restore the backup:

```
# sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -restore_backup
```
5. Type the Backup Name.
6. Select one of the following options to provide old master password:
 - Master password configured during the backup

OR

- Stash file (`/var/opt/hpe/wasl/sms/backup/stashfile`) saved during the backup (Ensure to delete it after restoration)

7. Type the Master and Recovery Password for the current setup.

The system restores the data successfully.

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

NOTE:

- The critical data on restored WASL SMS is encrypted with the new Master Password and the Recovery Key (if configured).
 - If you are restoring the WASL SMS Version 1.1 to WASL SMS Version 1.2 or later Virtual Appliance, it automatically migrates the database to WASL SMS Version 1.2 or later format.
-

Backup of 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 on to the WASL 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
```

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.

4. Type **Yes** to continue.

The backup gets 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 list all the backup.

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

The latest backup is listed at the end of backup list with the description provided. For example, `<BACKUP>.ebck` à `2018-12-3T12-56-55_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/2018-12-3T15-9-19_all_WASLSMS.*
```

Following are the 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 file to WASL 1.2 or later Virtual Appliance for restoration.

NOTE:

- The stash file is not backed up. You need to back up 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 # */opt/hpe/wasl/sms/tools/wasl_sms.sh -reset_password* command.
- Restoration is possible only on WASL Version 1.2 SMS Virtual Appliance.

-
8. **Restore to WASL Version 1.2 or later.**

Removing and reinstalling node packages

Removing of node packages will not remove any remediation done on the workloads on the node. You can rollback or reset these remediation from the SMS GUI first before removing node packages.

Follow the steps for removing and reinstalling the node packages:

Procedure

1. Click the required Workload.
2. This step is optional. You can skip the Rollback or Reset option and can continue from step 3.

Click the **Rollback** option.

Or

Click the **Reset** option. Click **Yes, reset** to restore the workload security state to the state prior to the first remediation operation.

3. Click **Undeploy Policy**.

NOTE: For more details on Rollback, Reset, and Undeploy Policy options, see *WASL User Guide*.

4. Click the drop-down arrow to select an element and a policy.
5. Click **Undeploy** to undeploy all profiles that is deployed on the Node.
6. Log in to the Node as root and run the following commands to remove the Node packages:

- For SLES OS workload, run the following command:

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

- For SLES for SAP HANA workload, run the following command to remove the `hpe_wasl_saphana.rpm` RPM:

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

- For RHEL OS workload, run the following command:

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

Some of the files such as snapshots, reports, deployed policies, certificates, and logs are not removed. The waslcore, waslcoreshare group, and waslhanauser user created during installation are also not removed.

These files and users are retained so that the system works properly when a user need to reinstall the Node packages and to monitor the node from the same registered WASL SMS.

To reinstall the node packages from the same registered WASL SMS, see **Node packages installation and setup** section.

7. Run the following commands to remove the files, users or groups:

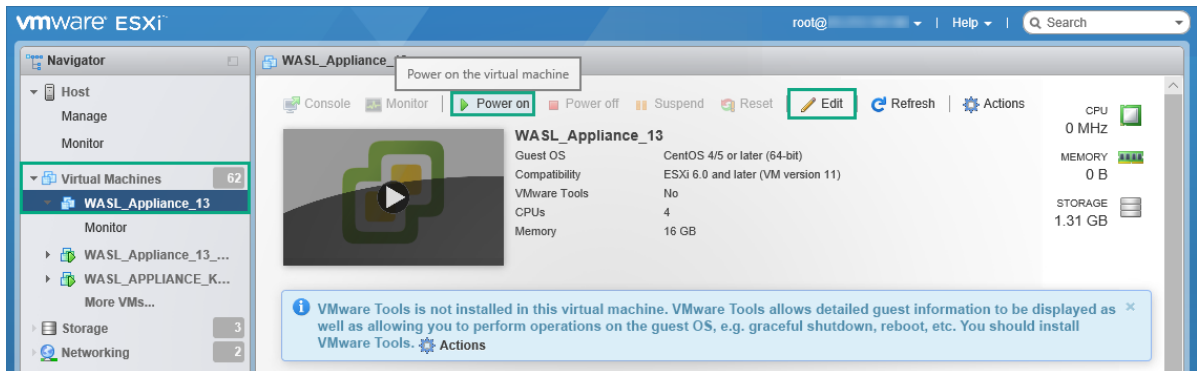
```
# rm -rf /opt/hpe/wasl/core
# rm -rf /var/opt/hpe/wasl/core
# userdel waslhanauser
# groupdel waslcore
# groupdel waslcoreshare
# rm /etc/sudoers.d/waslcore_install
```

