Hewlett Packard
Enterprise

HPE Storage Operations Manager

Software Version: 10.20
Windows® and Linux® operating systems

Hardening Guide

Document Release Date: August 2016
Software Release Date: August 2016

Legal Notices

Warranty

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. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

AMD is a trademark of Advanced Micro Devices, Inc.

© 2012 Google Inc. All rights reserved. Google™ is a trademark of Google Inc.

Intel®, Intel® Itanium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, and Windows Server® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SAP®, SAP® BusinessObjects™, and SAP® BusinessObjects™ Web Intelligence® are the trademarks or registered trademarks of SAP SE in Germany and in several other countries.

UNIX® is a registered trademark of The Open Group.

Oracle Technology – Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, see the `open_source_third_party_license_agreements.pdf` file in the `license-agreements` directory in the SOM product download file.

Acknowledgements

This product includes software developed by the Apache Software Foundation.
(http://www.apache.org)

This product includes software developed by the Indiana University Extreme! Lab.
(http://www.extreme.indiana.edu)

This product uses the j-Interop library to interoperate with COM servers.
(http://www.j-interop.org)

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

Visit the HPE Software Support web site at: **https://softwaresupport.hpe.com**

This web site provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software Support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

To find more information about access levels, go to:
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

Contents

Using this Guide

This document provides information for increasing the security of your SOM installation. The information in this document applies to SOM 10.20. For security configuration for another version of the product, see the appropriate documentation for that version.

Unless otherwise specified within a procedure, the expected use model for the content in this document is as follows:

1. Stop all SOM services (see "Start, Stop, or Restart All SOM Services" on page 13).
2. Apply the desired configurations as described in this document.

   > **Note:** Remember to back up each configuration file to a location outside the SOM directory structure before making any changes.

3. Start all SOM services (see "Start, Stop, or Restart All SOM Services" on page 13).

Communication Configuration

This topic describes the default security configurations for communication within SOM.

By default, SOM web server supports HTTPS protocols TLSv1.1 and higher versions (recommended) for communication. However, if you want to enable HTTP for communication, see "Enable Non-SSL Communications" below. For instructions on configuring SOM to use other protocols, see "Configure TLS Protocols" below.

Configure TLS Protocols

By default, SOM web server supports TLSv1.1 and higher versions of security protocols for communication. You can also configure SOM to use other higher or lower versions of security protocols for communication, as needed.

> **Note:** We strongly recommend that you do not enable the lower versions of security protocols (for example, TLSv1.0) unless they are needed for communicating with applications that do not support TLSv1.1 and higher protocols.

To configure the protocols, use the `com.hp.ov.nms.ssl.PROTOCOLS` parameter in the following file:

- *Windows*:

  `%OvDataDir%\nmsas\nnm\server.properties`
- *Linux*:

  `/var/opt/OV/nmsas/nnm/server.properties`

Enable Non-SSL Communications

By default, SOM supports HTTPS for communication.

> **Note:** We strongly recommend that you use HTTPS for communication with the SOM web server.

To enable HTTP for communication, set the `com.hp.ov.nms.ui.https.only` parameter to `false` in the following file:

- *Windows*:

  `%OvDataDir%\shared\nnm\conf\props\nms-ui.properties`
- *Linux*:

  `/var/opt/OV/shared/nnm/conf/props/nms-ui.properties`

For example:

```
com.hp.ov.nms.ui.https.only = false
```

Encryption

This topic describes the default security configurations for encryption and hashing within SOM.

- During installation, SOM generates a self-signed certificate using a 2048-bit encryption key, SHA1, and RSA.

  > **Note:** HP recommends using a CA-signed certificate instead of the self-signed certificate provided by SOM.

- For local authentication into SOM, SOM uses a salted SHA-256 password hash for storing SOM user passwords.
- For encryption of device passwords stored in the SOM database, SOM uses the AES 128 algorithm.

User Authentication

Users can authenticate into the SOM console by using a local user account or by using one of several external authentication components. Each approach requires administrative setup.

Local user accounts

Local user accounts are specific to the SOM installation only. SOM does not support password policy configuration for local user accounts.

> **Note:** If the security standards of your environment require a specific password policy (for example, minimum password length or password expiration), it is recommended to use an external mechanism for user authentication. See "External authentication" below.

For information about creating local SOM user accounts, see "Configure User Accounts" in the SOM help.

External authentication

The administrator of the external authentication component determines the security behaviors for all users and all applications that use that component.

SOM supports the following external authentication approaches:

- Integration with a directory service. For information, see "LDAP-Based Authentication" in the *SOM Deployment Guide*.
- PKI user authentication, which includes support for smart cards such as common access card (CAC). For information, see "Configuring SOM to Support Public Key Infrastructure User Authentication" in the *SOM Deployment Guide*.