You would have manually created the *waslcore_install* file during **Node packages installation and setup**.

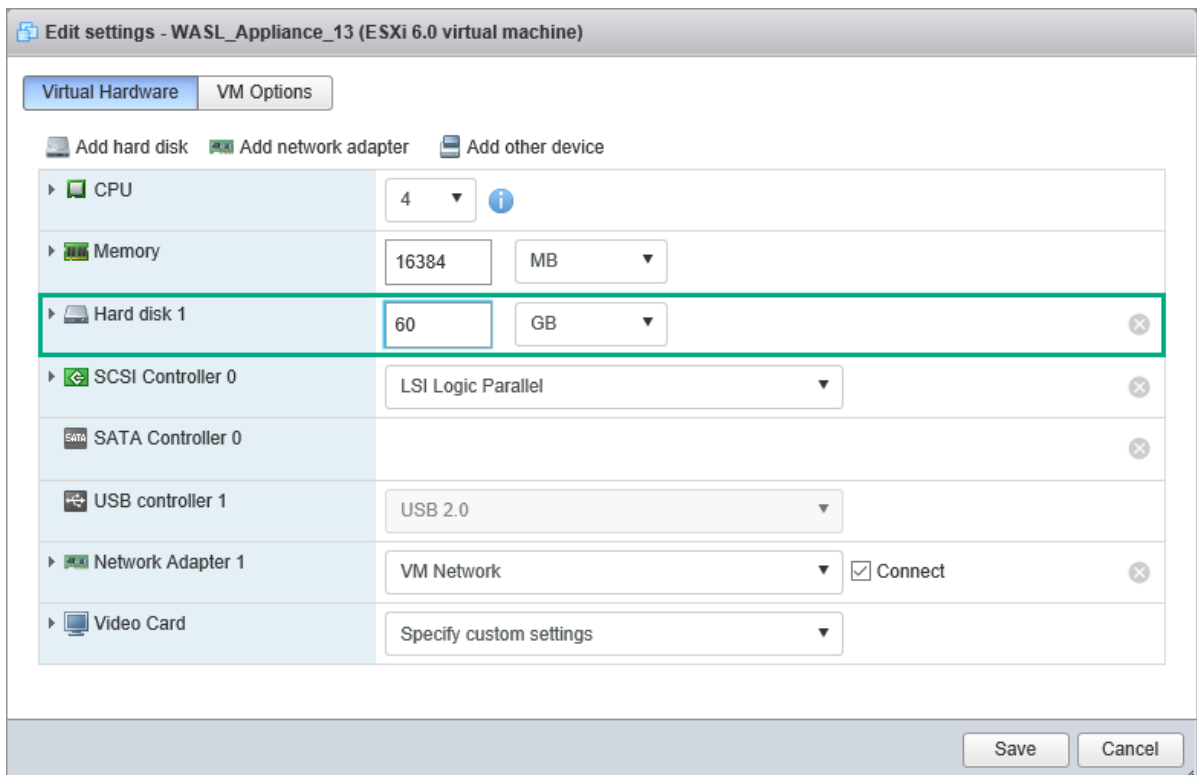
Extending the disk partitions

Procedure

1. **Stop the SMS** and **back up the virtual appliance** to a different location.
2. Log in to VMware ESXi web interface.
3. Click **Virtual Machine** and click the WASLSMS virtual appliance from the list.
4. Click **Power off** to shut down the virtual appliance.