SOM console session timeout

By default, the SOM console session timeout is 18 hours. The SOM administrator can change this value for all SOM console users in the **Console Timeout** field on the User Interface Configuration form (**Configuration > User Interface > User Interface Configuration**).

> **Note:** It is recommended to configure the session timeout in accordance with the policy for your environment.

Clickjacking Protection

SOM is configured for linked pages to open in new frames when the links are from the SAMEORIGIN as the SOM management server. This configuration is not changeable.

Strengthen Security

You can strengthen the security of SOM by applying any or all of the following changes:

- "Configure the Ciphers Used by the SOM Web Server" below
- "Limit User Access to the SOM Server" on the next page

Configure the Ciphers Used by the SOM Web Server

SOM supports the following ciphers for secure communications with the SOM web server:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

To change the list of protocols that SOM can use, uncomment and configure the `com.hp.ov.nms.ssl.CIPHERS` parameter in the following file:

- *Windows*:

  `%OvDataDir%\shared\nnm\conf\props\nms-jboss.properties`
- *Linux*:

  `/var/opt/OV/shared/nnm/conf/props/nms-jboss.properties`

This parameter contains an ordered list of one or more ciphers. If SOM is unable to use the first cipher in the list to establish a connection between the SOM web server and the user's web browser, SOM tries to use the next cipher, and so forth. (The preceding list shows the default cipher ordering.)

You can edit the value of the `com.hp.ov.nms.ssl.CIPHERS` parameter to delete ciphers that SOM should not use and to change the order in which SOM attempts to use the available ciphers.

If you change the list of supported ciphers, HP recommends ordering the ciphers list in order of strength. That is, place 256-bit encryption above 128-bit encryption.

HP recommends changing the order of the ciphers list to place 256-bit encryption above 128-bit encryption and to remove the weakest encryption algorithms as follows:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256

For example:

```
com.hp.ov.nms.ssl.CIPHERS=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_
SHA,TLS_RSA_WITH_AES_128_CBC_SHA256
```

Note:

- The value of the `com.hp.ov.nms.ssl.CIPHERS` parameter must be a comma-separated list that contains no white space and is one contiguous line.
- Save the cipher list before changing it. Removing ciphers from the `com.hp.ov.nms.ssl.CIPHERS` list can prevent SOM from starting.
- The web browser must support at least one of the configured ciphers.

Limit User Access to the SOM Server

It is recommended to limit traffic to the SOM server to only those users who should have access. Possible ways to limit this traffic include:

- Configure a firewall in front of the SOM management server.

  For information about the ports that SOM uses, see the *SOM Deployment Guide*.
- Isolate user access to the SOM management server on specific network interfaces only.

Distributed Denial of Service Attack Protection

A few Distributed Denial of Service (DDoS) attacks such as Slowloris/Slow read can be mitigated by implementing a third-party protection such as, Apache HTTP Server as Revers Proxy. For this use `mod_reqtimeout` and `mod_qos`.

Note: Due to the nature of these types of attacks, it is not possible to implement application-specific fixes or enhancements to prevent these types of attacks.

For more information, refer to the following:

https://www.howtoforge.com/how-to-defend-slowloris-ddos-with-mod_qos-apache2-on-debianlenny

Start, Stop, or Restart All SOM Services

Stopping the SOM services before changing the SOM configuration prevents conflicting data from being stored in the SOM database. Some procedures call for restarting the SOM services to read the updated configuration.

To start all SOM services

- *Windows*: Do one of the following:
  - From the Windows Start menu, run **All Programs > HP > Storage Operations Manager > ovstart**.
  - Run the following command:

    ```
    %OvInstallDir%\bin\ovstart
    ```
- *Linux*: Run the following command:

  ```
  /opt/OV/bin/ovstart
  ```

To stop all SOM services

- *Windows*: Do one of the following:
  - From the Windows Start menu, run **All Programs > HP > Storage Operations Manager > ovstop**.
  - Run the following command:

    ```
    %OvInstallDir%\bin\ovstop
    ```
- *Linux*: Run the following command:

  ```
  /opt/OV/bin/ovstop
  ```

To restart all SOM services

- *Windows*: Do one of the following:
  - From the Windows Start menu, run **All Programs > HP > Storage Operations Manager > ovstop**, and then run **All Programs > HP > Storage Operations Manager > ovstart**.
  - Run the following commands:

    ```
    %%OvInstallDir%\bin\ovstop
    %OvInstallDir%\bin\ovstart
    ```
- *Linux*: Run the following commands:

  ```
  /opt/OV/bin/ovstop
  /opt/OV/bin/ovstart
  ```

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Hardening Guide (Storage Operations Manager 10.20)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to storage-management-doc-feedback@hpe.com.

We appreciate your feedback!