5. Click **Edit** to modify the size of hard disk.
6. Enter the required **Hard disk 1** size to extend the disk partition.



7. Click **Save** and click **Power on**.
8. Click **Launch console** and log in with the root user credentials.

The virtual machine console opens in a new tab of the web browser.

9. Unlock the root account.

Use the root account to log in to the WASL virtual appliance.

10. Run the `lvs` command to view the details of the logical volumes (partitions).

11. Run the `cat /opt/hpe/wasl/sms/tools/partition_percentages.sh` command to view the percentage allocated for the different partitions.

By default, 100% of disk space is allocated to `/var` partition.

To change the default partitions, copy the `/opt/hpe/wasl/sms/tools/partition_percentages.sh` file as a separate file. For example, `/root/partition_percentages.sh`.

Modify the percentages in this file for the relevant partition variable.

12. Run the following command to increase the partition size:

```
/usr/bin/sh /opt/hpe/wasl/sms/tools/expand_partiton.sh default_size or
```

or

```
/usr/bin/sh /opt/hpe/wasl/sms/tools/expand_partiton.sh  
<path_to_user_defined_partition_percentages file>
```

NOTE: You can extend the disk partitions maximum two times.

13. Run the `lvs` command to view the details of the logical volumes (partitions).

14. Lock the root account.

15. Log in to the SMS virtual appliance as `wasladmin` user and **start the SMS.**

Best practices

HPE recommends to lock the root account immediately after resolving the WASL Virtual Appliance-related issues.

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Server Infrastructure Security Solutions

<http://www.hpe.com/go/security>

WASL websites

HPE WASL User Guide

OpenSCAP portal

<https://www.open-scap.org/>

For additional websites, see [Support and other resources](#).

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
<http://www.hpe.com/info/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
<http://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

www.hpe.com/support/hpesc

Hewlett Packard Enterprise Support Center: Software downloads

www.hpe.com/support/downloads

Software Depot

www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

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:

www.hpe.com/support/AccessToSupportMaterials

! **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.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

<http://www.hpe.com/support/selfrepair>

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

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

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

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

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:

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:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

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.

Sample run of SMS setup

Following are the sample runs of WASL SMS setup, Backup and Migration of WASL SMS data, and iptables rules:

WASL SMS setup

```
sudo /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).
```

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

Would you like to continue? [yes]:

```
===== 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]:wasladmin
Invalid input. Please try again with either 'yes' or 'no'.
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 forgotten or lost.

```
Enter the recovery password: *****
Confirm the recovery password: *****
```

Configuration of SMS with Security Settings is in-progress...

Successfully configured SMS with Security Settings.

```
=====
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]:

Creating Self-Signed Certificate....

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) [localhost.localdomain]:
Email Address [user@hostname.com]:
```

Successfully created Self-signed certificates for HPE WASL SMS

Successfully set up the HPE WASL SMS

Backup WASL SMS data

```
/opt/hpe/wasl/sms/tools
# ./wasl_backup.sh
No input argument
Usage: ./wasl_backup.sh -create_backup [-description "<description_text>"]
        ./wasl_backup.sh -list_backup [-name <backup_name>]
        ./wasl_backup.sh -help
# ./wasl_backup.sh -create_backup
WASL SMS found a stashfile (/opt/hpe/wasl/sms/data/stashfile).
The master password stored in the stashfile will be used to access and backup
WASL SMS data and configuration.
```

Note: The stashfile will not be saved into the backup.
In-order to restore the backup, this stashfile or the current
master password should be provided.
You need to either remember the current master password
or take a copy of the stashfile (/opt/hpe/wasl/sms/data/stashfile).

Would you like to continue? [yes]:

```
===== HPE WASL SMS BACKUP =====
```

Successfully created backup: /var//opt/hpe/wasl/sms//backup/2018-11-27T18-22-49_all_WASLSMS.ebck

```
# ./wasl_backup.sh -list_backup
```

```
===== HPE WASL SMS BACKUP LIST =====
```

All backups are available under /var//opt/hpe/wasl/sms/backup directory

```

Backup Name: 2018-11-27T18-22-49_all_WASLSMS.ebck | created on: 11/27/2018, 6:22:49 PM |
SMS VERSION: 1.1.0 | type: all | Description :
# scp /var//opt/hpe/wasl/sms/backup/2018-11-27T18-22-49_all_WASLSMS.*
wasladmin@<destination-IPAddress>:/var//opt/hpe/wasl/sms/backup/
wasladmin@xx.xx.xx.xx's password:
2018-11-27T18-22-49_all_WASLSMS.ebck          100% 3271KB   3.2MB/s   00:00
2018-11-27T18-22-49_all_WASLSMS.json        100%  273     0.3KB/s   00:00
#

```

Migrate to WASL Version 1.2

```

/opt/hpe/wasl/sms/tools
[wasladmin@wasldemo tools]$ sudo ./wasl_sms.sh -list_backup

===== HPE WASL SMS BACKUP LIST =====
All backups are available under /var//opt/hpe/wasl/sms/backup directory

Backup Name: 2018-11-27T18-22-49_all_WASLSMS.ebck | created on: 11/27/2018, 6:22:49 PM |
SMS VERSION: 1.1.0 | type: all | Description :

[wasladmin@wasldemo tools]$ sudo ./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).

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

Would you like to continue? [yes]:

===== 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 forgotten or lost.

Enter the recovery password: *****
Confirm the recovery password: *****

Configuration of SMS with Security Settings is in-progress...

Successfully configured SMS with Security Settings.

=====
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]:

Creating Self-Signed Certificate....

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) [wasldemo]:
Email Address [user@hostname.com]:

Successfully created Self-signed certificates for HPE WASL SMS

Successfully set up the HPE WASL SMS

===== Restore Backup SMS Data =====
If you have a previous deployment of SMS, then you can take a backup from the
previous deployment and restore it in this SMS instance.

Refer to the WASL Install and Setup guide for information on how to take a
backup and restore it.

Do you want to restore SMS data from the backup file? [no]:yes

Enter the 'Backup Name' to restore (use 'wasl_sms.sh -list_backup' to list all the backups):2018-11-27T18-22-49_all_WASLSMS.ebck

Master Password or 'stashfile' used during the backup is required to restore.

How do you want to provide the old master password?
1. Entering the password
2. Entering the stashfile location
3. Exit restore
Select an option [1]:

Enter the old master password:: *****

Require 'Master Password' and 'Recover Password' (if configured) to restore the
backup into the current setup.

Using the current master password from the stashfile.

Provide the Recovery Password of the current setup:: *****

===== HPE WASL SMS BACKUP RESTORE =====
Restored config files and DB successfully.
Restored policies successfully.
Restored reports successfully.
Restored logs successfully.
Data migrated successfully.

```

Unlock the root account

```

# sudo /opt/hpe/wasl/sms/tools/lockunlock_root.sh -unlock
[sudo] password for wasladmin: <<<<< Enter the password of wasladmin one again here
Enter the root user Password : <<<<< Enter a new password for root user
Confirm the root user Password : usermod: no changes <<<<< Re-Enter the new password once
again
root user is enabled with the given password. Please lock the root user after usage.

```

Lock the root account

```

# sudo /opt/hpe/wasl/sms/tools/lockunlock_root.sh -lock
root user is successfully locked.

```

iptables rules

Following iptable rules are configured in the virtual appliance:

```

# sudo iptables -S
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT DROP
-A INPUT -i lo -j ACCEPT
-A INPUT -s 127.0.0.0/8 -j DROP
-A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT

```

```

-A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p tcp -m tcp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT

```

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 #####

```

```

sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -setup

```

OR

```

sudo /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.

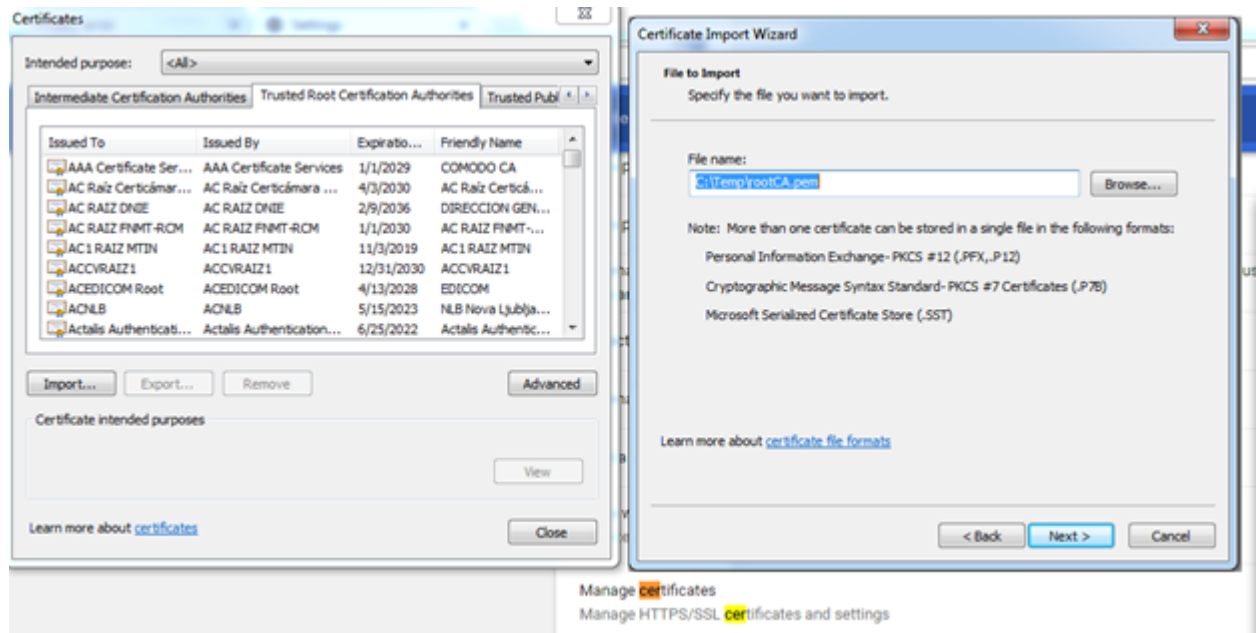
Enter your server key location [/etc/ssl/certs/wasl/key.pem]:/sign/sms.key

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 through **Menu->Settings->Advanced->Manage Certificate** in Chrome browser).



WASL Logs

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

Location	Name	Description
<i>/var/log/hpe_wasl_sms/</i>	<i>cert_gen.log</i>	Certificate generation details
<i>/var/log/hpe_wasl_sms/</i>	<i>wasl_sms.log</i>	<p>Main log file related to SMS. Many of the SMS errors gets logged here.</p> <p>We can enable HTTP/HTTPS access logs by setting <code>config.web.logger</code> to 'common' in configuration file: <code>/opt/hpe/wasl/sms/config/custom_config.js</code></p> <p>This log file is auto rotated daily by the configuration in <code>/etc/logrotate.d/hpe_wasl_sms</code> 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 <code>/etc/logrotate.conf</code> file. You can change the retention period or the log rotation interval by editing the <code>/etc/logrotate.d/hpe_wasl_sms</code> file. For more information on using logrotate feature on Linux, see man page of logrotate.</p>
<i>/var/log/hpe_wasl_sms/logs/</i>	<i>operationLog.txt</i>	Logs of all operations performed on SMS
	<i>WASLServerError.log</i>	Any internal errors seen by WASL (currently only policy module errors)
<i>SMS GUI Screen</i>	<i>Activity tab in SMS GUI</i>	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
<i>/var/opt/hpe/wasl/core/log/</i>	<i>./system/systemlog.txt</i>	Generic logging of different activity on Node on system workload
	<i>./hana/hanalog.txt</i>	Generic logging of different activity on Node on SAP HANA workload
<i>/var/opt/hpe/wasl/core/snapshot</i>	<i>./system/snapshot_<datetime>/snapshot/system_rollback.log</i>	Logs related to system snapshots taken during remediation and rollback/reset
	<i>./hana/snapshot_<datetime>/snapshot/snapshot.log</i>	Logs related to SAP HANA snapshots taken during remediation and rollback/reset

Table Continued

Location	Name	Description
	<code>./hana/ snapshot_<datetime>/ reset.log</code>	Logs related to SAP HANA rollback/reset
	<code><user_home_dir_doing_nod e_page_automatic_install_fr om_SMS> install_wasl_rpms.log</code>	Logs related to Node packages auto installation and setup

Hardened WASL SMS appliance

The WASL SMS appliance is secured by default to minimize the attack surface and eliminate the security risks. The following are few steps performed to harden the appliance:

- Pre-configured the appliance with system level firewall to block all network ports except the required ports (HTTPS - 443 and SSH - 22).
- Only `wasladmin` account (non-root system account) is enabled for login into the appliance.
- The services and software, which are not required, are disabled and removed from the appliance.
- Harden the appliance with a CIS benchmark based OS Security policy (OS Security Policy for WASL SMS Virtual Appliance). For more details, see *WASL User Guide*.

Disk partitions extension

Following is the sample run for extending the disk partitions for WASL appliance:

```
[root@WASLSMS ~]# lvs
  LV          VG      Attr          LSize   Pool Origin Data%  Meta%  Move Log
Cpy%Sync Convert
  home        centos -wi-ao----- 956.00m
  root        centos -wi-ao-----  7.45g
  swap        centos -wi-ao----- 956.00m
  tmp         centos -wi-ao----- 476.00m
  var         centos -wi-ao----- <18.63g
  var_log     centos -wi-ao-----  <3.73g
  var_log_audit centos -wi-ao-----  1.86g
  var_tmp     centos -wi-ao----- 476.00m
```

```
[root@WASLSMS ~]#
```

```
[root@WASLSMS ~]# sh /opt/hpe/wasl/sms/tools/expand_partiton.sh default_size
This program will change the disk partition.
```

```
It is highly recommended to backup WASL Appliance using 'sudo /opt/hpe/
wasl/sms/tools/wasl_sms.sh -create_backup'; and copy the backup file and the
stashfile to different machine.
```

```
Do you want to continue [yes/no]? [yes]:yes
```

```
Size of logical volume centos/var changed from <18.63 GiB (4769 extents) to
<28.63 GiB (7329 extents). Logical volume centos/var successfully resized.
Successfully extend the partitions in WASL appliance.
```

```
[root@WASLSMS ~]#
```

```
[root@WASLSMS ~]# lvs
```

```
  LV          VG      Attr          LSize   Pool Origin Data%  Meta%  Move Log
Cpy%Sync Convert
  home        centos -wi-ao----- 956.00m
  root        centos -wi-ao-----  7.45g
```

```
swap          centos -wi-ao----- 956.00m
tmp           centos -wi-ao----- 476.00m
var           centos -wi-ao----- <28.63g
var_log       centos -wi-ao----- <3.73g
var_log_audit centos -wi-ao-----  1.86g
var_tmp       centos -wi-ao----- 476.00m
[root@WASLSMS ~]#
```


Acronyms

Acronym	Definition
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, SP4	Service Pack 1, Service Pack 2, Service Pack 3, Service Pack 4
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